

**Y2K AND CONTINGENCY AND DAY 1 PLANS:
IF COMPUTERS FAIL, WHAT WILL YOU DO?**

JOINT HEARING
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
OF THE
COMMITTEE ON GOVERNMENT REFORM
AND THE
SUBCOMMITTEE ON TECHNOLOGY
OF THE
COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS
FIRST SESSION

OCTOBER 29, 1999

Committee on Government Reform

Serial No. 106-51

Committee on Science

Serial No. 106-54

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



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

U.S. GOVERNMENT PRINTING OFFICE

61-119 CC

WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

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

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

DAVID A. KASS, *Deputy Counsel and Parliamentarian*

CARLA J. MARTIN, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

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

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

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

MATT RYAN, *Senior Policy Director*

CHIP AHLSEWEDE, *Clerk*

TREY HENDERSON, *Minority Counsel*

COMMITTEE ON SCIENCE

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

SHERWOOD L. BOEHLERT, New York	RALPH M. HALL, Texas, RMM**
LAMAR SMITH, Texas	BART GORDON, Tennessee
CONSTANCE A. MORELLA, Maryland	JERRY F. COSTELLO, Illinois
CURT WELDON, Pennsylvania	JAMES A. BARCIA, Michigan
DANA ROHRABACHER, California	EDDIE BERNICE JOHNSON, Texas
JOE BARTON, Texas	LYNN C. WOOLSEY, California
KEN CALVERT, California	LYNN N. RIVERS, Michigan
NICK SMITH, Michigan	ZOE LOFGREN, California
ROSCOE G. BARTLETT, Maryland	MICHAEL F. DOYLE, Pennsylvania
VERNON J. EHLERS, Michigan*	SHEILA JACKSON-LEE, Texas
DAVE WELDON, Florida	DEBBIE STABENOW, Michigan
GIL GUTKNECHT, Minnesota	BOB ETHERIDGE, North Carolina
THOMAS W. EWING, Illinois	NICK LAMPSON, Texas
CHRIS CANNON, Utah	JOHN B. LARSON, Connecticut
KEVIN BRADY, Texas	MARK UDALL, Colorado
MERRILL COOK, Utah	DAVID WU, Oregon
GEORGE R. NETHERCUTT, Jr., Washington	ANTHONY D. WEINER, New York
FRANK D. LUCAS, Oklahoma	MICHAEL E. CAPUANO, Massachusetts
MARK GREEN, Wisconsin	BRIAN BAIRD, Washington
STEVEN T. KUYKENDALL, California	JOSEPH M. HOEFFEL, Pennsylvania
GARY G. MILLER, California	DENNIS MOORE, Kansas
JUDY BIGGERT, Illinois	VACANCY
MARSHALL "MARK" SANFORD, South Carolina	
JACK METCALF, Washington	

SUBCOMMITTEE ON TECHNOLOGY

CONSTANCE A. MORELLA, Maryland, *Chairwoman*

CURT WELDON, Pennsylvania	JAMES A. BARCIA, Michigan**
ROSCOE G. BARTLETT, Maryland	LYNN N. RIVERS, Michigan
GIL GUTKNECHT, Minnesota*	DEBBIE STABENOW, Michigan
THOMAS W. EWING, Illinois	MARK UDALL, Colorado
CHRIS CANNON, Utah	DAVID WU, Oregon
KEVIN BRADY, Texas	ANTHONY D. WEINER, New York
MERRILL COOK, Utah	MICHAEL E. CAPUANO, Massachusetts
MARK GREEN, Wisconsin	BART GORDON, Tennessee
STEVEN T. KUYKENDALL, California	BRIAN BAIRD, Washington
GARY G. MILLER, California	

EX OFFICIO

F. JAMES SENSENBRENNER, JR., Wisconsin+	RALPH M. HALL, Texas+
--	-----------------------

CONTENTS

Hearing held on October 29, 1999	Page 1
Statement of:	
Dyer, John, Principal Deputy, Social Security Administration; Marvin J. Langston, Deputy Assistant Secretary of Defense for C3I and year 2000, Department of Defense, accompanied by Rear Admiral Bob Willard and Bill Curtis, Department of Defense; John Gilligan, Chief Information Officer, Department of Energy; Paul Cosgrave, Chief Information Officer, Internal Revenue Service; and Norman E. Lorentz, senior vice president, Chief Technology Officer, U.S. Postal Service	47
Willemssen, Joel C., Director, Civil Agencies Information Systems, U.S. General Accounting Office; and John Spotila, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget	12
Letters, statements, etc., submitted for the record by:	
Cosgrave, Paul, Chief Information Officer, Internal Revenue Service, prepared statement of	86
Davis, Hon. Thomas M., a Representative in Congress from the State of Virginia, prepared statement of	11
Dyer, John, Principal Deputy, Social Security Administration, prepared statement of	50
Gilligan, John, Chief Information Officer, Department of Energy, prepared statement of	75
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	113
Langston, Marvin J., Deputy Assistant Secretary of Defense for C3I and year 2000, Department of Defense, prepared statement of	62
Lorentz, Norman E., senior vice president, Chief Technology Officer, U.S. Postal Service, prepared statement of	91
Morella, Hon. Constance A., a Representative in Congress from the State of Maryland:	
Letter dated October 15, 1999	102
Prepared statement of	3
Spotila, John, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, prepared statement of	36
Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of	8
Willemssen, Joel C., Director, Civil Agencies Information Systems, U.S. General Accounting Office, prepared statement of	14

Y2K AND CONTINGENCY AND DAY 1 PLANS: IF COMPUTERS FAIL, WHAT WILL YOU DO?

FRIDAY, OCTOBER 29, 1999

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY OF THE COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON TECHNOLOGY OF THE COMMITTEE ON SCIENCE,

Washington, DC.

The subcommittees met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Connie Morella (chairwoman of the Subcommittee on Technology) presiding.

Present: Representatives Morella, Davis, and Turner.

Staff present from the Subcommittee on Government Management, Information, and Technology: J. Russell George, staff director and chief counsel; Matt Ryan, senior policy director; Bonnie Heald, communications director and professional staff member; Chip Ahlswede, clerk; Rob Singer, staff assistant; P.J. Caceres and Deborah Oppenheim, interns; Trey Henderson, minority counsel; and Jean Gosa, minority staff assistant.

Mr. DAVIS. This hearing will come to order. I would ask unanimous consent that the cochair of the House Task Force on the Year 2000 Problem, the Honorable Connie Morella of Maryland, chairwoman of the House Science Subcommittee on Technology, chair today's meeting.

Without objection, so ordered.

Mrs. MORELLA. Thank you. Thank you, Mr. Davis.

I want to welcome all of you on, the past 3½ years, my Science Committee Technology Subcommittee and the Government Reform Committee's Government Management, Information, and Technology Subcommittee, chaired by Steve Horn of California, who incidentally couldn't be here this morning. We have been engaged in the review of the year 2000 computer problem with a series of joint hearings and initiatives. Our two subcommittees, which comprise the House Y2K Working Group, have been pushing for greater Federal Y2K focus to correct the millennium bug.

Since we first began our oversight hearings, we've seen vast and significant progress from our Federal agencies. And in most instances, Y2K was finally mandated as an agencywide priority. Management leadership was required where previously there was none, and we're very pleased with the results we've seen.

We have been comforted by the actions of a greater majority of Federal agencies. But unfortunately, with only 63 days remaining before the January 1st, 2000, deadline, there still remains some

concern about certain agencies, especially with regard to their contingency and day 1 plans. To be fully prepared for Y2K, every organization must ensure that their day 1 strategies are ready and that practical contingency plans are in place.

Contingency plans provide assurance that a Federal agency has covered all predictable possibilities to ensure that its mission-critical operations can continue without disruption.

Our day 1 strategy provides a comprehensive set of actions to be executed by a Federal agency during the last days of 1999 and the first days of 2000. For those who may have watched the recently concluded World Series on television, you may have seen an advertisement, teaser, for an upcoming network movie on Y2K. In an effort to hype the movie and to create interest in viewers, in the teaser an ominous voice boomed, Y2K, what if they're wrong?

Despite its questionable entertainment value, I think the movie is the one that will actually have it all wrong. One of the most effective methods, however, to survive the movie's hype and to calm any fears that may result is for Federal agencies to have effective contingency plans and day 1 strategies that provide all Americans adequate assurances our Federal Government will not be adversely attacked and affected by Y2K.

Recently, the Office of Management and Budget [OMB], provided guidance to assist Federal agencies in preparing day 1 plans. These plans are prepared for finite timeframes, like the end of December through early January, to help mitigate any problems that may arise. They should address the full scope of agency activity that will be underway during that period.

For example, agencies must prepare to mitigate the impact of possible failures in internal systems, buildings and other infrastructures. Furthermore, the plan should include agency efforts to assess the Y2K impact on its business partners, such as State and local governments, in delivering the Federal programs.

I'm pleased to welcome representatives of a number of Federal agencies to discuss and review the status of their contingency plans and day 1 strategies. And I look forward to the testimony from the Social Security Administration, the Department of Defense, the Department of Energy, the Internal Revenue Service and the Postal Service. And in our first panel, we will hear from the General Accounting Office and the Office of Management and Budget.

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

Opening Statement of
Congresswoman Constance A. Morella

Chairwoman, Technology Subcommittee
House Science Committee

**Y2K Contingency and Day One Plans:
If Computers Fail, What's the Plan?**

Oversight hearing on the status of
business continuity and contingency plans (BCCP) of certain federal agencies

Friday, October 29, 1999

In the past 3½ years, my Science Committee's Technology Subcommittee and the Government Reform Committee's Government Management, Information and Technology Subcommittee, chaired by Steve Horn of California, have been engaged in the review of the Year 2000 computer problem with a series of joint hearings and initiatives.

Our two subcommittees, which comprise the House Y2K Working Group, has been pushing for a greater Federal Y2K focus to correct the millennium bug.

Since we first began our oversight hearings, we have seen vast and significant progress from our Federal agencies – in most instances, Y2k was finally mandated as an agency-wide priority and management leadership was required where previously there was none.

While we have been comforted by the actions of the great majority of Federal agencies, unfortunately with just 63 days remaining before the January 1, 2000 deadline, there still remains some concern about certain agencies – especially with their contingency and Day One plans.

To be fully prepared for Y2K, every organization must ensure that their Day One strategies are ready and that practical contingency plans are in place.

Contingency plans provide assurance that a federal agency has covered all predictable possibilities to ensure that its mission-critical operations can continue without disruption.

A Day One strategy provides a comprehensive set of actions to be executed by a federal agency during the last days of 1999 and the first days of 2000.

For those who may have watched the recently concluded World Series on television, you may have seen an advertisement teaser for an upcoming network movie on Y2K.

In an effort to hype the movie and to create interest in viewers, in the teaser, an ominous voice boomed, “Y2K – What if they’re wrong?”

Despite its questionable entertainment value, I think the movie is the one that will actually have it all wrong.

One of the most effective methods, however, to survive the movie's hype and to calm any fears that may result is for federal agencies to have effective contingency plans and Day One strategies that provide all Americans adequate assurances our federal government will not be adversely affected by Y2K.

Recently, the Office of Management and Budget (OMB) provided guidance to assist Federal agencies in preparing "Day One" plans.

These plans are prepared for finite timeframes, like the end of December through early January, to help mitigate any problems that may arise.

They should address the full scope of agency activity that will be underway during that period.

For example, agencies must prepare to mitigate the impact of possible failures in internal systems, buildings, or other infrastructure.

Furthermore, the plan should include agency efforts to assess the Y2K impact on its business partners, such as State and local governments, in delivering Federal programs.

I am pleased to welcome representatives of a number of federal agencies to discuss and review the status of their contingency plans and Day One strategies and I look forward to the testimony from the Social Security Administration, the Department of Defense, the Department of Energy, the Internal Revenue Service, and the Postal Service.

Mrs. MORELLA. And it's now my pleasure to recognize the ranking member on the Subcommittee on Government Management, Information, and Technology, the gentleman from Texas Mr. Turner.

Mr. TURNER. Thank you, Madam Chairman. I want to commend you and Chairman Horn, the chairman of my subcommittee, for your diligence in trying to be sure that we are ready in the Federal Government for January 1, 2000.

We all know that the public faces some risk that critical services provided by both the government and the private sector may be disrupted by the Y2K computer problem. And as we get closer to January 1st, we need to redouble our efforts to be sure that any disruption is reduced to a minimum.

Because this is the first time we've ever dealt with a problem of this nature and magnitude, I'm sure that we should expect the unexpected. And for that reason, we've asked every Federal agency to have in place a business continuity and contingency plan, and a day 1 strategy to reduce the risk of failures occurring in their systems, programs, and services.

Without such plans, when unpredicted failures occur, agencies would not be able to have a well-defined response, nor have adequate time to remedy whatever problem may arise. So I'm confident that the review of the agencies' efforts today will be productive. I think if the Federal Government reaches January 1st, 2000, without significant disruptions, a large part of that credit will be due to the work of these two subcommittees that for many months now have diligently worked to be sure that the Federal Government is prepared and ready.

Thank you, Madam Chairman. I look forward to hearing the testimony today.

Mrs. MORELLA. Thank you very much, Mr. Turner. And I appreciate your being here, too.

[The prepared statement of Hon. Jim Turner follows:]

STATEMENT OF THE HONORABLE JIM TURNER
GMIT HEARING ON "Y2K AND CONTINGENCY PLANNING"
10/28/99

Thank you. The public faces the risk that critical services provided by the government and the private sector could be disrupted by the Y2K computer problem. As each day draws us closer to January 1, 2000, we need to redouble our efforts to ensure that the federal government is Y2K compliant. Because this is the first time we encountered a problem of this nature and magnitude, we should expect the unexpected. I think we should also invoke Murphy's Law and anticipate that "Everything that can go wrong, will go wrong."

Therefore, each federal agency must have in place a Business Continuity and Contingency Plan and Day One strategy for reducing the risk of failures occurring in its facilities, systems, programs, and services during the weekend of the Y2K rollover. Without such plans, when unpredicted failure occurs, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Such strategies should focus on actions to be taken shortly before, during, and after the rollover. Because each agency is different, there is no single approach to BCCP and Day One planning.

Both the Office of Management and Budget (OMB) and the General Accounting Office have provided guidance plans to assist federal agencies in preparing for their BCCPs and Day One Plans. These plans provide a conceptual framework for helping agencies develop strategies and plans to reduce the risk of an adverse Y2K impact on their operations. The Day One guidance draws on the Day One plan of the Social Security Administration, which is viewed as a model plan.

We have a cross section of witnesses to inform us how the federal agencies are preparing their BCCPs and Day One Plans. The risk to government operations due to a Y2K disruption can be mitigated by the development of an effective BCCP and Day One strategy. This type of planning represents the best insurance policy we have against a Y2K disaster, and I commend the Chairman for his focus on this issue.

Mrs. MORELLA. There's recognition that Congress on the House side is not in session today; therefore, a number of the members of the subcommittees will be reading the testimony and discussing it upon their return.

It's now my pleasure to recognize for an opening statement Mr. Davis, who is the chairman of one of the subcommittees of Government Reform, the District of Columbia Subcommittee, and is a member of the Subcommittee on Government Management, Information, and Technology.

Mr. DAVIS. Thank you very much.

This is the 23rd hearing of the year on the year 2000 computer problem that this subcommittee has held during the first session of the 106th Congress. Over the last 3 years, the subcommittees have spent countless hours discussing mission-critical systems and embedded chips. Federal departments and agencies have spent far more hours attempting to fix these potential problems.

Most recently we have looked at the Federal programs, such as Medicare and Medicaid, that affect millions of the Nation's most vulnerable citizens, the elderly, the impoverished and the sick. But now with only 63 days remaining until the January 1st deadline, it's time to talk about the contingencies, the what-ifs.

What if, despite the best efforts, some computers fail? What if they continue working but spew out erroneous data? How prepared are Federal departments and agencies to cope with these possible situations? What are their plans? What are their plans for day 1, the critical days leading up to midnight January 1st and the days immediately afterwards?

I'm concerned to hear that the Internal Revenue Service has found some unsolved problems with its inventory. Could other Federal agencies find similar discrepancies? Just, frankly, the IRS under their leadership at this point, I think, is one of the most progressive in terms of dealing with the computers and the like. The head of the IRS comes out of that industry.

Clearly, we need to have a candid discussion on contingency plans today. We need to ensure that the Federal Government and the services it provides will not fail, whether the date is December 31st, 1999, or January 1st, 2000.

Thank you.

Mrs. MORELLA. Thank you, Mr. Davis.

[The prepared statement of Hon. Thomas M. Davis follows:]

**Opening Statement
Rep. Tom Davis, R-VA
House Subcommittee on Government Management,
Information, and Technology**

This is the 23rd hearing on the Year 2000 computer problem that we have held during this first session of the 106th Congress.

Over the last three years, the subcommittees have spent countless hours discussing mission-critical systems and embedded chips. Federal departments and agencies have spent far more hours attempting to fix these potential problems.

Most recently, we have looked at Federal programs such as Medicare and Medicaid, programs that affect millions of the nation's most vulnerable citizens —the elderly, the impoverished, and the sick. But now, with only 63 days remaining until the January 1st deadline, it is time to talk about the contingencies — the "what ifs."

What if, despite best efforts, computers fail? What if they continue working, but spew out erroneous data? How prepared are Federal departments and agencies to cope with these possible situations? What are their plans? What are their plans for "Day One" —the critical days leading up to midnight, January 1st, and the days immediately afterward?

I am concerned to hear that the Internal Revenue Service has found some unresolved problems with its inventory. Could other Federal agencies find similar discrepancies?

Clearly, we need to have a candid discussion on contingency plans today. We need to ensure that the Federal Government and the services it provides will not fail — whether the date is December 31, 1999, or January 1, 2000.

Mrs. MORELLA. And now as we usually do, we will swear in our witnesses, and on the first panel, Mr. Willemssen and Mr. Spotila.
[Witnesses sworn.]

Mrs. MORELLA. The record will show that the panelists have sworn to tell the truth.

And now, as is, again, our tradition, we will give you each about 5 minutes, approximately, to give your testimony, knowing full well that your entire testimony will be included verbatim in the record.

And so we will start now, as usual, with Mr. Willemssen. I don't know how many hearings you've been at, sir, but you really have been stalwart. We feel that you're part of the committee. Thank you, Mr. Willemssen.

STATEMENTS OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE; AND JOHN SPOTILA, ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Mr. WILLEMSSEN. Thank you, Chairwoman Morella, Ranking Member Turner, Congressman Davis. Thank you for inviting GAO to testify today on Y2K business continuity and contingency planning and day 1 planning.

As requested, I will briefly summarize our statement. We've previously testified on the importance of Y2K business continuity and contingency planning. No one knows exactly for sure what the roll-over period will bring, and, therefore, such planning is essential to helping ensure continued agency operations in the event that disruptions occur.

Over time we've seen major improvements in the Federal agencies' efforts in business continuity and contingency planning. For example, in early 1998, we testified that several agencies reported that they plan to develop contingency plans only if they fell behind schedule in completing their Y2K work. By contrast, less than a year later, in January 1999, we testified that many agencies had reported that they had either completed or had drafted contingency plans. These improvements continue. For example, we reviewed agencies' most recent submissions to OMB of updated continuity and contingency plans and found that all agencies had identified key business processes as called for in our guidance. A key aspect of business continuity and contingency planning is validating or testing plans. It's one thing to develop a written plan, but quite another to see whether the plan will actually work as envisioned. That's why we've emphasized the need for testing of contingency plans.

In reviewing the high-level plans submitted to OMB, we were able to identify 20 agencies that discussed their validation strategies. These strategies encompassed a range of activities, including desktop exercises and simulations. In addition to reviewing these high-level plans, we've previously reported on the business continuity and contingency planning of agencies and their components, and we found some uneven progress. For example, we found some agencies have instituted key processes, while other agencies still have a ways to go.

Another important element of business continuity and contingency planning that has not yet been adequately addressed is the potential cost of implementing plans. Our guide calls on agencies to assess the costs and benefits of identified alternative contingency strategies. We also testified in June that OMB's assessment of agency plans should consider whether agencies provided estimated costs, and, if not, OMB should require that this information be submitted so that it is available on a governmentwide basis. However, OMB has not yet required agencies to provide these cost estimates, although we did identify five agencies which did so in their submissions.

Regarding day 1 planning, earlier this month we did issue a guide to assist agencies in implementing their strategies. Briefly the objectives of a day 1 strategy are to, one, position the organization to readily identify year 2000 induced problems, take needed corrective actions, and minimize adverse impact on agency operations and key business processes. And second, it's very important that the organization be in a position to provide information on their Y2K condition to their top executives, other business partners and to the public. Our guidance provides a conceptual framework for helping agencies address those objectives.

For the day 1 plans that were due on October 15th, OMB asked agencies to address seven key elements, elements such as a schedule of activities, contractor availability, communications with the work force, and communications with the public. A review of the submissions found that about 40 percent of the agencies addressed all required elements.

Another important part of day 1 planning is ensuring that the day 1 strategy can actually be executed; therefore, day 1 plans and their key processes and timetables should be reviewed and, if feasible, rehearsed. Our review of day 1 plans found that 19 agencies discussed rehearsing their strategies, although some did not provide specific dates of their planned or completed rehearsals.

That completes a summary of my statement. And I would be pleased to address any questions you may have. Thank you.

Mrs. MORELLA. Thank you Mr. Willemssen.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10 a.m. EDT
Friday,
October 29, 1999

YEAR 2000 COMPUTING CHALLENGE

Federal Business Continuity and Contingency Plans and Day One Strategies

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



GAO/T-AIMD-00-40

Mr. Chairman, Ms. Chairwoman, and Members of the Subcommittees:

Thank you for inviting us to participate in today's hearing on the status of agencies' business continuity and contingency plans and Day One strategies. The public faces the risk that critical services provided by the government and the private sector could be disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors.

The risk to government operations due to these many potential points of failure can be mitigated by the development of effective business continuity and contingency plans. In addition, Day One strategies—developed either as part of business continuity and contingency plans or separately—can help agencies manage the risks of the rollover period during late December 1999 and early January 2000.

As requested, after a brief background discussion, today I will (1) discuss the state of the government's business continuity and contingency planning and (2) describe the status of Day One strategies.

BACKGROUND

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.¹ We have also issued guidance to help organizations successfully address the issue.² Two of our publications—on business continuity and contingency planning and on Day One planning and operations—provide guidance on the subject of this hearing.

Our business continuity and contingency guide describes the tasks needed to ensure the continuity of agency operations in the event of Year 2000-induced disruptions. The Day One guide provides a conceptual framework for developing a Day One strategy and reducing the risk of adverse year 2000 impact on agency operations during late December 1999 and early January 2000.

Business continuity and contingency plans are essential. Without such plans, when failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their

¹High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

²Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997); Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998); Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998); and Year 2000 Computing Challenge: Day One Planning and Operations Guide (GAO/AIMD-10.1.22, issued as a discussion draft in September 1999 and in final form in October 1999).

business partners as well as on services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Accordingly, in April 1998 we recommended that the President's Council on Year 2000 Conversion require agencies to develop contingency plans for all critical core business processes.³

Since 1998, the federal government has improved its approach to business continuity and contingency planning. The Office of Management and Budget (OMB) has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide for federal use. In addition, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13, OMB required agencies to submit high-level versions of these plans by June 15.

As noted in our business continuity and contingency planning guide, a key element of such a plan is the development of a zero day or Day One risk reduction strategy. In testimony on January 20, 1999, we noted that the Social Security Administration had

³Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

developed a Day One strategy and suggested that OMB consider requiring other agencies to develop such a plan.⁴ In its September 1999 quarterly report, OMB subsequently required agencies to submit Day One strategies to OMB by October 15, 1999 as well as updated high-level business continuity and contingency plans.

WHILE WORK REMAINS, AGENCY
BUSINESS CONTINUITY AND CONTINGENCY
PLANNING HAS IMPROVED

Although more work remains, agency business continuity and contingency planning has evolved and improved since 1998. In March 1998 we testified that several agencies reported that they planned to develop contingency plans only if they fell behind schedule in completing their Year 2000 fixes.⁵ In June 1998, we testified that only four agencies had reported that they had drafted contingency plans for their core business functions.⁶ By contrast, in January 1999 we testified that many agencies had reported that they had completed or were drafting business continuity and contingency plans while others were in the early stages of such planning.⁷ Finally, as we testified in August, according to an OMB official, all of the major departments and agencies had submitted high-level business continuity and contingency plans in response to OMB's May 13, 1999

⁴Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD 99-50, January 20, 1999).

⁵Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998).

⁶Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998).

⁷GAO/T-AIMD-99-50, January 20, 1999.

memorandum.⁸

With respect to OMB's latest request for high-level plans, the 24 major departments and agencies and the U.S. Postal Service⁹ have submitted updated business continuity and contingency plans. However, while the Department of the Treasury and the General Services Administration reported that they had provided their plans to OMB, we did not receive these plans in time to include them in our analysis and, therefore, we analyzed 23 submissions.

While OMB's May 1999 memorandum directed agencies to describe their overall strategies and processes for ensuring the readiness of key programs and functions across the agency, it did not detail the format or reporting elements that the agencies were to follow. Accordingly, the plans vary considerably in terms of format and level of detail. Some agencies, such as the Departments of Justice and Labor described their general approach or strategy while others, such as the Departments of Education and Transportation, provided program or component agency specific plans that contained more detailed information. As an example of the first type of plan, the Social Security Administration's high-level plan identified broad areas of risk and general mitigation strategies and contingencies. However, as we testified in July,¹⁰ the Social Security Administration has also completed local contingency plans to support its core business

⁸Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-266, August 13, 1999).

⁹With respect to our analysis of high-level plans and the Day One Strategies, the term agencies will hereafter include the Postal Service.

¹⁰Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999).

operations, and has obtained contingency plans for all state disability determination services as well as developed, in conjunction with the Department of the Treasury and the Federal Reserve, a Benefits Payment Delivery Y2K Contingency Plan. In contrast, the Department of Education provided OMB with its detailed contingency plans for its core business processes and their supporting systems.

In their high-level plans, some agencies provided details of the types of contingencies that could be implemented in the event of a Year 2000-induced failure. For example,

- The Social Security Administration described the risk that its field offices would be unable to issue certain types of payments due to Year 2000-related problems with automated support. In this event, the Social Security Administration stated that it would coordinate with the Department of the Treasury to address the problem. Further, in the event that it is known by December 1999 that enterprises such as local banks and/or the Postal Service were not ready to make delivery of payments in early January, the Social Security Administration stated that it would consider plans to issue payments early.
- The Department of Education described the risk of a registration system failure at a school that prevents it from determining the title IV (student financial aid)¹¹ eligibility of its students. Education's risk mitigation/contingency activity if this occurs is threefold. First, Education stated that it will encourage schools to take steps to obtain

¹¹Title IV of the Higher Education Act of 1965, as amended.

registration and pre-registration information before January 2000 for students beginning or continuing classes after January 1. Second, Education stated that it will encourage schools to develop other processes, including manual processes, for determining the enrollment status and eligibility of students who begin classes after January 1, 2000. Third, for students enrolled or pre-registered in fall 1999 classes, Education will allow schools to package aid and credit students' accounts using fall 1999 enrollment or pre-registration information, but not to disburse funds directly to students or parents. After the system is repaired, funds will have to be returned for any student who was ineligible. To implement these contingencies, Education stated that it would not enforce certain requirements and provided directions that a school is to follow (e.g., if a school makes a short-term loan to a student in lieu of paying a credit balance, the school may not charge the student interest on that loan).

- The Department of Veterans Affairs' Veterans Health Administration's contingency planning guidebook provides sample templates to be used as guides or models by its health care facilities. For example, to prepare for the potential problem that a facility would be unable to provide water in its inpatient wards for patients' needs and staff infection control, the facility could prepare locations for bottled water and stock waterless soaps. In the event that a failure actually occurred and action was needed, an assessment of the situation could be reported to a facility's command center, and bottled water centers established with control mechanisms.

All of the high level plans in our review identified core business processes, as called for

in our guide. For example, the Department of Labor identified and described seven core business functions: (1) benefits programs, (2) national employment and/or economic conditions tracking, (3) job training programs and employment assistance, (4) workers' benefits, (5) worker safety and health policy and oversight, (6) labor and employment policy and oversight, and (7) program support.

A key aspect of business continuity and contingency planning is validation, which evaluates whether individual contingency plans are capable of providing the needed level of support to the agency's core business processes and whether the plan can be implemented within a specified period of time. In instances in which a full-scale test may not be feasible, the agency may consider end-to-end testing of key plan components. Moreover, an independent review of the plan can validate the soundness of the proposed contingency strategy. We were able to identify 20 agencies that discussed their validation strategies in their high-level plan. These strategies encompassed a range of activities, including reviews, desktop exercises, simulations, and/or quality assurance audits.

In addition to reviewing high-level plans, we have assessed and reported on the business continuity and contingency planning of several agencies or their component entities and have found uneven progress. Some had instituted key processes while others had not completed key tasks. For example:

- As we reported on October 22, the Department of Justice's Federal Bureau of

Investigation had made progress in its Year 2000 business continuity planning.¹² However, because Justice had not explicitly required and emphasized the importance of business continuity plans, the Bureau had started late in undertaking its planning effort and was faced with a compressed time frame for testing and finalizing its plans. In addition, as of August 1999, the Bureau did not have many of the management controls and processes needed to effectively guide its planning activities. For example, the Bureau had not (1) developed a master schedule and milestones, (2) defined all of its core business processes, (3) assessed the costs and benefits of alternative continuity strategies, or (4) planned for the testing phase of its business continuity planning effort. We recommended improvements to the Federal Bureau of Investigation's planning activities, including that it establish and implement effective controls and structures for managing its business continuity planning. In commenting on our report, Justice indicated that it and the Bureau had taken the first steps in implementing our recommendations.

- In testimony last week we stated that, because of deficiencies in their contingency plans, the Department of State and the U.S. Agency for International Development lacked assurance that they could sustain their worldwide operations and facilities into the next century.¹³ For example, State's business continuity and contingency plan did not identify and link its core business processes to its Year 2000 contingency plans and procedures, and the department had not yet tested its plans with Year 2000-

¹²Year 2000 Computing Challenge: FBI Needs to Complete Business Continuity Plans (GAO/AIMD-00-11, October 22, 1999).

¹³Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning (GAO/T-AIMD-00-25, October 21, 1999).

specific scenarios. In the case of the U.S. Agency for International Development, we found that it had identified one core business process in its business continuity and contingency plan but did not identify or address other key agency functions. Moreover, the U.S. Agency for International Development provided little information on contingency planning activities for its missions, and it was unclear when the agency expected to complete its business continuity and contingency planning process.

- As we reported on October 14, the Department of Justice's Drug Enforcement Administration had managed its business continuity planning efforts in accordance with the structures and processes recommended by our guide, and had made progress toward completing its plans.¹⁴ However, while progress had been made, the Drug Enforcement Administration still had many tasks to complete, with little time to address schedule slippages. For example, at the time of our review, it had not validated its business continuity strategy; defined, documented, or reviewed test plans; or prepared test schedules and test scenarios. The agency planned to complete testing of its plans by the end of November.
- The Internal Revenue Service's business continuity and contingency plans that addressed issuing refunds and receiving paper submissions were inconsistent in two key areas—performance goals and mitigating actions—as we reported in September.¹⁵ This raised questions about whether these two plans provided sufficient assurance that

¹⁴Year 2000 Computing Challenge: DEA Has Developed Plans and Established Controls for Business Continuity Planning (GAO/AIMD-00-8, October 14, 1999).

¹⁵IRS' Year 2000 Efforts: Actions Are Under Way to Help Ensure That Contingency Plans Are Complete and Consistent (GAO/GGD-99-176, September 14, 1999).

the Internal Revenue Service had taken all necessary steps to reduce the impact of a potential Year 2000 failure. For example, neither of the plans specified completion dates for the mitigating actions nor did the plans specify which individuals would be responsible for completing those actions. In response to our concerns, Internal Revenue Service officials agreed to make changes to these two plans and to review other business continuity and contingency plans for consistency and accuracy.

Business continuity and contingency plans are also key to ensuring that the government's highest priority programs are not adversely affected by the Year 2000 problem. In the case of some of the government's essential programs, not only is it important that the federal government have effective plans but their partners (such as states) must also have such plans in order to ensure program continuity. Accordingly, in its March 26, 1999, memorandum designating the government's 42 high-impact programs, such as food stamps (OMB later added a 43rd high-impact program), each program's lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work.

Our reviews have shown that some high-impact programs are farther along than others with respect to business continuity and contingency planning. For example:

- Yesterday we testified on the contingency planning progress of the Department of Veterans Affairs' two high-impact programs, benefits and health care.¹⁶ The Veterans Benefits Administration's regional offices and Veterans Health Administration's medical facilities have completed their business continuity and contingency plans but testing is incomplete. Only five of 58 Veterans Benefits Administration' regional offices had completed testing of their business continuity and contingency plans (all are now required to complete testing by November 15). In addition, while all of the Veterans Health Administration's medical facilities completed emergency power drills, other portions of their plans, such as the possibility of water and gas shortages, have not been tested.
- On October 6, we testified on the readiness status of the 10 high-impact state-administered federal programs, including the business continuity and contingency plans being developed by the states for these programs.¹⁷ With respect to the three such programs overseen by the Department of Agriculture's Food and Nutrition Service (e.g., food stamps), it was unclear whether all states had adequate plans to ensure the continuity of these programs. Indeed, as of September 15, Food and Nutrition Service officials told us that only two states had submitted suitable

¹⁶Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs (GAO/T-AIMD-00-39, October, 28, 1999).

¹⁷Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs (GAO/T-AIMD-00-9, October 6, 1999).

contingency plans.

In the case of the Department of Health and Human Services' Health Care Financing Administration's (HCFA) Medicaid program, of the 33 states and two territories that had been reviewed by a business continuity and contingency plan contractor, 11 were high risk, 11 were medium risk, and 13 were low risk. Regarding the five high-impact programs of the department's Administration for Children and Families administered by the states (e.g., Temporary Assistance for Needy Families), business continuity and contingency planning was one of the most common areas of concern cited in 19 state assessment reports available as of September 27, 1999.

With respect to the Department of Labor's Unemployment Insurance program, a contractor rated states' business continuity and contingency plans from low to high in terms of their compliance with Labor's requirements for coverage of core business functions of benefits and tax systems. Based on the contractor's completed reviews, the quality of state plans varied widely. For example, according to Labor's contractor, (1) 23 benefits and 14 tax plans had a low/very low degree of compliance with Labor's requirements, and (2) 9 benefits and 5 tax plans had a high degree of compliance with Labor's requirements.

- In September, we reported that the Department of Agriculture's Food Safety Inspection Service had not established milestones for completing complementary business continuity and contingency planning with its partners for its food safety

inspection high impact program. The food safety high-impact program's partners include 25 states with approval to operate their own inspection programs.¹⁸

- As we testified on September 27, HCFA continued to make steady progress on its agencywide and 29 internal business continuity and contingency plans for its high-impact Medicare program, but the status of contractor plans was unknown and the results of HCFA's reviews of managed care organizations' plans were not promising.¹⁹ With respect to its internal plans, HCFA had completed an agencywide business continuity and contingency plan but essential validation activities remained. Regarding the Medicare contractors plans, HCFA's contractor and our review both found that not all Medicare contractors have specified detailed procedures that are required for executing and testing their business continuity and contingency plans. In the case of the managed care organizations, as of September 2, 1999, HCFA had received plans from 310 of the 383 managed care organizations. Its review of these 310 plans concluded that 69 percent needed major improvement, 18 percent needed minor improvement, and 13 percent were reasonable.

Mr. Chairman, on October 26, 1999, we briefed your Subcommittee staff on the results of our review of 11 high-impact programs, performed at your request. We found mixed progress on the business continuity and contingency planning for these programs. For example, the Defense Finance and Accounting Service reported completing the

¹⁸Year 2000 Computing Challenge: Readiness of USDA High-Impact Programs Improving, But More Action Is Needed (GAO/AIMD-99-284, September 30, 1999).

¹⁹Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues (GAO/T-AIMD-99-299, September 27, 1999).

development and testing of its business continuity plan for military retiree and annuity pay while the Immigration and Naturalization Service had not completed or tested the business continuity plan for its immigration program. In other cases, such as the Postal Service's mail delivery program, the business continuity plans had been prepared but testing was not completed.

One key aspect of business continuity and contingency planning that has not been adequately addressed is the potential cost of implementing plans. Our business continuity and contingency planning guide calls on agencies to assess the costs and benefits of identified alternative contingency strategies. Accordingly, we testified in June that OMB's assessment of agencies' high-level plans should consider whether agencies provided estimated business continuity and contingency plan costs and, if not, OMB should require that this information be provided expeditiously so that it can give the Congress information on potential future funding needs.²⁰

OMB has not required agencies to provide estimates of their business continuity and contingency plans. Nevertheless, in their August 1999 quarterly reports, we identified five agencies that specified estimated costs for some aspects of their business continuity and contingency plan development and/or implementation. For example, the Department of Health and Human Services estimated that it would cost about \$99 million to implement its business continuity and contingency plans and Day One strategies regardless of how the year 2000 affects its operations, but its estimate does not include

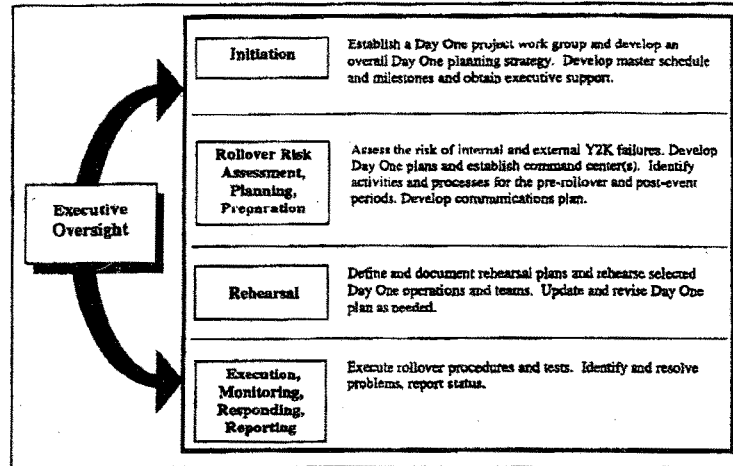
²⁰Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

the cost of invoking the business continuity and contingency plan. The Department of Education's quarterly report stated that, as of August 13, 1999, its business continuity and contingency plan preparation costs were estimated at \$3.2 million, and estimated that it would cost \$7.5 million in the event that all of the plans had to be implemented (which it believed to be of very low probability).

DAY ONE PLANNING IS ONGOING

Day One strategies are necessary to reduce the risk to facilities, systems, programs, and services during the weekend of the critical rollover period. Accordingly, such strategies describe a wide range of complex, interrelated activities and geographically distributed processes that must be executed shortly before, during, and after the rollover. Earlier this month we issued a Day One strategy guide.²¹ As shown in figure 1, the guide addresses four phases supported by executive oversight: (1) initiation; (2) rollover risk assessment, planning, and preparation; (3) rehearsal; and (4) execution, monitoring, responding, and reporting.

²¹GAO/AIMD-10.1.22, October 1999.

Figure 1: Year 2000 Day One Planning and Operations Structure

In its September 1999 quarterly report, OMB required agencies to submit Day One strategies by October 15. OMB subsequently asked agencies to address seven elements in their plans: (1) a schedule of activities, (2) personnel on call or on duty, (3) contractor availability, (4) communications with the workforce, (5) facilities and services to support the workforce, (6) security, and (7) communications with the public. OMB also told the agencies to consider our Day One strategy guidance carefully. All agencies have submitted such draft or final strategies to OMB (either as part of their business continuity and contingency plan or as a separate document). However, while the U.S. Agency for International Development and the General Services Administration reported that they

had provided their plans to OMB, we did not receive these plans in time to include them in our analysis. Therefore, we analyzed 23 agencies' submissions.

Our review of the agency strategies found that about 40 percent (9 of 23) addressed all seven elements. For example, in our testimony yesterday we noted that the Department of Veterans Affairs addressed all of OMB's elements.²² This department and its agencies had developed a Day One strategy that should help the department manage risks associated with the rollover period and better position itself to address any disruptions that may occur. For example, the strategy included a timeline of events between December 31 and January 1 and a personnel strategy and leave policy that identifies key managerial and technical personnel available to support day one operations.

With respect to specific elements, we were able to identify 15 agencies that included a schedule of activities and 17 that addressed staffing issues. Also, in a few cases, agencies addressed either OMB's internal communications element or external communication element but not both. Further, some elements were addressed in a general manner and/or indicated that more work needed to be completed. For example, one agency reported that it is developing procedures to ensure its ability to identify, report, and respond effectively to Year-2000 related events.

²²GAO/T-AIMD-00-39, October 28, 1999.

An important part of Day One planning is ensuring that the Day One strategy is executable. Accordingly, the Day One plans and their key processes and timetables should be reviewed and, if feasible, rehearsed. Our Day One strategy review found that 19 agencies discussed rehearsing their strategies, although some did not provide specific dates of planned or completed rehearsals.

In summary, business continuity and contingency plans and Day One strategies are key to managing and reducing the risks associated with the change to the year 2000. In the area of business continuity and contingency planning, noteworthy progress has been made since early 1998, although more work remains. With respect to Day One strategies, while about 40 percent of agencies addressed all of OMB's elements in their submissions, it is clear that much more work remains.

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

Contact and Acknowledgments

For information about this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at willemssen.aimd@gao.gov. Individuals making key contributions to this testimony included Margaret Davis, Mirko Dolak, Jim Houtz, and Linda Lambert.

(511781)

Mrs. MORELLA. We now look forward to hearing from Mr. Spotila.

Mr. SPOTILA. Good morning, Chairwoman Morella and Congressman Turner and Congressman Davis. Let me start by thanking you for your continuing interest in the Y2K problem. As I indicated to you in my testimony on October 6th, your early and continued involvement in this issue has made a dramatic difference in the Federal Government's preparedness.

Before discussing our day 1 planning efforts, let me update you on the status of our other work. As of October, the agencies report that 99 percent of Federal mission-critical systems are compliant, an increase from the 98 percent that I reported earlier this month.

This reflects notice from five more departments; Agriculture, Commerce, Energy, Health and Human Services and Transportation, that their critical systems are ready. Although a small number of critical systems are still not quite done, in all cases the agencies involved have assured us that they will complete their work before the end of the year. Moreover, they all have contingency plans in place for these systems. Compared to where we were just last year, this is a huge accomplishment.

Even though we expect all of our mission-critical systems to be ready by January 1st, it is still important that every agency have a business continuity and contingency plan, or BCCP, in place, including a detailed day 1 plan. These plans describe the steps each agency will take to prepare for the 1st of January. They should address the full scope of agency activity with steps to mitigate the impact of any failures involving internal systems, buildings or other infrastructure.

Agencies must be ready to assess the impact of any Y2K problem on their partners and constituencies and to provide them with appropriate assistance. They must also be ready to provide information about any Y2K problem to their management partners and the public.

As GAO's day 1 guidance notes, effective day 1 planning will position an agency to identify year 2000 induced problems, take corrective action and minimize adverse impact on agency operations and key business processes. We are working closely with the agencies and GAO to share information about how best to develop effective plans. GAO and OMB have issued coordinated guidance to the agencies.

My staff has reviewed agency plans and is working with agencies to improve those plans. We are all learning as we go. The work we are asking agencies to do has never been done before. In an organization as large and diversified as the Federal Government, there is no one-size-fits-all solution, and given this challenge, the agencies have responded well.

Based on our initial review of agency plans, we believe most large agencies are on track. While they need to add more detail to the plans, most do address all of the critical elements of effective day 1 planning. A few of the larger agencies have had more difficulty. Here we have engaged them at a senior level to ensure that their efforts improve. I have already spoken personally with several agencies to see that their plans are revised to address our concerns.

OMB staff are following up these discussions with each agency individually. While a few of the small and independent agencies have done excellent work, a number of them have provided incomplete plans or none at all. To help speed their work, we are meeting with them next week. We will have one or two of the agencies that provided excellent plans describe what the plans should entail. I note that GAO has agreed to participate in that meeting as well. Their work has been invaluable to agency progress in this area.

After further work with the agencies, we will ask them to provide us with revised plans next month. From our review of the existing day 1 plans, we are beginning to see some patterns of best practices. The importance of good communications cannot be underestimated. If unforeseen problems arise, agencies must be able to communicate with their work force, their partners and the public.

Assuring the ability to communicate is so important that a redundant communications capability should be put into place. The best plans provide a detailed schedule of activities that will take place during the rollover period. They anticipate the sequence and timing of such activities as shutting down computer systems and bringing them back up, checking their viability and contacting key business partners.

The best plans ensure that the right personnel will be available at the right time, whether on duty or on call and whether on or offsite. Such personnel may be contractors or employees and may include building technicians, computer programmers, telecommunications experts, program staff, contracting officers, legal counsel, public affairs staff and senior management.

Finally, we are aware that the Y2K transition is an opportunity for those who might want to disrupt agency activity, whether mischiefmakers or those with criminal intent. The best plans describe additional steps to guard against such security risks, whether to facilities, personnel or systems.

We are all on a learning curve here. As we identify other best practices, we will share them across agencies. Such cooperation will continue to be essential to our success in preparing for Y2K. We are entering the home stretch of our year 2000 efforts. As in any race, it is time to begin sprinting toward the finish. Day 1 plans are the critical last piece of our preparations. There will be no letup in our efforts during the remaining 63 days.

Thank you for the opportunity to continue to share information with you on the administration's progress. I would be pleased to answer any questions you may have.

Mrs. MORELLA. Thank you, Mr. Spotila.

[The prepared statement of Mr. Spotila follows:]



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF
JOHN T. SPOTILA
ADMINISTRATOR.
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE
THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
OF THE COMMITTEE ON GOVERNMENT REFORM
AND BEFORE
THE SUBCOMMITTEE ON TECHNOLOGY
OF THE COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

October 29, 1999

Good morning, Chairman Horn, Chairwoman Morella, and members of the subcommittees. I am pleased to appear before you to discuss the Federal government's progress on developing business continuity and contingency plans (BCCPs) and day one plans. I would like to start by thanking you and all of the members of the subcommittees for your continuing interest in the Y2K problem. Your early and continued interest in this issue has made a dramatic difference in the Federal government's preparedness.

Your letter of invitation indicated that today's hearing was about the readiness of the Federal government's business continuity and contingency plans and day one plans. As I discussed during my October 6 testimony before the Subcommittees, business continuity and contingency planning is one of our highest priorities during the remaining days before January.

Before discussing business continuity and contingency planning efforts in depth, let me briefly update you on the status of our work on making mission critical systems compliant. As of October, the Federal agencies report that 99% of Federal mission critical systems are compliant -- an increase from the 98% that I reported earlier this month. And during this month five more Departments: Agriculture, Commerce, Energy, Health and Human Services, and Transportation; reported that all of their mission critical systems are now compliant. Relative to where agencies were just last year, this is a remarkable accomplishment. While we are pleased with the continued progress, like you, we are concerned that not all mission critical systems are compliant yet. However, all of the agencies with mission critical systems that are not yet compliant have assured us that they will complete their work before the end of the year. Furthermore, as extra

insurance, they have contingency plans in place for all of those systems.

Efforts To Date

As I testified when I was here earlier this month, although we expect all Federal mission critical systems to be ready by January 1, 2000, it is still important that every agency, no matter how well prepared, have a business continuity and contingency plan in place. To assist the agencies in their planning efforts, we issued guidance on risks and assumptions that agencies should follow in developing their BCCPs, suggested that agencies follow GAO's guidance in developing their plans, and asked the agencies to submit their headquarters level plans for OMB review by June 15. OMB staff provided the agencies direct staff-level feedback on those plans during the summer. We summarized those plans in our September report to the Congress.

Day One Planning

In September, we began to work with the agencies government-wide on preparing their plans for the roll-over period, their day one plans. Day one plans are an essential part of a BCCP, as they describe the steps an agency will undertake during the pre-rollover and post-rollover periods. Day one plans should address the full scope of agency activity that will be underway during that period. That includes steps to mitigate the impact of possible failures in internal systems, buildings, or other infrastructure. It also includes steps to assess the impact of the problem on agency partners in delivering Federal programs and agency constituencies and to provide appropriate assistance to them. Finally, it includes steps to provide information about the impact of the problem to management, business partners, and the public. It is during the execution of a day one plan that triggers may be recognized that will cause other facets of an agency's BCCP or Continuity of Operations Plan (COOP) to come into play.

It is during the execution of the day one plan that an agency's ability to conduct business will be verified. In a real sense, execution of the day one plan is the beginning of the live testing of all of the work that has gone on before it in preparing for the Y2K problem. Day one plans are the lynchpin that ties facility, systems and, program preparation together with BCCP and COOP planning. As GAO's day one guidance notes, effective day one planning will position an agency to readily identify year 2000 induced problems, take corrective actions, and minimize adverse impact on the agency's operations and key business processes.

Because day one planning is of such importance, we began working closely with the agencies and GAO to share experiences and information about how best to facilitate the development and implementation of effective plans. GAO and OMB issued complementary guidance to assist the agencies in preparing their plans. We asked for copies of agency plans by October 15, and we are continuing to work with them to improve their plans. I have attached a copy of the OMB guidance to my statement.

At the inception of this effort, we anticipated preparing these plans would be a significant

challenge. All of us are on a learning curve concerning the development of these plans. The work we are asking agencies to do has never been done before. In addition, the effort is complicated by the fact that it must be done so quickly. And, in an organization as large and diversified as the Federal government, there is no one-size-fits-all solution. Given this challenge the agencies have, overall, responded well.

Based on our initial review of the agency plans, the majority of the large agencies are on-track in preparing their plans. While most need to develop more detail to fill-out the plans, their submissions show that they are or soon will be addressing all of the critical elements of effective day one planning. OMB staff will continue working with each agency individually, providing them feedback during the coming weeks to help them complete their efforts.

As one might expect, a few of the larger agencies are lagging behind. We have already begun engaging those agencies in a dialogue at policy levels to ensure that their efforts improve. In fact, I have already spoken personally with senior policy officials in several agencies, and I have received assurances that their plans will be revised to address our concerns. OMB staff are following-up my discussions and working with each of those agencies individually as well.

While a few of the small and independent agencies have provided excellent plans, a number of them have either not provided a plan or have provided incomplete plans. To help speed their work, we are arranging a meeting with them next week. Our plan is to have one or two of the agencies that provided excellent plans present their approach, then have an in-depth discussion with all of them on what their plans should entail. I should note that GAO has agreed to participate in that meeting as well. Their work has been invaluable to the progress of Federal agencies in developing effective BCCPs and now day one plans.

It is our intent to request that agencies provide us with revised plans next month.

Best Practices

As we have reviewed day one plans from the various agencies, we are beginning to see some patterns of best practices in preparing plans. Today I would like to mention four of those that are of particular importance.

Communications. The importance of good communications linkages cannot be underestimated. The essence of day one planning is to prepare for events, some of which are unpredictable. In order to respond, it will be essential that agencies be able to communicate with their workforce, with their business partners, with their particular constituencies, and potentially with the public at large. Assuring the ability to

communicate is of such importance that a redundant communications capability should be put into place.

Schedule of Events. The best plans provide a detailed schedule of activities that will take place during the roll-over period. These plans incorporate management decisions made in advance on the sequence and timing of such activities as shutting down buildings and computer systems and bringing them back-up, checking their viability, and contacting key business partners.

Personnel. The best plans also ensure that the right personnel will be available at the right time, whether on-duty or on-call and whether on- or off-site. Such personnel may be contractors or employees and may include building technicians, computer programmers, telecommunications experts, program staff, contracting officers, legal counsel, public affairs staff, and senior management.

Security. Aside from any risks directly related to Y2K, agencies are aware that the millennium transition is an opportunity for those who might want to disrupt agency activity, whether mischief-makers or those with criminal intent. The best plans indicate that agencies will be taking additional steps to guard against such security risks, whether to their facilities, their personnel, or to their systems.

As I noted earlier, we are all on a learning curve in preparing for the roll over. While I have identified these initial four best practices, others will become apparent as agencies continue developing and testing their plans – and we will share them across agencies. Such cooperation has been and will continue to be essential to our success in preparing for Y2K.

Conclusion

Thank you for the opportunity to continue to share information with you on the Administration's progress. We are entering the home stretch of our year 2000 efforts. As in any race, it is time to begin sprinting toward the finish. Day one plans are the last piece of our preparations – and a critical piece since they are how all of the other pieces come together. I can assure you that there will be no let-up in our efforts during the remaining 63 days.

I would be pleased to answer any questions you may have.

Mrs. MORELLA. I am particularly pleased having both of you here, because you have been partners in trying to make sure that the Federal agencies, as well as the outreach and end-to-end testing, has been taking place.

As we start our questioning, I will start off with Mr. Willemssen. In your statement you mention several agencies at risk of not having solid, well-tested contingency plans, including the IRS, that will be testifying today, Federal Bureau of Investigations, Drug Enforcement Agency, Agency of International Development.

I would like to have you tell us what you see the real-life consequences of not having plans ready.

Mr. WILLEMSSEN. To the extent that agencies do not have contingency plans and continuity plans ready, and to the extent that those plans haven't been well tested, those agencies run the risk that in the event that disruptions occur, their responses to those disruptions will be more ad hoc and chaotic in nature, rather than very well planned with a clear roadmap on who is to do what and when, and who to report to who on what is going on.

That is the whole basis of having these plans in place and testing these plans. To the extent that that isn't there, we do run this risk of an untrained response that is a more ad hoc in nature, that may not be the right response, and, therefore, the response may not address the Y2K problem that may have occurred.

Mrs. MORELLA. So the planning is critically necessary even though that may not be the end either, there may be some other implications and consequences resulting from it, but far better than to have what could happen without those contingency plans.

You mentioned also in your statement the Y2K risk facing State-run programs—this concerns me greatly—like Medicaid and unemployment insurance. Again, what are the consequences of not having those plans ready?

Mr. WILLEMSSEN. The likely consequences in those kinds of benefit-driven programs is that, in the event that there are Y2K disruptions and contingency plans aren't ready to be implemented, benefits could be delayed or benefit amounts could be inaccurate. And, therefore, it's critically important that the contingency plans be pursued and be tested.

I'm more optimistic actually in this area now because of some of the fine efforts of the lead Federal agencies in understanding that this is a critical issue, and States are beginning—even those States that were lagging behind—are beginning to address this very forcefully. So I think there's reason for much more optimism, even compared to just a few weeks ago.

Mrs. MORELLA. Agencies should not be advising the public, should they, of possible consequences in terms of enlightening them?

Mr. WILLEMSSEN. I think agencies have to make a very reasoned decision on what they announce to the public and what they don't. As a side note, many of the business continuity and contingency plans and day 1 strategies do have some level of classification such as for official use only. One of the reasons for that relates to something you had mentioned early on. There's a possible security risk to the extent that agencies publish too much information about what they plan to do in the event of a Y2K disruption. So that's

something that I think agencies have to make a reasoned decision on.

I think the bottom line is making sure that plans are in place, that they have been tested, and that all the agencies are poised during the rollover period to address any disruptions that may result.

Mrs. MORELLA. Thank you.

Mr. SPOTILA, according to OMB—and I very much appreciate your coming out with the requirement that by October 15th, the agencies have their day 1 plans and contingency plans in effect. But according to OMB, day 1 plans should include specific data such as personnel that should be on call or on duty. And I wonder, what do you believe will be the number of Federal employees that will be on call or on duty, as the statement designates, on January 1st, 2000?

I guess what I'm asking you is, how does this compare, January 1st, 2000, with a regular day for the Federal Government?

Mr. SPOTILA. We don't yet have a specific number of people that we anticipate will be on duty in this effort. One of the general comments that I made in my testimony concerning the day 1 plans was that a number of the agencies need to supply more detail than they have. To some degree this is a process where we think we will get more specific information very quickly in the weeks to come.

Certainly not everyone will be working. We anticipate in each case that core staffs will be available, targeted much more at the specific needs of agencies on an individual basis. Some of those needs relate to verifying that the systems are going to work, bringing them down, bringing them back up again. Some of them involve response capability. In some cases, there will be people on call who will not physically be onsite as the rollover occurs.

We will have better information as we get closer to the end of the year in this regard, but we don't quite have it yet.

Mrs. MORELLA. But obviously there will be a tremendous number of people who will be ready who will be on call, as you say—

Mr. SPOTILA. That's true.

Mrs. MORELLA [continuing]. Ready to respond? It would be interesting as you continue on in the remaining couple of months to keep us apprised of that, too.

And one final question, before I turn to Mr. Turner for his line of questioning, is that Mr. Willemsen mentioned something that I think you would agree with, and that is that we don't really have the cost estimates of what implementation is going to cost. And I'm curious about what you're going to do to require it.

I don't think you've required it at this point, cost estimates. And I think they should be something that we should be able to scrutinize.

Mr. SPOTILA. We have had discussions with the agencies on this subject. Our sense has been that the most important focus for the agencies right now should be getting their plans, their detailed plans, ready so that we know what it is they're going to do or what they feel they will need to do.

From a costs standpoint, the agencies understand at the moment that they are expected to absorb these costs initially; they all have resources, we think, to do that. We made sure to tell them that if

any feel that budget considerations are interfering with their plans, they need to let us know, and we will make sure that resources are available.

We certainly will come back to the question of cost estimating, but we need to do it after the plans are ready in more detail so we know what it is that we are actually dealing with. It's not something we're insensitive to, but it is true we have not made this a priority equal to getting ready for the event itself.

Mrs. MORELLA. You might consider having at least some estimates submitted to scrutinize, because it was my understanding that it was in August 1999 when I think it was Department of Health and Human Services estimated that it would cost about \$99 to implement contingency and day 1 plan.

Mr. SPOTILA. I think that we will, in fact, ask for estimates. We've actually gotten some of them in already. We've encouraged agencies to give us estimates as they are ready to do so, and I think as we proceed closer to the end of the year, that is something we will be asking of them.

Mrs. MORELLA. Thank you.

I am now pleased to recognize Mr. Turner for his line of questioning.

Mr. TURNER. Thank you, Ms. Morella.

In my opening comments I made reference to the fact that we probably should all put ourself in the state of mind where we are ready to expect the unexpected. And one of the things that has concerned me, even after all of our efforts to prepare for Y2K it still seems to be very possible whether it's through efforts by those who would do harm to our country or simply from those who are on some college campus disseminating information over the Internet, that perhaps we could have on January 1st a lot of misinformation designed with ill intent or simply out of a spirit of being a prankster to try to mislead people and to cause people to take certain actions they might not otherwise take based on the information that that is disseminated.

I was wondering whether or not we have considered, or perhaps Mr. Koskinen in his efforts has considered creating some type of rapid response team that would act as a clearinghouse as we enter the new year to provide a source of credibility regarding misinformation or information that may circulate, whether it be over the Internet or through some other medium, about the existence or nonexistence of Y2K problems.

It seems to me that that type of panel would need to be people of some renown who bear credibility, perhaps a three-member panel of members who would be the spokespersons regarding Y2K problems. Madam Chairman, I know you get the same kind of e-mail I do. There's always some kind of rumor circulating on the Internet about something the government is about to pass or put a tax on the Internet or something like that, and we all end up writing these letters back saying that's just a rumor, there's no basis, there's no legislation pending on that subject.

It just strikes me that on January 1st, there's a possibility that some may try to circulate misinformation that might cause people to take actions that otherwise they would not take. If we had a panel in place of credible individuals through which all of that in-

formation could clear, then they could turn to the agencies and turn to the private sector to get the truth, and then be in a position to respond through the media regarding what are the facts. Perhaps, we could avoid some problems that might otherwise occur.

Have we given any thought to that, or have any of the efforts of Mr. Koskinen directed in that way?

Mr. SPOTILA. Actually, Congressman, we've been giving quite a bit of thought to that. Let me address it in two respects. First of all, as I mentioned in my testimony, from a security standpoint we're asking each agency in its day 1 plan to address the question of protecting systems from anyone who would cause mischief. That's an element here.

With respect to misinformation that might be put out, here, too, agencies will be focused on how that information might relate to them individually. In a coordinated way, the Information Coordination Center will help, John Koskinen and the President's Council on Year 2000 Conversion have a plan for collecting and exchanging information in this area, working closely with their private sector coordinators and others throughout State and local government to be in a position to verify what information is true and to be able to disseminate it.

The Coordination Center will play a key role in terms of overall coordination, even though we are also looking at individual agencies to be prepared to address agency specific concerns.

Mr. TURNER. Well, I would urge you to maybe pursue it a little bit further, because I think if we could enlist the assistance of some high-profile personalities who have credibility, a Walter Cronkite type who would be a spokesperson, along perhaps with one or two others. I don't think it's going to help if there's some rumor or misinformation floating, say, on the Internet, and it's reported that the government denies the report. Unfortunately, we all know the government oftentimes does not have the credibility that we might need.

So it would seem to me if we could attach a personality to that effort that would be known to be trustworthy by the American public, perhaps we could avoid some problems that otherwise might occur.

Mr. SPOTILA. I think that's a very constructive suggestion. We certainly will bring that up with John Koskinen and see what can be done in that area.

Mr. TURNER. Thank you. I don't have any other further questions.

Mrs. MORELLA. What are you going to be doing, Mr. Spotila, on that day? Where are you going to be?

Mr. SPOTILA. I think I will—actually, I asked my staff to tell me where they think I should be.

Mrs. MORELLA. Never leave yourself so wide open.

Mr. SPOTILA. I'm certainly making myself available to be right on duty here. But we're trying to determine whether that would be positive or negative in the view of the people that are actually going to be dealing with our problems.

Mrs. MORELLA. But I appreciate Mr. Turner asking that question because as we go on, I would like to find out, you know, specifically how that ICC is going to operate.

Mr. SPOTILA. Yes.

Mrs. MORELLA. I have a question, the same question actually for both of you. IRS is going to be a witness on our next panel, and recently IRS reported that the poor quality of its computer inventory poses a high risk to its Y2K effort. I quote that exactly. That was quoted in a letter to Mr. Archer, the chairman of the Ways and Means Committee. And it says the quality of the IRS's inventory currently poses a high risk to the Y2K effort.

Therefore, my question to both of you is, in your opinion, what can be done to—or what can the IRS do to mitigate that potential Y2K problem, those failures, and does the IRS have a practical contingency plan in place? They will have an opportunity to respond, but I wanted to hear from you before we dismiss this first panel.

Mr. WILLEMSSEN. Well, one, Chairwoman Morella, I think it is of concern to hear a major Federal agency still talking about the term "inventory" at this late date. In testifying on the IRS, which I did as far back as February 1997, I know the IRS has a far-flung information systems structure, many of their systems out in the field, many of the systems homegrown, so it is a difficult endeavor to get a handle on all of those.

In terms of your direct question on what should they do, I think it's just ensuring that their key business processes, whether they're tax refunds or tax processing, however IRS has defined them, that they have thoroughly decomposed those processes and identified their key systems that they need to be ready in order to do business as usual come the turn of the year.

Mrs. MORELLA. Do they have time to do that?

Mr. WILLEMSSEN. I think one thing in their favor is given the background of the Commissioner of the Internal Revenue Service, he's made it very clear this has been a top priority for him for some time, and he also made it clear, I think, in hearings I've been at with him that this was a massive undertaking, that it had risks associated with it. And I think there is time to focus again on those most important business processes and decompose them and focus on the supporting systems.

Mrs. MORELLA. Mr. Spotila.

Mr. SPOTILA. From our perspective, I agree completely with Mr. Willemssen in all of those respects. We're concerned. We have not had quite as much information of IRS as we would like to see. We recognize the importance of this, and we certainly are going to do what we can do to help the situation.

Mrs. MORELLA. Well, we will be interested to also hear from IRS about, you know, what they are doing, particularly in light of that rather frightening statement.

Let me ask you about GAO, you recently reported that only 40 percent of Federal agencies submitted complete contingency plans with information on the seven criteria that you have established. What are you going to do to make sure that agencies complete these plans?

Mr. WILLEMSSEN. Well, in terms of their day 1 strategy and the required seven elements of OMB, I would concur with Mr. Spotila's comments that OMB is working with these agencies to followup where there are holes and where more information is needed. I

think we also have to keep in mind that many agencies were out front and had a lot of this detail all pulled together; many did not.

The requirement for day 1 strategies was initially contained in OMB's September 13th quarterly report summary. So that was the first time a requirement was sent out. OMB's guidance on what to include, I believe, came out on October 13th, and then the strategies were due 2 days later.

So we're talking about a very compressed time. I think we have to give the agencies that did get a late start some recognition that they have time to improve, but this has to be a top priority at this point in time. I think OMB shares that view, and through our reviews and evaluations, we have not seen evidence of agencies resisting day 1 concept. What they don't have in many cases are all the details worked out yet, and that's what they have to focus on now.

Mrs. MORELLA. I know that GAO is the one who has suggested that OMB come up with the criteria, which they did so well, established the October 15th deadline. Now, in light of the question that I asked Mr. Willemssen, which is directed to you now, do you have another deadline that you have established where you say you now must get the responses, your contingency plans in effect by another deadline?

Mr. SPOTILA. We're proceeding on two levels: one, individually with agencies, based on what they have submitted to us, or in a couple of instances where they have not submitted to us, to work with them to get this fixed.

We've also told them informally that we will be asking them for a new updated report next month, so there is going to be a new November deadline for them. That has not formally gone out yet, but they have all been advised that it is coming. Our priority has been working with GAO and working with the agencies to get these plans in their proper shape.

Mrs. MORELLA. It appears as though they may be working very long days in order to do it, and I think you should set an early November deadline for that, too.

Mr. SPOTILA. We intend to.

Mrs. MORELLA. I guess I just have one more question so we can get on to our next panel. And I know that you have always been available to respond to other questions that we may submit.

Another day 1 strategy requirement is to include data on contractor availability. Do you believe that this requirement is being followed, being overlooked? Because I think it's exceedingly important, and we've discussed this in a number of our other hearings, exceedingly important for interoperability and for the successful operation of many of the Federal mission-critical systems.

What have your investigations revealed thus far with respect to Federal contractors?

Mr. WILLEMSSEN. In taking a look at the strategies that have been submitted thus far, it's a bit of a mix. Some of the agencies haven't addressed the issue, and don't know the availability. Other agencies are still working on this. I think this is a fairly critical issue, and it's critical from a couple respects. One is making sure from a governmentwide basis that not everyone thinks they have a relationship with the same vendor, and making sure that that

vendor isn't overextended. And then second is laying out in specified detail exactly who to contact with that contractor or vendor should disruptions occur.

Mrs. MORELLA. Mr. Spotila, would you like to comment on that?

Mr. SPOTILA. Yes. Once again I would agree. I think in general, with most of the agencies, we need more detailed information on this subject. One of our observations is that a number of the agencies need to do more in this area. Some have done real well. Social Security whom you will be hearing from, has done an excellent job. NASA and the Department of Transportation have done very well. But there are a number of agencies that need to add considerable detail here, and that's one of the areas we're pressing.

Mrs. MORELLA. This is going to be one of the questions we're going to ask to our second panel what they're doing, and I'm glad that you're both very aware of it and continue to ask for that response.

Just finally the issue of computer security, this is one, as you know, I think is critically important as it relates to Y2K and even beyond that. How certain are you that the remediation efforts of the Federal systems have been conducted by firms that are U.S.-owned, and then if you would like to comment on what the risks might be that foreign agents or those with antigovernment views might have access to sensitive computer data. If I could ask both of you if you can answer that.

Mr. WILLEMSSEN. I will answer that in two ways. One is to give you my nonscientific answer that I think overall if you compare what has happened on remediation to what we thought would happen in the 1996 or 1997 timeframe, we've been a little surprised that more of the remediation work was actually done in-house and by existing contractors as it pertains to Federal agencies than we would have thought. There really wasn't as much work that went outside of the existing agency-contractor relationships as we would have envisioned.

Point two, we share your concern about Y2K security risks. Frankly, we haven't at this point done a lot of work on this. We do have some ongoing work looking at that right now with some high-profile agencies, such as the Federal Aviation Administration and Department of Energy. At these agencies we are pursuing the issue to see what kind of controls and processes the agencies have in place.

Overall, I think that the executive branch is very, very aware of this particular issue, and it's brought up in almost every meeting I'm in on Y2K over the last couple of months.

Mr. SPOTILA. I would echo those comments. In general, OMB does not have individual agency information in this regard. We've relied on the agencies and their decisionmaking process. We have worked in coordination with the National Security Council, with the President's advisor on counterterrorism Mr. Clark, and the CIAO office. This is something we are sensitive to. We have looked at security concerns here, and we think that the right steps are being taken, but it certainly is not something that we are taking for granted.

Mrs. MORELLA. Well, I'm glad to hear that because I think it's critically important. We focus on it because this whole concept of

the potential for the computer security could dwarf the problems of Y2K.

Mr. Turner, do you have any final comments?

Mr. TURNER. No final questions, thank you.

Mrs. MORELLA. I want to thank panel one for the work you've done not only in your presentations and responses today, but continuously that you've done. Thank you very much.

Mr. WILLEMSSEN. Thank you.

Mr. SPOTILA. Thank you.

Mrs. MORELLA. Now we will ask the second panel to come forward. Mr. Dyer, Mr. Langston, Mr. Gilligan, Mr. Cosgrave, Mr. Lorentz.

Gentlemen, before you get comfortable, as we did with the first panel, I would ask you kindly to stand and raise your right hand. [Witnesses sworn.]

Mrs. MORELLA. Again, the record will demonstrate affirmative response to that.

So we're pleased to have on our second panel John Dyer, Principal Deputy of the Social Security Administration; Dr. Marvin J. Langston, Deputy Assistant Secretary of Defense for C31 and the Year 2000, Department of Defense; John Gilligan, Chief Information Officer of the Department of Energy; Mr. Paul Cosgrave, who is the Chief Information Officer of the Internal Revenue Service; Mr. Norman E. Lorentz, Senior Vice President, Chief Technology Officer of the United States Postal Service.

Gentlemen, I'm glad you're here, it's very important that we hear from you. And I think it was appropriate that you also heard the testimony of GAO and OMB preceding you. And again, following sort of a 5-minute rule, we're very flexible about it.

We will start off, and I will let you know that we will hope to have time for questioning and that your entire statement will be in the record, so you can give us a synopsis, if you desire. So we will start off with you then.

Mr. Dyer, thank you for being here.

STATEMENTS OF JOHN DYER, PRINCIPAL DEPUTY, SOCIAL SECURITY ADMINISTRATION; MARVIN J. LANGSTON, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR C3I AND YEAR 2000, DEPARTMENT OF DEFENSE, ACCOMPANIED BY REAR ADMIRAL BOB WILLARD AND BILL CURTIS, DEPARTMENT OF DEFENSE; JOHN GILLIGAN, CHIEF INFORMATION OFFICER, DEPARTMENT OF ENERGY; PAUL COSGRAVE, CHIEF INFORMATION OFFICER, INTERNAL REVENUE SERVICE; AND NORMAN E. LORENTZ, SENIOR VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER, U.S. POSTAL SERVICE

Mr. DYER. Madam Chairwoman and Representative Turner, I appreciate the opportunity to discuss the Social Security Administration's day 1 and business continuity and contingency plans for the year 2000 changeover. As a recognized leader in Y2K readiness, we are confident that our monthly payments to 50 million people and the earnings records of 145 million workers will not be affected; however, in the case of the unexpected, we are prepared.

To begin with, all of our mission-critical systems are certified as year 2000 compliant, along with all of the State disability deter-

mination services referred to as DDSs. Additionally, joint testing of payment files and direct deposit procedures have been successfully completed, as is the Federal Reserve Board testing with financial institutions, including Social Security transactions. Last, as for trading partners, Treasury and the Postal Service are also on board to handle ongoing and incoming exchanges.

At this point I would like to review step by step our plans for the last days of 1999 and the first days of 2000. For December 30th to January 3rd, designated personnel will inspect, evaluate and report on virtually every office. Social Security headquarters will stop receiving on-line transactions from field offices at 5 p.m. Eastern Standard Time on December 30th, allowing all officials to collect all of our 1999 computer transactions.

On December 31st, our computer systems will finish updating SSA's master files. Just before midnight, the Social Security's main data center in Baltimore will switch to jet fuel generators until the power company notifies the agency that everything is fine.

Immediately after midnight, December 31st, 1999, teams will begin assessing our systems' capability to process transactions for the year 2000. Later that day, staff at selected offices across the country will enter data. We will also test the 800 number. Throughout New Year's Day, a group of programmers will run checks on the computer systems for our 1,400 facilities.

Social Security managers will report to their offices, checking all equipment and reporting their findings to regional offices, which will then forward the data to the command center in Baltimore. Approximately 100 sites will serve as barometer offices, including the 55 that do the disability determinations.

Agency technical staff will test software systems by conducting a series of typical transactions. The Baltimore command center will monitor the processing. If problems are found, teams will be dispatched to make the necessary repairs. Besides assessing Social Security's infrastructure, our command center will communicate with several non-SSA sites, such as the Treasury command center, to be alerted to any problems that banks may have in posting electronic fund transfers. Moreover, we will advise the White House Information Coordination Center, the media and the Congress of SSA's status. Then on January 3rd, Social Security will open for business as usual.

SSA's day 1 strategy is part of our overall business continuity and contingency plan. The plan prepares the agency to avoid a possible crisis if its automated systems are unable to recognize the year 2000. Within this larger plan, we have local plans for each field office, teleservice centers, processing centers, hearing offices and the State DDSs. We have developed contingencies for benefit payment delivery, building operations, human resources and communications.

For over a year both Social Security and SSI payments have been made with year 2000 compliant systems. Furthermore, we have developed a benefit payment delivery plan with the Treasury Department and the Federal Reserve. In November 1999, next month, field office employees will receive training as to the actions and procedures they are to follow if such an unanticipated problem occurs. SSA also has contingency plans that deal with unforeseen

emergencies, such as inclement weather, natural disasters, accidents or equipment failure.

We want the public to understand that we're prepared for the year 2000 conversion. We want the public to have accurate information. Misinformation and confusion could generate overwhelming workloads and cause disruptions. Therefore we appreciate the Congress and others updating the American public about the actions Social Security and other Federal agencies have taken to prepare for the year 2000.

For our part we're committed to informing Members of Congress if serious problems develop. If a service to any of our local offices is interrupted, and contingency plans are implemented, the manager of the affected office will call the congressional office with specific information on how it will provide service to the congressional representative, congressional offices and to the constituents normally served by that office.

In fact, on September 23rd, we sent a letter to the Congress outlining these steps and listed the names and phone numbers of the managers of each local office in each State responsible for calling you.

Because of our early planning and testing, Social Security fully expects that all of our processes will function properly in the new millennium, and that we will continue to provide world-class service to the American people.

I'm happy to answer any questions you might have. Thank you.

Mrs. MORELLA. Thank you, Mr. Dyer. I know that Social Security Administration started in 1989 in their preparation.

[The prepared statement of Mr. Dyer follows:]

FOR RELEASE UPON DELIVERY

**Y2K READINESS OF SSA's
BUSINESS CONTINUITY AND CONTINGENCY PLAN
and
DAY ONE PLAN**

STATEMENT BY

**JOHN R. DYER
PRINCIPAL DEPUTY COMMISSIONER**



**BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
AND THE
SUBCOMMITTEE ON TECHNOLOGY**

October 29, 1999

Chairman Horn, Chairwomen Morella, Representative Turner, Representative Barcia and Members of the Subcommittees:

I appreciate being here today to discuss the Social Security Administration's (SSA) Day One Plan and Business Continuity and Contingency Plans for the Year 2000 changeover. I would like to thank the subcommittees for holding this hearing to make the public aware of SSA's plans for a continuation of service if the unexpected should happen.

Social Security is recognized as a leader in preparing our systems for the Year 2000, and we are confident that the monthly payments to 50 million people and the earnings records of 145 million workers will not be affected. Social Security's benefit payment systems are Year 2000 ready.

Status of Year 2000 Preparation

We are happy to report that all of our mission critical systems that ensure the continuity of SSA's core business processes are now certified as Year 2000 compliant. These automated systems are the means by which SSA is able to provide service on demand to the public, the Agency client population, other government entities, and large and small corporations and individual businesses.

We worked with the State Disability Determination Services (DDS) to make sure that the 55 State DDSs that have automated systems to support the disability determination process are year 2000 compliant. As of January, 1999 all of the State DDS systems are Year 2000 compliant.

Joint testing of payment files has been successfully completed. End to end testing from SSA, through Treasury and the Federal Reserve (Automated Clearing House) for direct deposit payments were also successfully completed in August 1998. In addition, the Federal Reserve has been conducting tests with financial institutions and Social Security

transactions are included in those test files. Critical Federal systems supporting the Social Security program at SSA, Treasury, and the Postal Service are ready for the 21st century and will be able to provide benefits to more than 48 million Americans under the Social Security and Supplemental Security Income (SSI) programs without interruption throughout 1999 and in the year 2000. Millions of Americans rely on such monthly payments. In fact, since October 1998, payments for both Social Security and SSI programs have been made with Year 2000-compliant systems.

We recognize that it is not enough for SSA to be Year 2000 compliant if our trading partners are not ready. We have worked closely with our trading partners. I am pleased to report that all outgoing and incoming exchanges are compliant and implemented.

Today, I would like to discuss SSA's plan of action for the days immediately surrounding the millennium change, our overall contingency plan, our plans addressing potential problems with the national power grid and utility companies, and public overreaction to the Year 2000 issue.

Day One Strategy

Our Day One Strategy is a comprehensive set of actions that will be executed during the last days of 1999 and the first days of 2000. The strategy also includes the activities leading up to the critical century rollover date, such as identification of key personnel involved, preparation of facilities checklists, establishment of the Year 2000 command center, a schedule for testing systems over the rollover weekend, and other activities. Implementation of the Strategy will ensure, to the extent possible, that SSA's facilities and systems will be fully operational on January 3, 2000—the first business day of the new century. That is, service to the public and our trading partners will continue without interruption due to the change of century date. We are proud that the Government Accounting Office has recognized SSA for developing our day-one strategy and it is being used as an example to be followed government wide.

Walkthrough of SSA 's Year 2000 Activities December 30 - January 3

Let me give you a brief picture of what will happen beginning Thursday December 30. SSA will have a Year 2000 command center in Baltimore. During the time period from December 30 to January 3, designated personnel throughout SSA will inspect, evaluate, and report on virtually every office throughout SSA.

Under SSA 's Day One plan, agency computers will shut down earlier than usual on Thursday, December 30. Taking the systems off-line will allow officials to collect all their 1999 computer transactions from nearly 1,400 offices, including those from Guam and Hawaii.

During the night and continuing into Friday, the Social Security computer systems will finish updating SSA 's master files. This will complete the processing of the 1999 transactions.

Just before midnight Friday, Social Security 's main data center in Baltimore will switch to generators powered by jet fuel. The agency has stockpiled sufficient jet fuel to operate for several days. While we do not expect any disruptions to the region 's power grid, we are taking this precaution to guard against any electrical surges that could damage our equipment.

When the power company lets the agency know everything is fine, we will turn off the generators and hook back into regular power lines. The power switching will not require the agency to turn off our computers.

Immediately after the stroke of midnight on December 31st, 1999, teams will begin assessing the health of SSA 's equipment and software. This is the first opportunity in the actual Year 2000 environment to be assured of our systems ' capability to process transactions for the Year 2000.

On Saturday, January 1st, SSA's online computer systems will be available for use and staff at selected offices will key in data. Taking this action gives SSA the opportunity two full days before we open our doors to the public to assess the health of our systems and we can correct any problems that might occur.

It will allow us to assess the Baltimore infrastructure that supports our field office computer processing, including the hardware and software, and infrastructure elements: electrical power, telephones, security systems, elevators, water supply, and so on are in working order. The agency will also test the 800 number telecommunications system. If any component cannot function properly at that time, corrective action will be undertaken immediately.

The Baltimore command center will also be in communication with several non-SSA sites. SSA will be in communication with the Treasury Command Center to discuss and take any action on any problems that banks are experiencing in posting electronic fund transfers. We will be in communication with the White House Information Coordination Center and the media, as necessary advising them of the status of SSA. SSA will keep members of Congress informed of our overall status that weekend if we encounter any national-level problems.

On Saturday morning, New Year's Day, groups of programmers will work throughout the day to run checks on the computer systems for 1,400 facilities including field office, toll-free telephone calling centers, hearings and appeals offices, regional offices and the Baltimore headquarters. Social Security managers will report to their offices and make sure all equipment is working. The managers will report their findings to regional offices, which will forward data to the command center in Baltimore.

Approximately 100 sites have been selected to serve as barometer offices, including 55 offices that make disability determinations. The agency's technical staff will test software systems by conducting a series of typical transactions, such as processing

applications for benefits. The Baltimore command center will monitor the processing and check to see that the systems are working properly. If problems are found, teams will be dispatched to make necessary repairs. The teams will have Saturday night and Sunday to fix problems.

SSA understands the security risks associated with the rollover weekend. We have developed and put in place specific plans to address both physical security and electronic security.

On Monday morning, January 3rd, Social Security will open for business. We have worked hard to ensure that, to the greatest extent possible, that SSA's facilities and systems will be fully operational on this first business day of the new century.

Business Continuity and Contingency Plan

SSA's Day One Strategy is part of SSA's overall Business Continuity and Contingency Plan. The plan was first issued March 31, 1998, and it is updated quarterly. We completed testing our contingency plan last month. The plan is consistent with Government Accounting guidelines and is being used as a model by other agencies and the private sector.

The purpose of this plan is to ensure the continuity of SSA's core business processes, including disability claims processing functions supported by the Disability Determination Services. Our automated systems are the means by which SSA is able to provide service on demand to the public, and are crucial to SSA's ability to fulfill our mission. This plan prepares the Agency to avoid a crisis that could result if its automated systems are unable to recognize Year-2000 dates. The plan identifies risks and threats, establishes mitigation strategies for the identified risks and threats, and provides contingencies in the event risk mitigation fails.

The risk of failure is not limited to SSA's internal systems. SSA's ability to provide world class service to beneficiaries, workers and their families depend on a complex infrastructure that is crucial to our ongoing operations. Power, data, and voice telecommunications, along with the Agency's computer operations hardware and software, are essential to ensuring that SSA's business processes are able to continue uninterrupted.

As risk mitigation strategies are in place, the degrees of risk are reduced and the possibility that the contingency plan would need to be implemented are similarly reduced. Our Business Continuity and Contingency Plan is also being used to identify areas where more detailed plans are needed.

As part of this plan, we have in place local plans for each of our field offices, teleservice centers, processing centers, hearing offices and State DDSs. We have developed contingency plans for benefit payment and delivery, building operations, human resources, and communications.

For over a year, payments for both Social Security and SSI programs have been made with Year 2000-compliant systems. Since we are aware that one weak link anywhere in the chain, including the links representing our business partners as well as the public infrastructure, can cause major disruption to business operations, we developed a benefit payment and delivery plan in conjunction with the Treasury Department and the Federal Reserve. This plan provides alternate ways of getting payments to Social Security beneficiaries. In November 1999 Field Office employees will receive training as to the actions and procedures they are to follow, should an unanticipated problem occur with a financial institution.

Power

At any given time, unforeseen factors such as inclement weather, natural disasters, accidents, or equipment failures can and do have some affect on power. SSA is accustomed to planning and responding to emergencies and other unexpected events. SSA has contingency plans in place to deal with such emergencies. For example during the recent Hurricanes that struck North Carolina there were some disruptions in service. However, proper contingency planning and advance preparation allowed quick recovery and resumption of services. If regional or national level outages are experienced, SSA has plans to suspend SSA activities at locations without backup power systems until utilities are restored. Our agency can move people to work and work to people. We have in place an 800 telephone number system that can redirect phone calls to other parts of the country

Public Overreaction

Currently, one of our greatest concerns is misinformation and confusion over what may occur during the changeover to 2000. A public reaction to misinformation could potentially generate overwhelming workloads, causing disruptions to our business operations. We want the public to understand that we have prepared for the Year 2000 conversion. We have plans to insure a continuation of service if the unexpected happens.

We are thankful for the lead taken by the Congress, John Koskinen, as Chairman of the President's Council on Year 2000 Conversion Efforts and Joel Willemssen and others at the General Accounting Office to keep the American public informed concerning the actions that we, as well as other Federal agencies have taken to prepare for the Year 2000.

Conclusion

In conclusion, we are committed to keeping the members of Congress fully informed if a serious problem develops. In the event that any service to any of our local offices is interrupted and contingency plans are implemented, the manager of any affected Social Security office will call the local Congressional office as soon as possible. The manager will let them know how we will provide service to the Congressional representative, Congressional office and the constituents who are normally serviced by that office.

On September 23, 1999, we sent each member of Congress a letter outlining the steps we will take to keep you informed of any disruption of services, including the names and phone numbers of the managers in each local office within your State who will be responsible for calling you in the event of service disruption.

SSA is proud of our reputation as a leader in addressing Year 2000 issues. Because of SSA's early planning and testing, we fully expect that SSA's processes will function properly. We are confident that we are prepared for the arrival of the new millennium. I will be happy to answer any questions that you may have.

Mrs. MORELLA. Mr. Langston, Dr. Langston.

Mr. LANGSTON. Chairwoman Morella, Mr. Turner, thank you very much for your continued interest in this subject. The Department of Defense is very proud of the progress that we have made over the past 15 months of this ongoing year 2000 preparation effort.

I'm joined this morning by Rear Admiral Bob Willard, who has been spearheading this effort in our unified forces and services, and also Mr. Bill Curtis, who has been our full-time person leading and directing the year 2000 event for the past period of time.

We have addressed this issue in four major activities. Those activities comprise systems compliance, operational evaluation and testing, contingency planning, leadership preparation and a transition period which has begun. I will just spend a few minutes outlining the activity in these areas for you.

In the systems compliance area we are tracking and repairing over 7,500 systems. Over 2,000 of those are mission-critical systems. The rest are non-mission-critical systems. And in addition, we have 600 installations and 350 domains among our main megacenter mainframe computers that we have worked to repair. Of those systems we are confident that all of them will be repaired and ready to go for this event, and currently we are over 98 percent of our mission-critical systems.

In the operational evaluation and testing area, this is the largest effort in DOD's history. We have never conducted such an integrated and large operational evaluation of our systems. We have done it in two major ways. We have enlisted the uniformed services through the support from the chairman of the Joint Chiefs of Staff to conduct operational evaluations, which are threaded evaluations of systems operations that support our primary military functions. And we've also conducted functional evaluations of all of the support operations that foundation the Department; for example, financial systems, logistics systems, and personnel systems.

We have also conducted a whole series of service integration tests which are specific to each of our military services and verify that those systems of systems among the services are capable of supporting our needs.

In the contingency planning and leadership preparation area, the chairman of the Joint Chiefs of Staff has conducted a series of chairman contingency assessments personally led by the chairman and supported by our four-star uniformed commanders. They address mobilization, deployment operations and sustainment. And these evaluations were 2 week-long periods of removing tens of major systems from each of those areas to evaluate the impact of the loss of those systems and the support of the contingency plans that would be put in place should those systems be removed on military operations.

In each of those cases we determined that our contingency plans were an important element of what was needed, and that we, in fact, could conduct military operations should we lose those large number of systems.

We also conducted business continuity planning in terms of both systems continuity plans and operational continuity plans, meaning that we have a continuity plan for every system, and we have a

continuity plan for every operational functional area that is a combination of systems or a larger function, and therefore we have a way to support loss of capability in any one of these events.

We've also enlisted the support of all of our inspector generals, both the service inspector generals and the DOD inspector generals, on all of our assessment agencies to make sure that we have prepared good contingency plans and they are in good shape for these operations.

And finally, in preparation for our leadership, we have conducted a series of table top exercises which were literally day-long workshops that prepared the senior leaders to explore an enormous amount of unknown, what-if types of questions to determine how we would operate the Department through any kind of unknown surprise events.

Finally, the fourth area is a transition day 1 operations period which we did begin in September, the 1st of September, and we will operate through the 1st of March or the end of March of this coming year. A major part of this activity has been the preparation of a consequence management plan to help all of our warfighting commanders and base commanders understand how they can respond to situations and external requests from the Department for aid and support throughout the United States or other nations in the world. And in that process, we have also established a posture-level instruction which allows across five posture levels each of our commanders to understand how we are postured and how they are to respond specifically to those posture levels.

For example, in this consequence management activity our first priority is, as Dr. Hamre, the Deputy Secretary, has reiterated several times, is to support national command authority or military operations in any form. Our second priority is to support standing operations. Our third priority is to support civil authorities and public health and safety. And our fourth priority is to support civil authorities in support of economic or national quality of life. These are all well laid out and detailed plans which we continue to refine wherever we find the need for such.

Finally, I would point out that we have had an ongoing operation with foreign nations and our NATO allies with a large amount of effort concentrated on the Russians and their interaction with us for early warning events and for mitigating any nuclear mishaps or missteps related to nuclear weapons. We are currently planning to put in place our Center for Year 2000 Strategic Stability in Colorado Springs. We have conducted successful negotiations with the Russians for them to participate in this event. They will be arriving in Colorado Springs on the 22nd of December and working with us through the 15th of January for that particular operation.

So in conclusion, I would suggest that we have conducted a very extensive activity over this past year. The activity actually transformed when Secretary Cohen and Dr. Hamre tasked the uniform commanders and the under secretaries of the functional support areas to be personally responsible for the operations and mission continuity through this period of time. I believe that it's fair to say that the Department literally does contingency planning all the time because of the nature of our business. We do continuously report activities on a 24 by 7 basis throughout the normal year, and

the year 2000 event for us is a significant event that we do not take lightly, but it does fit directly into our normal operations, and we feel that we will be ready and prepared to support any national security situation throughout this period. Thank you.

Mrs. MORELLA. Thank you, Dr. Langston.

[The prepared statement of Mr. Langston follows:]



Statement
of

Dr. Marvin J. Langston
Deputy Assistant Secretary of Defense
(Deputy Chief Information Officer and Year 2000)

Before the
Joint Hearing of the

Subcommittee on Government Management, Information, and Technology

Committee on Government Reform

and the

Subcommittee on Technology

Committee on Science

United States House of Representatives

YEAR 2000 PREPAREDNESS

Business Continuity and Contingency and Day One Plans

October 29, 1999

Table of Contents

Introduction.....	1
DoD Y2K Continuity and Contingency Planning.....	2
Business Impact Analysis.....	3
Core Functions	3
Planning Assumptions	3
General Planning Assumptions	3
CONUS.....	3
OCONUS.....	4
Site-Specific Planning Assumptions	4
Other Risks to DoD Operations.....	4
Domestic Infrastructure Disruptions.....	4
Host Nation Infrastructure Support Disruptions	4
NATO/Allied Systems Interoperability Disruptions.....	4
Contingency Planning Oversight and Tracking.....	4
System Contingency Plans.....	4
Operational Contingency Plans.....	5
Year 2000 Transition Period/Day One.....	5
Leadership Preparation for Decision-Making	6
CJCS Contingency Assessments	6
Table Top Exercises.....	6
Consequence Management Planning.....	7
Conclusion	7

Introduction

The scope and complexity of the Y2K problem for the DoD is unparalleled in the federal government. The Department of Defense has over 3 million people – active, Guard, Reserve, and civilian – spread all over the world. To administer this community takes over 1.5 million individual computers at hundreds of locations around the globe. As of the Monthly Report to the Office of Management and Budget (OMB), submitted on October 15, 1999, DoD has 9,480 systems, of which 25 percent (2,369) are mission critical systems. The Department also operates 637 military installations around the world and in the United States, which are like small towns, and rely on supporting infrastructure systems also vulnerable to Y2K problems. In addition, the Department will have 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. Over one-third of the government's mission critical systems are in the Department of Defense.

There are four major components of the DoD Year 2000 Program: Systems Compliance – making sure all individual systems are Year 2000 compliant in accordance with the OMB five-phase process; Operational Evaluation/Testing – to buy increased assurance that our systems work in the real world; Contingency Planning – taking prudent precautions in case systems or capabilities become unavailable due to Year 2000 related problems; and Transition Period Operations – managing the remaining challenges and reporting and responding to Year 2000 related events. This statement will focus on the last two of these components and address DoD Business Continuity and Contingency Planning (BCCP) Efforts and Day One Planning.

The DoD does contingency planning all the time for military operations and for its business functions. Consequently, the Department was well prepared for the BCCP requirements generated by the Year 2000 problem. The mission critical systems in DoD have system contingency plans in place that are being rehearsed and refined and reviewed by external and internal auditors. The Chairman of the Joint Chiefs of Staff conducted a series of "Contingency Assessments" to determine whether key warfighting tasks could be accomplished if key systems became unavailable. These exercise involved all facets of the Department and were a critical element in evaluating the feasibility of contingency plans for major warfighting support functions. The Department conducted a series of Table Top Exercises for senior leaders, including participation in a National level TTE in September. The TTE prepared senior leaders for possible policy decision that might be generated by Year 2000 related problems.

For Day One operations, the Department is also well prepared. Throughout DoD, elements are conducting reporting and response to situations all over the world all the time. In fact, 24 hours a day, 7 days a week is the norm for DoD operations centers. Operational reporting procedures are in place, robust, and frequently exercised in real world operations. The Department is tuning these procedures to address the information technology and critical infrastructure issues that may be raised by Year 2000 problems. In addition, the Department is taking prudent "Day One" measures to ensure key personnel availability; prepositioning of key response assets; and availability of redundant communications throughout the date transition period. In fact, because of the wide range of date that may generate information technology problems, DoD designated the period September 1, 1999 through 31 March 2000 as the date transition period. While most of the focus thus far has been on the 31 December 1999 to 1

January 2000 date roll over, DoD is also planning for a similar focus on the leap year transition in February of 2000.

Finally, DoD's first priority is to execute the national military strategy. To ensure that capability, the Department has established and promulgated priorities and procedures for managing Military Support to Civil Authorities and Foreign Disaster Assistance with the normal channels. The Department will use normal channels to report and process requests for assistance, which involve the Federal Emergency Management Agency for MCSA and the Department of State for FDA. In addition, DoD continues to work with the President's Council on Year 2000 Information Coordination Center on the information required and procedures for Year 2000 related information.

In summary, despite the enormity of the problem, DoD will be ready for the Year 2000. The remainder of this statement provides more details on DoD contingency planning and Day One/Transition Operations.

DoD Y2K Continuity and Contingency Planning

Like all U.S. Government Agencies, DoD is using Contingency Planning to ensure continuity of critical functions in the event of unforeseen disruptions to DoD and Government Systems or the supporting infrastructure. Y2K Contingency Planning within DoD takes on different forms and uses different names than other agencies, but is built on the same foundation as the GAO recommended approach to Business Continuity and Contingency Planning.

Information requirements, methods and techniques to be used in developing all contingency plans are outlined in the DoD Year 2000 Management Plan. Amplifying guidance has been promulgated by each of the DoD Components. A DoD Commander's Y2K Preparedness Handbook was published by the OASD(C3I)Y2K Office to assist in the process of determining local risks, based on the infrastructure supporting each site.

The two primary types of Y2K continuity and contingency plans within DoD are:

- System Contingency Plans – which document the planned actions associated with a timely restoration of a system to full functionality following a Y2K-related disruption to the hardware and software associated with the system. Within DoD, System Contingency Plans are required for all date-aware mission-critical systems and strongly recommended for most other systems. The status of system contingency plans for mission-critical systems is being tracked in the DoD Y2K Database.
- Operational Contingency Plans – which document the planned actions associated with maintaining a pre-designated minimum level of capability during any disruptions to the supporting systems or infrastructure. Operational Contingency Plans may be written in support of a single system or application, in support of a single mission or function, or in support of the full range of missions or functions performed by a DoD entity. When the planning is in support of a single system or application, the system contingency planning information and the operational contingency planning information are often combined in a single plan. Operational Contingency Plans may

be known in some DoD Components as Continuity of Operations Plans, Operational Continuity Plans or Business Continuity Plans.

Business Impact Analysis

Impact Analysis is performed using operational risk analysis procedures standard for all DoD planning processes. Most DoD missions are characterized by extremely long and complex information chains. To ensure that these chains were thoroughly examined, the Joint Chiefs of Staff, each of the Unified Commands, the Services and most DoD Agencies used a technique called *Thin Line of Systems Analysis* to determine the critical paths by which information flowed during the execution of their primary missions. Identifying the *thin lines* served to ensure that all mission-critical systems were identified for each DoD mission/function. Systems comprising these *thin lines* were all involved in end-to-end testing to ensure that all elements were fully Y2K compliant.

Core Functions

The Department of Defense is a very complex organization. Under its present organization, there are three primary allocations of responsibility. These may be described as follows:

- Warfighting, which is the responsibility of the Joint Chiefs and the Unified Commands
- Organize, Train and Equip, which are the Title X responsibilities of the Services.
- Support Functions (Logistics, Personnel, Health/Medical, Communications, Intelligence) which are the responsibilities of designated Principal Staff Assistants (PSAs) within the Office of the Secretary of Defense.

The DoD commands are assigned missions from various higher authorities. These missions can be analyzed and linked to elements from the applicable Service or Joint Mission Essential Task List (METL). The missions and METLs of each DoD command correspond to the core functions of that command.

Planning Assumptions

There are two major categories of planning assumptions: general assumptions applicable across DoD, and site specific assumptions applicable to a unique location.

General Planning Assumptions

DoD Operations occur worldwide and thus the general planning assumptions are separated into CONUS and OCONUS locations.

CONUS

For purposes of preparing DoD business continuity and contingency plans, DoD Components should assume that electric power, natural gas, water service, waste treatment, financial services, transportation, public voice and data communications, the Internet, mail service, and the mass media will be available domestically, although it is possible that there will be localized disruptions in some areas. Each Command preparing an operational contingency plan shall make a determination as to the degree to which the general assumption applies to the sites(s) covered by that particular plan.

OCONUS

In non-U.S. locations, DoD follows the general planning assumptions of the State Department, which, in cooperation with other agencies, is gathering Y2K information on a country-specific basis. The State Department has designated the Head of Mission in each country to be the U.S. lead on Y2K issues there, and agencies with interests overseas should work with the State Department to understand the risks to their operations and to develop appropriate assumptions.

Site-Specific Planning Assumptions

The Commander / Director responsible for each DoD site or facility is responsible for determining the appropriate site-specific planning assumptions for that location. This entails due diligence in seeking out the Y2K status of local suppliers of critical services and supplies to that site in support of its core functions.

Other Risks to DoD Operations

The principal external risks to DoD Operations may be separated into three categories: Domestic Infrastructure Disruptions; Host Nation Infrastructure Support Disruptions; U.S. and NATO/Allied Systems Interoperability Disruptions.

Domestic Infrastructure Disruptions

Domestic infrastructure disruptions are addressed during the normal contingency planning process. DoD planners make full use of the extensive information available through the Internet and the large number of DoD Y2K-related websites.

Host Nation Infrastructure Support Disruptions

Regional Discussions with Host Nations for OCONUS installations have been used to ensure that Y2K planning assumptions are valid, as discussed previously. In addition, the OASD(C3I)Y2K Office has representatives working directly with NATO to facilitate the process of information exchange among NATO planners. Since the most critical status updates are those to be collected in the final months before the Date Transition Event, this process will grow in emphasis during 1999.

NATO/Allied Systems Interoperability Disruptions

Interoperability Testing has been planned to ensure systems interoperability with Allied and NATO systems. The operational contingency plans developed by Joint and Allied Commands will address procedures to be followed in case of unforeseen disruptions.

Contingency Planning Oversight and Tracking

Oversight and tracking for contingency plans differs based on the type of contingency plan: system or operational.

System Contingency Plans

These plans, a responsibility of Chief Information Officers and Program Managers, are centrally tracked as to its status for all mission-critical systems. Oversight responsibilities with respect to Plan viability and completeness fall primarily on the CIO or Program Manager. Many system plans also received additional oversight during the Operational Readiness Assessments, other testing and during DoD IG and Service IG visits and inspections. The OASD(C3I)Y2K

office reviews all test reports and IG reports involving contingency plans and advises the cognizant staff as to its recommendations.

Operational Contingency Plans

In keeping with DoD's management strategy of centralized policy development, decentralized planning and execution, the Joint Chiefs, the PSAs and the Services are each responsible for determining the elements which must do Operational Contingency Planning in that organization. In general, all units with a Director or Commanding Officer are required to develop these plans. Tracking and Oversight responsibilities remain with the organization and the status of operational contingency plans is not captured in the DoD Y2K Database. DoD IG and Component IG offices provide an additional level of oversight.

Year 2000 Transition Period/Day One

The Department has designated the period September 1, 1999, through March 31, 2000, as the "Y2K Date Transition Period." This period encompasses possible events occurring from the 9/9/99 date and from the February 29, 2000, leap year date. To prepare for the unprecedented nature of possible Y2K problems, DoD is developing procedures to ensure its ability to identify, report, and respond effectively to Y2K-related events.

As indicated in the earlier response on national security responsibilities, DoD formed a Year 2000 Consequence Management Integrated Process Team (IPT). The IPT consisted of representatives from all elements of the Department, including the Services, Joint Staff, OSD Principal Staff Assistants, and the Director of Military Support (DOMS). The IPT reviewed current guidance, processes, and procedures for providing domestic Military Support to Civil Authorities (MSCA). The IPT also reviewed the organizational structure, processes, and procedures necessary to respond to requests for foreign disaster assistance. Based on recommendations made by the IPT, DoD is:

- Ensuring resource visibility and refining its allocation processes by identifying DoD assets that have utility in providing Military Support to Civil Authorities.
- Refining operations and reporting procedures and developing an agreed to lexicon to ensure the creation and maintenance of a "common operational picture."
- Developing a strategy to ensure that DoD resources are applied in the most effective and efficient manner possible.
- Developing specific Y2K training materials to ensure everyone involved in MSCA knows the specific methods for dealing with Year 2000-related requests.
- Refining its procedures for ensuring real-time decision support information to DoD authorities to include creation of an Infrastructure Monitoring and Decision Support Activity. The Activity will monitor critical Defense systems and infrastructures, public broadcasts, and the Internet to provide infrastructure reliability and decision-support information to the Executive Support Center.

Throughout 1999, DoD conducted a series of events to prepare senior leadership for possible decisions required by Y2K contingencies and evaluated the Department's operational contingency plans.

Leadership Preparation for Decision-Making

There were two major activities in preparing DoD leadership for dealing with Y2K: Chairman of the Joint Chiefs of Staff (CJCS) Contingency Assessments and Table Top Exercises

CJCS Contingency Assessments

The CJCS conducted Exercise POSITIVE RESPONSE Year 2000 (PRY2K). PRY2K was a series of four command post exercises scheduled from February to September 1999 and was the first national level exercise conducted under conditions of multiple Y2K mission critical system failures. The PRY2K assessed the ability of DoD to respond with timely decisions in a Y2K degraded environment and focused on the strategic national tasks of mobilization, deployment, employment, intelligence-surveillance-reconnaissance (ISR), and sustainment.

This series of exercises was designed to achieve senior participation in and awareness of the operational impact of Y2K mission critical systems failure during the mobilization, deployment, employment, and sustainment processes. The concept was to remove mission critical systems and capabilities from play during the conduct of a robust warfighting scenario and then assess DoD ability to respond with timely decisions. In addition, the exercises assessed the ability of the Services to execute operational contingency plans and to mitigate problems associated with Y2K. Finally, senior members of the warfighting community shared lessons learned and other vital information via secure videoteleconference (SVTC). The Secretary of Defense, CJCS, Service Chiefs, and CINCs participated in the SVTC following each exercise with a goal of recommending a strategy to the National Command Authorities to mitigate the impact of mission critical systems failure

Table Top Exercises

In addition to the CJCS Contingency Assessments, the Department announced its plan for preparing the DoD leadership for the impact of Y2K on national security in a December 8, 1998, memorandum titled, "Participation in Department of Defense and National Level Y2K Table Top Exercises." This memorandum outlines exercise activities conducted at the defense and national level. The exercises expose participants to a reasonably worst case scenario induced by potential Y2K failures. These activities enhance participants' understanding of potential Y2K impacts on national security; assist in the development of policy recommendations; provide continuing impetus to accelerate progress on fixing Y2K systems problems; and facilitate effective contingency planning. The four-part program, depicted in Figure 4 below, included:

- A set of three functionally oriented one-day policy seminars held in November and December 1998 that identified some 70-80 policy-level issues that formed the foundation for further Table Top Exercise activities.
- A daylong Table Top Exercise policy workshop held on 30 January 1999. Participants represented the key decision-makers of DoD, including the Deputy Secretary of Defense, the State Department, the Federal Emergency Management Agency (FEMA), the President's Y2K Coordinator, and congressional staffers.
- A DoD Defense/National Security game conducted on September 8, 1999 and completed before the national level exercise. The DoD game focused on policy and crisis management in response to a national security emergency. The DoD senior leadership fully participated, including the Deputy Secretary of Defense, the Vice-

Chairman of the Joint Chiefs of Staff, the Service Under Secretaries, the DoD CIO, selected Principal Staff Assistants and the Directors of specified Defense Agencies. The State Department and FEMA also participated in the exercise.

- This activity led up to a National-level Y2K Table Top Exercise on September 18, 1999. This White House Y2K office inter-agency exercise was supported jointly by DoD and FEMA.

Consequence Management Planning

The Department of Defense has been working with other Federal agencies on consequence management and continuity of operations planning and recognizes the potential for multiple competing demands for DoD resources throughout the Y2K date transition period. Because of this, in January 1999, the Department conducted a high level review of its "consequence management" policies, procedures, and organizations. Actions taken after the review ensured DoD was prepared to support a potentially increased number of requests for both domestic and international assistance.

The first priority is to ensure DoD ability to conduct ongoing or imminent support to the National Command Authorities, warfighting, peacekeeping, intelligence, nuclear command and control, or critical infrastructure protection operations. Consequently, the Secretary of Defense, or his designated representative, approval is required before committing organizations and assets engaged in Priority 1 activities to support Y2K-related requests for assistance.

Likewise, the approval of the Chairman of the Joint Chiefs of Staff, or his designated representative, is required before assets or organizations engaged in Priority 2 activities can be committed to support Y2K related requests for assistance.

Other units may provide support to civil authorities with first priority to maintenance of public health and safety and second priority to maintenance of the economy and the nation's quality of life.

Throughout 1999, DoD has been actively collaborating with federal agencies and organizations to further the Department's (and the Nation's) ability to develop and exercise the information flow and procedures necessary to effectively respond to Y2K date related events.

Conclusion

The DoD approach to BCCP is to provide centralized policy guidance with DoD components developing appropriate plans based on that guidance and executing them appropriately. While some planning assumptions have changed for individual plans, the overall BCCP guidance remains valid and accurate as published earlier. With respect to Day One planning and activities, DoD is well tested and positioned in terms of preparation, monitoring and response activities as outlined in GAO publication, "Y2K Computing Challenge: Day One Planning and Operations Guide" (October 1999).

- The DoD components have gone to commendable lengths to prepare both their systems and their personnel for the transition. Y2K Leave/Travel policies have been

promulgated and informational messages regarding personal preparation have been broadcast in a variety of mediums.

- A system configuration management policy for Y2K to minimize changes has been promulgated, with documented procedures for obtaining necessary waivers.
- Infrastructure risk assessments have been performed by Defense Logistics Agency and by the commands responsible for coordinating and providing utilities and critical infrastructure services to DoD facilities.
- Organizational Y2K "command posts," existing operations centers, and facility special action teams have been designated. Operational forces will use their proven mechanisms for reporting and responding to changes in capability or readiness. The readiness of DoD business functions will be monitored by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Y2K Decision Support Activity (DSA). The business units of the DoD (e.g. Defense Logistics Agency, Defense Finance and Accounting Service) will report status and outages of mission critical systems to the DSA if and when they occur. Each Defense Agency and the major organizations of the services have established help desks and action teams to quickly respond to any system-related problems, while Continuity of Operations Plans ensure that core DoD missions will continue at acceptable levels.
- Y2K "Posture Levels" have been established by the Joint Staff and implemented by the Services, Commanders in Chief of the Combatant Commands, and key Defense Agencies. These posture levels provide planning and action assumptions for DoD components and a means to synchronize actions in anticipation of or response to any disruptions occurring during the date transition.

The Department of Defense will be prepared to execute its national security responsibilities before, on, and after January 1, 2000. The Department's comprehensive systems compliance efforts, operational evaluations and end-to-end testing, and systems and operational contingency plans are being developed and executed within a solid management structure. All Year 2000 efforts are receiving the personal attention of the Department's senior leadership. Finally, these efforts are being rigorously scrutinized by independent auditors, including the Department's Inspectors General and the General Accounting Office.

The Y2K problem is one of enormous scope and complexity for the Department of Defense, which has over one-third of the Federal Government's mission critical systems. Despite this challenge, the high percentage of systems compliance already achieved, combined with the results of end-to-end and operational evaluations already conducted and system contingency plans already tested, provides a high degree of confidence the Department will be able to execute the national military strategy unimpeded by Y2K-related problems.

Mrs. MORELLA. Mr. Gilligan, pleasure to hear from you sir.

Mr. GILLIGAN. Thank you, Madam Chairwoman Morella and Congressman Turner. I welcome this opportunity this morning to discuss the Department of Energy's contingency, business continuity and zero day plans. As Chief Information Officer for the Department of Energy, I am responsible for the oversight, coordination and facilitation of the Department's ongoing efforts to address year 2000 issues.

The Department has made great progress since the last time we testified before this subcommittee in June 1998, and I am pleased to be here to discuss our progress with you. Achieving 100 percent year 2000 compliance has been one of Secretary Richardson's top goals for the Department. When I joined the Department in October 1998, the Department was the recipient of a failing grade on its year 2000 progress from this committee, and turning around the year 2000 program was my highest priority.

As you are aware, we were able to rapidly improve our progress to a B grade in early 1999. I am pleased to report to you today that 100 percent of the Department's 420 mission-critical systems are year 2000 compliant and have approved contingency plans, and that the Department is more than 99.8 percent complete in remediating over 200,000 non-mission-critical systems, embedded chips, telecommunications systems, data exchanges and work stations.

The Department has taken a phased approach similar to other large government agencies to its year 2000 preparation activities. Phase I of our program focused on remediating the Department's 420 mission-critical systems and approximately 200,000 non-mission-critical systems.

Phase II focused on implementation of additional risk reduction and mitigation measures to help ensure that no Department mission is compromised due to year 2000 transition, and development of business continuity and zero day plans to ensure the continuation of the Department's core business processes in the event of a year 2000 related failure.

Phase III of our program is now focusing on refining our business continuity and zero day plans that we have developed. This will ensure that we have clear processes to deal with potential year 2000 induced problems and that we have identified individual roles and responsibilities for monitoring, evaluating and responding to year 2000 related events across the Department.

As I mentioned earlier, phase I of our year 2000 program is nearly 100 percent complete. During the course of our phase I year 2000 activities, the Department has also focused particular attention on the systems that protect the health and safety of the public, our workers and the environment. As of the 1st of October, all of our more than 540 health and safety-related systems are either year 2000 compliant or year 2000 ready, and we will continue to focus close attention on these systems. Furthermore, positive validation of the functionality of all operational health and safety systems will be required within 12 hours of the year 2000 transition to ensure the continued safety of the public, our workers and the environment.

Phase II of our year 2000 program is almost fully complete as well. During phase II we focused on implementation of additional

risk reduction and mitigation measures to help ensure that no departmental mission is compromised due to the year 2000 transition. We have conducted external independent verification and validation of the year 2000 remediation efforts as well as end-to-end testing for all mission-critical systems and health and safety-related systems with year 2000 date-related issues. I am pleased to report that external IV&V and end-to-end testing activities are complete for more than 99 percent of these systems.

Phase II of our program also focused on developing business continuity and zero day plans to ensure the continuation of our core business processes in the event that year 2000 failures occur. Due to the complexity and diversity of the Department's missions and activities and the recognition that the year 2000 transition poses a unique risk for each site, the Department required business continuity plans for each of our 42 sites. Sites have exercised their contingency and continuity plans during phase II of our program. Our first formal readiness exercise was conducted on April 9th and resulted in lessons learned and best practices on contingency plans. On September 8th and 9th, 42 sites participated in our second year 2000 exercise. Sites tested failure scenarios and their planned response to year 2000 related events, rehearsed their zero day procedures and tested the Department's procedures for reporting year 2000 events to our headquarters. Sites reported that the exercise was very helpful in evaluating contingency and business continuity plans and shared with my office a significant number of lessons learned.

We also sponsored two Department-wide workshops on business and continuity planning in May and October to share our year 2000 lessons learned and best practices.

We are now implementing phase III of our program, which involves refining our business continuity and zero day plans. In our review of site and business continuity plans, we have found that they have addressed many of the elements contained in the General Accounting Office's day 1 planning guidance. However, we recently received comments from the Office of Management and Budget that our headquarters business continuity plan had some weaknesses, in particular with respect to lack of prioritization of key processes, inadequate discussion of our cybersecurity efforts and insufficient detail on our procedures and responsibilities during the rollover period.

I have reviewed the plan and concur with OMB's assessment. Fortunately, with the solid foundation of contingency planning already completed, these weaknesses can be corrected quickly. I have directed actions to revise our headquarters business continuity plan by November 12th and resubmit it to OMB.

However, even after November 12th, we will continue to fine-tune our plans to reflect final staffing decisions and the results of year 2000 preparation drills within the Department and with the President's Information Coordination Center.

At the Department's headquarters our zero day procedures include the coordination of the Department of Energy as well as national and international energy sector year 2000 monitoring and reporting activities. We have developed plans with the electricity, oil and natural gas industries to receive reports of year 2000 related

events as well as to analyze potential impacts of any disruptions, including potential cybersecurity incidents.

Our Emergency Operations Center at the Forrestal Building will operate as the year 2000 command center for the collection, compilation and analysis and reporting of departmental site and energy sector year 2000 status information to the President's Information Coordination Center.

Since March 1999, my staff and I have visited more than 30 departmental sites to assess their progress toward implementing OMB and departmental guidance, to assess the compliance of the status of their systems and to share year 2000 best practices and lessons learned. I can say firsthand that all of the Department's employees are focused on year 2000 and continue to work aggressively that we will have a successful and smooth transition. In my opinion, each site is well-positioned to manage the risk potential of year 2000 related failures. Final efforts over the next 63 days will ensure that we will effectively handle any year 2000 events regardless of source.

Secretary Richardson and I are proud of the Department's efforts to ensure that 100 percent of our systems are year 2000 compliant, and we are confident in our planning efforts for the year 2000 transition. Our focus and commitment will continue as we complete our preparation efforts. I look forward to your questions. Thank you.

Mrs. MORELLA. Thank you, Mr. Gilligan.

[The prepared statement of Mr. Gilligan follows:]

Statement of John M. Gilligan
Chief Information Officer
U.S. Department of Energy

Before the

Subcommittee on Technology
Committee on Science
and
Subcommittee on Government Management, Information and Technology
Committee on Government Reform

U.S. House of Representatives

October 29, 1999

Thank you Chairman Horn, Chairwoman Morella, and Members of the Subcommittees for the opportunity to discuss the Department of Energy's contingency, business continuity and zero day plans. As Chief Information Officer (CIO) for the Department of Energy, I am responsible for the oversight, coordination, and facilitation of the Department's ongoing efforts to address Year 2000 issues.

The Department has made great progress since the last time we testified before this Subcommittee in June 1998, and I am pleased to be here to report our progress and discuss our planning activities.

Organizationally, the Department's progress is guided by a Year 2000 Council, established by the Secretary to direct the development and implementation of an overall Year 2000 plan that addresses internal Departmental activities, domestic energy efforts, and international energy activities. I co-chair the Year 2000 Council along with the Deputy Secretary of Energy, T.J.

Glauthier. In addition, a Year 2000 Steering Committee was established to implement the Council's direction and coordinate Department-wide Year 2000 compliance efforts.

The Department's Year 2000 progress is monitored through a Year 2000 Systems Database that is accessed and updated through the World Wide Web. System owners throughout the Department are responsible for submitting information to the Database on remediation of the Department's mission- and nonmission-critical systems, and health- and safety-related systems on a continual basis.

Achieving 100 percent Year 2000 compliance has been one of Secretary Richardson's top goals for the Department. When I joined the Department in October 1998, the Department was the recipient of a failing grade on its Year 2000 progress from this Committee, and turning around the Year 2000 program was my highest priority. As you are aware, we were able to rapidly improve our progress to a "B" grade in early 1999. Secretary Richardson and I are proud of the success we have achieved in preparing the Department for the transition to the Year 2000. I am pleased to report that 100 percent of the Department's 420 mission-critical systems are Year 2000 compliant. In addition, as of today, the Department is more than 99.8 percent complete in remediating nonmission-critical systems, embedded chips, telecommunications, data exchanges, and workstations.

Overall Department of Energy Year 2000 Progress

The Department has taken a phased approach, similar to other large government agencies, to its Year 2000 preparation activities. Phase I of our program focused on remediating the Department's 420 mission-critical systems, and developing the contingency plans for these systems should they experience Year 2000-related events. Phase II of our program focused on: (1) implementation of additional risk reduction and mitigation measures to help ensure that no Departmental mission is compromised due to the Year 2000 transition; and (2) development of site business continuity plans to ensure the continuation of the Department's core business processes in the event that mission- or nonmission-critical systems experience Year 2000-related failures. Phase III of our program is now focusing on refining the business continuity and zero

day plans we have developed. This will ensure that we have clear processes to deal with potential Year 2000-induced problems, and that we have identified individual roles and responsibilities for monitoring, evaluating, and responding to Year 2000-related events across the Department. Phase III also focuses on ensuring that all systems that have been remediated, reviewed and tested remain Year 2000 compliant should changes be required to these systems.

Phase I Activities

As I indicated earlier, Phase I of our Year 2000 program is nearly 100 percent complete. In addition to our success in remediating the Department's systems, contingency plans have been completed and approved for all of the Department's mission-critical systems, and health- and safety-related systems with Year 2000 date-related issues.

In accordance with the guidance my office issued in January 1999 on development of contingency plans, each of these system contingency plans describe the following: contingency alternatives that were evaluated; criteria and triggers for invoking the plan; roles and responsibilities for contingency-related actions; testing of and training on the plan; procedures for invoking and operating in contingency mode; and criteria and procedures for returning to normal operating mode. The Department also required certification of each contingency plan by senior line management.

Health- and Safety-Related Systems

During the course of our Year 2000 activities, the Department has also focused particular attention on the systems that protect the health and safety of the public, our workers, and the environment. In January 1999, the Defense Nuclear Facilities Safety Board expressed concern that the lack of emphasis on health- and safety-related systems may have been encouraging sites to expend scarce resources on bringing business systems into compliance at the expense of similar efforts for health- and safety-related systems. The Board requested that the Department identify those health- and safety-related systems at defense nuclear facilities that may have Year 2000 compliance issues, and provide the schedule for their remediation, testing, and independent

validation and verification. My office expanded the scope of this effort to also include health- and safety-related systems at non-defense nuclear facilities and high/moderate hazard non-nuclear facilities, and mandated that these systems be subject to the same formality of reporting and rigor of review and testing as mission-critical systems.

As of October 1, 1999, all of the more than 540 health- and safety-related systems are either Year 2000 compliant or Year 2000 ready. The Department will continue to focus close attention on the Year 2000 compliance of health- and safety-related systems. Furthermore, positive validation of functionality of all operational health- and safety-related systems will be required within 12 hours of the Year 2000 transition, to ensure the continued safety of the public, our workers, and the environment.

Phase II Activities

Phase II of our Year 2000 program is also almost fully complete. During Phase II, we focused on implementation of additional risk reduction and mitigation measures to help ensure that no Departmental mission is compromised due to the Year 2000 transition. In December 1998, the Department issued guidance for conducting external, independent validation and verification (IV&V) of the Year 2000 remediation process for all mission-critical systems. I am pleased to report that external IV&V activities are complete for more than 99 percent of these systems. IV&V activities remain to be completed for three mission-critical systems at our Headquarters facility, with one system scheduled for completion on October 29, 1999.

In February 1999, the Department issued guidance for conducting end-to-end testing of complete sets of interrelated systems, including mission-critical systems, associated nonmission-critical systems, and supporting technology infrastructure that are necessary for ongoing mission or business operations. I am pleased to report that end-to-end testing is complete with the exception of three mission-critical systems at our Headquarters facility and one health- and safety-related system at Oak Ridge National Laboratory. One Headquarters system is scheduled for completion on October 29, 1999.

Phase II of our program also focused on developing business continuity and zero day plans to ensure the continuation of our core business processes in the event that mission- or nonmission-critical systems experience Year 2000-related failures. Due to the complexity and diversity of the Department's missions and activities, and the recognition that the Year 2000 transition poses a unique risk for each site, the Department required business continuity plans for each of our 42 sites. Examples of the activities the Department's sites are responsible for include: overseeing the Nation's leading scientific laboratories; ensuring the safety, security, and reliability of the U.S. nuclear weapons stockpile; and managing radioactive wastes, surplus nuclear materials, and spent nuclear fuels.

The Department's guidance on business continuity planning, issued in January 1999, was based on the U.S. General Accounting Office's guidance for business continuity and contingency planning. The Department's guidance directs that site business continuity plans identify and describe core business processes and activities. The guidance also directs site business continuity plans to describe: key assumptions to continue business in the event of a Year 2000-related event; risk, vulnerability, and failure scenarios; plans to continue business in the event of Year 2000-related failures; and a zero day strategy and procedures. The Department also requires the sites to continuously review, test, and revise their business continuity and zero day plans, as necessary, and to update plans based on new information from review and testing activities.

In addition to copies of the plans themselves, we required certification of each business continuity plan by senior line management. I am pleased to report that business continuity plans are complete for each of our sites, although updates continue to be made as I will explain in a moment.

Department of Energy Year 2000 Exercises

To assist sites in exercising their plans, on April 9, 1999, the Department conducted its first formal Year 2000 readiness exercise to gather lessons learned and best practices data on contingency planning, and to establish a baseline for a subsequent Department-wide Year 2000

drill. Participating sites included Sandia National Laboratories, the Pantex Plant, the Hanford Site, Bonneville Power Administration, Oak Ridge Operations Office, and Rocky Flats Engineering and Environmental Technology Site. Some sites tested contingency plans for their most critical systems while other sites focused on emergency response capabilities in the event of a Year 2000-related failure.

On September 8-9, 1999, 42 Departmental sites participated in the first Department-wide Year 2000 drill. During the drill, sites tested various failure scenarios and their planned responses to Year 2000-related events, rehearsed their zero day procedures, and tested the Department's procedures for reporting Year 2000 events to Headquarters. Sites reported that the drill was very helpful in evaluating contingency and business continuity plans, and they shared with my office a significant number of lessons learned in the following areas: operating a Year 2000 Command Center; developing checklists to guide staff through the activities that must be accomplished before, during, and after the Year 2000 transition; monitoring the Year 2000-related events which occur; ensuring business resumption teams operate effectively; ensuring site communications during the Year 2000 transition are managed efficiently; and reporting Year 2000-related events during and after the transition. These lessons learned are now being incorporated into updates of our contingency plans, business continuity plans and zero day plans. The lessons learned were also posted to the Department's Year 2000 Home Page.

Department of Energy Lessons Learned Workshops

Furthermore, the Department has sponsored two Department-wide workshops to share Year 2000 lessons learned and best practices. On May 27-28, 1999, the first workshop was conducted to discuss lessons learned from the April 9, 1999 exercise and to assist sites in developing their contingency and business continuity plans. To further assist sites in their planning activities, the workshop also featured discussions with representatives from the private sector (including AlliedSignal, Eastman Kodak Company, Xerox Corporation, and Chevron Corporation); the electric power and telecommunications sectors; the Federal Emergency Management Agency; and Lt. General Peter Kind (ret.), Director of the President's Information Coordination Center.

A second Department-wide workshop was conducted on October 13-14, 1999 to discuss lessons learned from the September 8-9, 1999 drill, outstanding issues regarding business continuity and zero day planning activities, Year 2000 rollover reporting requirements to Headquarters, and the role of the Department's Emergency Operations Center during the rollover. More than 75 participants representing the Department's facilities Nation-wide participated in the workshop, along with representatives from the telecommunications and electric power sectors, and the Director of the President's Information Coordination Center, once again. Lessons learned from the September 8-9, 1999 drill were also posted to the Department's Year 2000 Home Page.

Phase III Activities

We are now implementing Phase III of our Year 2000 program, which involves achieving 100 percent of remediation of remaining nonmission-critical systems and refining our business continuity and zero day plans. In our review of site business continuity and zero day plans, we have found that sites are addressing many of the elements contained in the U.S. General Accounting Office's Day One Planning Guidance. For example, sites have: assessed the risk of internal and external Year 2000 failures; developed schedules for key events; developed procedures for monitoring internal and external Year 2000 events, including the establishment of Year 2000 Command Centers; developed procedures for testing key systems, including the use of infrastructure and system checklists; established business resumption teams to respond to Year 2000 events; developed recovery procedures in the event Year 2000 failures occur; developed procedures for reporting events internally and to Headquarters; developed rollover staffing plans, including leave and compensation policies; and developed rollover communications procedures.

However, we recently received comments from the Office of Management and Budget (OMB) that our Headquarters business continuity plan has significant weaknesses, in particular with respect to lack of prioritization of key processes, inadequate discussion of our cyber security efforts, and insufficient detail on our procedures and responsibilities during the rollover period. I have reviewed the plan and concur with OMB's assessment. Fortunately, with the solid foundation of contingency planning already completed, these weaknesses can be corrected quickly. I have directed actions to revise our Headquarters business continuity plan by

November 12, 1999. We will submit this update to OMB and this Subcommittee. However, I should note that even after November 12, 1999, we will continue to fine-tune our plan to reflect final staffing decisions as well as the results of Year 2000 preparation drills within the Department and with the President's Information Coordination Center.

At Department of Energy Headquarters, our zero day procedures includes the coordination of Departmental as well as energy sector Year 2000 monitoring and reporting activities. We have developed plans with the electricity, oil, and natural gas industries to receive reports of Year 2000-related events as well as to analyze the potential impacts of any disruptions. The Department's Emergency Operations Center in the Forrestal Building will operate as the Year 2000 Command Center for the collection, compilation, analysis and reporting of Departmental site and energy sector Year 2000 status information to the President's Information Coordination Center.

Phase III efforts are also focused on managing changes to the Department's systems to ensure that all systems that have been remediated, reviewed, and tested remain Year 2000 compliant should changes be required to these systems. In August 1999, my office issued configuration management guidance and required the sites to incorporate this guidance into their local configuration management processes.

Conclusion

Since March 1999, I and my staff have visited more than 30 Departmental sites to assess their progress towards implementing OMB and Departmental guidance, assess the compliance status of health- and safety-related systems, identify and share Year 2000 best practices and lessons learned, and improve Department-wide dialogue on Year 2000 issues and solutions. I can say first-hand that all of the Department's employees are focused on the Year 2000 transition and continue to work aggressively to ensure that we will have a successful transition to the Year 2000. Each site is well positioned to manage the risk of potential Year 2000-related failures and final efforts over the next 63 days will ensure that we will effectively handle any Year 2000 event regardless of the source.

Secretary Richardson and I are proud of the Department's efforts to ensure that 100 percent of our systems are Year 2000 compliant and we are confident in our planning for the Year 2000 transition. Our focus and commitment will continue as we complete our preparation efforts.

Mrs. MORELLA. Now pleased to recognize Mr. Cosgrave.

Mr. COSGRAVE. Thank you, Madam Chairwoman, and thank you, Representative Turner. I'm very happy to be here today to discuss the status of the Internal Revenue Service's Y2K business continuity and contingency plans and day 1, or as we refer to it, our end game plans. I'm joined to as well by Bob Albicker, my deputy. Mr. Albicker along with myself and our Commissioner Mr. Rossotti have all personally made this our No. 1 priority. I am also joined today by Mr. John Yost, who is our full-time executive managing this program. This is a program that he oversees consisting of approximately 100 people that are directly in his program office, plus he directly oversees the thousands of people in the Internal Revenue Service who engage in Y2K activities on a daily basis.

In order to save time, I'll refer you to our general update on the overall status of our program which is in my written testimony, and I'll focus just on contingency planning and day 1 planning.

The IRS is taking every step it can to mitigate the risks that are involved with the Y2K challenge. Two ways that the IRS is a prepared to address risks are through business continuity and contingency plans as well as day 1 plans. With respect to contingency plans, the IRS has developed 40 individual contingency plans that are aligned with the 40 most critical business processes that outline the necessary procedures to follow in the event any of our mission-critical tax-processing systems suffers a major failure.

We followed the planning format suggested to us last year by the General Accounting Office. We've completed testing all but two of those plans and have addressed GAO's suggestions from a recent review of those plans. These contingency plans concentrate on those areas that have the greatest impact on tax-processing activities in addition to areas that could be particularly affected by the Y2K problem. Because of the extensive renovation and testing work that we have performed, we do not anticipate a major failure; however, we have developed the necessary contingency plans, and we are ready in the event they are needed.

These plans address such issues as preserving files and data, how to handle personnel, and procedural issues and delivery of service until computer systems are restored. I must emphasize, however, that these plans do not provide replacement computer systems for our existing computer systems, and instead they rely on alternative manual processes. Because we have performed extensive end-to-end testing, we believe that it is highly unlikely that we will need to invoke such plans; nevertheless, we have tested them and are prepared to implement them if necessary.

As for day 1 or end game planning, the IRS has devised an end game strategy that will guide our activities during the critical rollover weekend of December 31st, 1999, through January 2, 2000. The end game strategy builds on our current information system problem reporting resolution process and identifies specific validation checklists to be used during the rollover weekend.

The plan also recognizes a unique problem facing the IRS. This problem is a result of the annual startup of the filing season, which this year occurs simultaneous with the millennium rollover weekend.

To ensure maximum risk reduction, therefore, the IRS is taking the following actions. No. 1, we are backing up and then quiescing the systems beginning at 10 p.m. On December 29th, 1999. This means the systems will be turned on, but will not be running business applications. On January 1, 2000, the systems will be brought back up to their normal operating status, this time updated with our filing season 2000 programs and validated against quality control checklists prior to the first day of business on January 3rd, 2000.

Second, we are ensuring that sites and systems are operational before the first business day of the new year by conducting a validation check of all systems end facilities at over 500 different posts of duty.

Third, we are reporting any problems that are encountered throughout the weekend through our existing problem reporting channels. All our organizations will be required to affirm that they have checked critical facilities and systems at their sites to our year 2000 command center, which will serve as the IRS nerve center during the rollover weekend. Reports will be provided to the Commissioner, myself, Mr. Albicker, et cetera, on a regular basis as well as to the Department of Treasury every 4 hours during the rollover weekend.

Please keep in mind the successful rollover weekend is just a small part, however, of meeting the Y2K challenge. Problems for us may arise well into the new year impacting the filing season. For example, our computers may generate erroneous notices to taxpayers as late as March or April. However, we have procedures in place to resolve any problems that arise, including scanning for large erroneous dollar amounts and dates specifying 1900. Additionally, the command center will continue to operate through April 15th, 2000, or longer if necessary, depending on the status of the filing season. We will rehearse our rollover weekend plan on November 20th, 1999, to prepare participants for this event and to fine-tune our end game strategy.

In conclusion, we're confident the IRS will be capable of fulfilling its mission in the year 2000 and beyond. While we recognize that risks still exist, we believe we are taking the necessary steps to address them. Thank you.

Mrs. MORELLA. Thank you, Mr. Cosgrave.

[The prepared statement of Mr. Cosgrave follows:]

**STATEMENT OF PAUL J. COSGRAVE
CHIEF INFORMATION OFFICER OF THE INTERNAL REVENUE SERVICE
BEFORE
THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND
TECHNOLOGY**

October 29, 1999

Mr. Chairman and Distinguished Members of the Committee:

Thank you for the opportunity to discuss the status of the Internal Revenue Service's (IRS') Business Continuity and Contingency plans and Day One, or End Game, plans. Before addressing these topics, I want to quickly update you on our progress towards meeting the Year 2000 (Y2k) challenge.

- Approximately 99% of our 135 mission critical application and telecommunication systems are now compliant, have been tested, and implemented in production.
- The vast majority of our hardware and telecommunications equipment has been made compliant. Any remaining components connected to our network are scheduled to be compliant before the end of year.
- We have obtained signed certifications from all of our 1,434 external trading partners agreeing to our Y2k compliant date format for data exchange. We have exchanged test data with our trading partners for all but two of our files requiring conversion. We are also testing file exchanges with our 12 key external trading partners in a date-forward environment.
- We have already conducted four successful End-to-End tests that have included applications, hardware, telecommunications, and commercial software products. We conducted the tests using both current and Year 2000 dates. Our final end-to-end test, using our programs for the upcoming filing season, is well underway.
- Most of our Y2k compliant systems were used during the 1999 Filing Season, which was one of the most successful in recent history.

The IRS is taking every step it can to mitigate the risks that are involved with the Y2k challenge. Two ways that the IRS has prepared to address risk are through Business Continuity and Contingency Plans and Day One Plans.

Contingency Plans

The IRS has developed contingency plans that outline the necessary procedures to follow in the event that any of our mission-critical tax processing systems suffers major failure. We have completed testing on all but two of these plans and have addressed GAO's suggestions from a recent report on our contingency plans. These

addressed GAO's suggestions from a recent report on our contingency plans. These contingency plans concentrate on those areas that have the greatest impact on tax processing activities in addition to areas that could be particularly affected by the Y2k problem. While we don't anticipate a major failure, we have the necessary plans ready in the event they are needed.

These plans address such issues as preserving files and data; how to handle personnel and procedural issues; and delivery of service until our computer systems are restored. I must emphasize that these plans do not provide replacement computer systems for our existing computer systems.

For example, if we were unable to automatically issue refunds, our contingency plans do not provide alternate information systems to issue refunds but call for manually issuing refunds as a stopgap measure. How the plan would be implemented would depend on the time of year and the number of refund returns in our inventory. For example, a failure in January, when inventories are relatively low, would give us more time to invoke our contingency plan. At peak processing times, we would need to invoke our contingency plan within days of the systems failure in order to process the largest number of manual refunds within the 45-day interest-free period. In this scenario we would issue manual refunds to those taxpayers "most in need", i.e., to taxpayers meeting hardship criteria, and to taxpayers filing refund returns who have adjusted gross incomes beginning with \$10,000 or less and increasing in increments of \$5,000 depending on our capability for issuing manual refunds.

However, I would like to emphasize that our returns processing systems, both paper and electronic, have been made Y2k compliant and have successfully completed initial End-to-End testing.

End Game Planning

The IRS has also devised a Day One or "End Game" strategy that will guide our activities during the critical "Roll-Over" weekend of December 31, 1999, through January 2, 2000. The End Game strategy builds upon our current information system problem reporting and resolution process and identifies specific validation checklists to be used during the rollover period. The IRS plans to:

- Backup and then "quiesce" the systems beginning at 10:00 p.m. on December 29, 1999. This means the systems will be turned on, but will not be running business applications. On January 1, 2000, the systems will be brought back up to their normal operating status, updated with our filing season 2000 programs, and validated against quality control checklists prior to our first business day on January 3, 2000.

- Ensure that sites and systems are operational before the first business day of the Year 2000 by conducting a validation check of all systems and facilities at every post of duty except a small percentage of our smaller, remote locations which would have limited impact on the taxpaying public.
- Report any problems that are encountered through our existing problem reporting channels. Organizations will also be required to affirm that they have checked critical facilities and systems at their sites to our Year 2000 Command Center, which will serve as the IRS' nerve center during the rollover period. Reports will be provided to the Commissioner and to the Department of Treasury every four hours during the rollover weekend.

Please keep in mind that a successful rollover weekend is just a small part of meeting the Y2k challenge. Problems may arise well into the new year, impacting the filing season. For example, we may generate erroneous notices to taxpayers. However, we have procedures in place to resolve any problems that arise. Additionally, the Command Center will continue to operate through March 1999 or longer if necessary, depending on the status of the filing season. One of the Command Center's products will be detailed in a "Health of the Organization Report" that will help us monitor the overall condition of IRS operations throughout the filing season.

We will "rehearse" our Roll-Over Weekend plan on November 20, 1999, to prepare participants for this event and to fine-tune our End Game strategy.

CONCLUSION

In conclusion, we are confident that the IRS will be capable of fulfilling its mission in the Year 2000 and beyond. While we recognize that risks still exist, we believe that we are taking the steps necessary to address them. As we continue our end game planning and closely monitor our schedule and progress, we will apprise the Committee of any Year 2000-related errors we experience, their impact on taxpayers, and our actions to alleviate any added taxpayer burden. I thank you again for the opportunity to discuss the IRS' Y2k efforts and appreciate the continued support of the Committee.

Mrs. MORELLA. I'm now pleased to recognize Mr. Lorentz of the Postal Service.

Mr. LORENTZ. Good morning, Chairwoman Morella and Representative Turner. With me this morning are Nick Barranca, who is the Vice President of Operations Planning, and Rick Weirich, who is our Vice President of Information Systems and our Chief Information Officer.

I'm pleased to report this morning that we have completed all the technical work on our mission-critical systems, including independent verification, testing, and implementation of a system freeze.

We began testing our mail processing equipment in 1998 and extended to other sites last year. In August, at our Merrifield northern Virginia site, we started a 6-week test of critical mail processing equipment. This equipment ran continuously in a year 2000 calendar mode, in a live processing environment, testing all equipment types and all mail types. This facility handles 5 million pieces of mail a day, and we have experienced no problems.

We have also created plans to protect against potential disruptions of other systems and processes. We respond to disruptions every day. In the last 2 weeks we've dealt with Hurricane Irene in Florida and the Hector Mines earthquake in Los Angeles. Locally, last year's storm in Montgomery County left 48 of 60 Montgomery County delivery units that were without power, and we delivered mail. I know in my home in Bethesda, all 3 days that we were without power, I got normal mail delivery even though I had to walk outside to read it.

Our business continuity plans and contingency plans are building on our experience and formalizing our response to disruption, both internal and external. Our continuity plans deal with the external infrastructure. Our internal contingency component plans deal with the infrastructure all the way from timekeeping to mail processing. Our plans includes working with customers, with other Federal agencies, and particularly with agencies that deliver benefit payments to the American people.

We anticipate that some of the mailers may divert electronic communications to hard copy mail. With that in mind, we're holding the enlarged infrastructure that we normally put in place for the holiday season, including staff, transportation, and sorting capability, through January.

So what is day 1 going to look like for us? First of all, it's going to be business as usual, but prepared for whatever might occur. Robust day 1 plans are developed to preempt any kind of problems. Systems are in place to identify, report, track, resolve any Y2K issues.

To communicate internally, with customers, with employees and with all stakeholders, we have emergency communication capability. Our network operations center has been converted into an internal ICC. Our national and field operations centers will operate 24 by 7 to assess USPS status and provide resource and decision support.

Our day 1 activities will also involve onsite participation at the President's Council's Information Coordination Center and Joint Public Information Center. At a recent meeting of the President's

Council on Year 2000, Chairman John Koskinen recognized us as the early warning beacon. We are the only organization that goes everywhere, every day, and we'll be very happy to perform in that role.

Our plans have focused on Y2K as a business problem. And we have three very simple goals: To protect our customers by delivering the mail, to protect our employees' safety and pay; and to protect our business by collecting the money due and paying what we owe.

We also have a heightened awareness to security problems. We have engaged reputable contractors with full security background checks and clearances, and we are providing instructions to the field to protect against any viruses. In a forward-looking mode, we're also working with the President's Council on cyber assurance issues. Protecting our work protects America's mail.

We believe that the United States Postal Service is ready, and I look forward to answering your questions.

Mrs. MORELLA. Thank you, Mr. Lorentz.

[The prepared statement of Mr. Lorentz follows:]



**STATEMENT OF NORMAN E. LORENTZ
SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER
UNITED STATES POSTAL SERVICE**

**BEFORE A JOINT HEARING OF THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
OF THE
COMMITTEE ON GOVERNMENT REFORM,
AND THE
SUBCOMMITTEE ON TECHNOLOGY
OF THE
COMMITTEE ON SCIENCE**

**HOUSE OF REPRESENTATIVES
OCTOBER 29, 1999**

Good morning, Chairman Horn, Chairwoman Morella, and subcommittee members.

On behalf of the United States Postal Service and its 800,000 employees, I am pleased to have this opportunity to report again on our progress in meeting the challenge of the Year 2000 computer problem. With me today are Nicholas Barranca, Vice President of Operations Planning, and Richard Weirich, Vice President of Information Systems.

Since we last met in February, the Postal Service has been busy—very busy. We welcome today's opportunity to bring you up to date on our activities.

The American people, and the businesses and government agencies *they* rely on, will be relying on the Postal Service—perhaps more than ever—as we close the door on the twentieth century and enter the twenty first.

It is our job to be ready for them—and we will be. Whether it is the challenge of traditionally heavy year-end mail volumes, or those extraordinary volumes increased by the potential diversion of electronic communications into the postal mailstream, we have worked to prepare our system for business as usual come the new year.

We are aggressively managing our efforts against a structured and thorough work plan that assigns accountability, sets specific goals, and measures progress against those goals.

And our progress has been significant. We have remediated—or fixed—all mission-critical systems. Each has also been tested and independently verified as capable of properly operating to, through, and beyond the Year 2000 date change.

To maintain the stability of our remediated systems, we have placed a freeze on virtually all system changes through the end of March.

For critical mail processing equipment, successful field tests were conducted at major facilities in each of our eleven geographic areas. This involved sorting "live" mail, in an actual operating environment, with system clocks turned ahead to Year 2000 dates.

On August 30, we began an extended "fail safe" test of automated processing equipment at our huge Northern Virginia processing facility, where equipment clocks were turned forward to December 30 and operated in a Year 2000 calendar mode for six weeks.

For most of us, August 31 was just another night. But for the equipment in our Northern Virginia plant, it was New Year's Eve. By all reports, the celebration was quiet, there was no run on aspirin the next morning, and the mail continued to move—for the full six weeks—without a hitch.

At the same time, we also passed two key "early warning" dates: September 9th—nine-nine-ninety-nine—and September 11, the beginning of the Postal Service's fiscal year 2000. In some programs, the date field represented by a string of four nines could have been read as an "end program" command. Similarly, the representation of the fiscal year by the two digits "zero-zero" could have presented problems similar to those threatened by the calendar year rollover. However, our system work included both dates and neither presented us with any operational problems. In fact, we experienced our smoothest fiscal year rollover in five years.

But our Year 2000 initiative is about more than simply computers. Like other organizations, the Postal Service relies on other business partners and suppliers to help us connect more than 130 million households and businesses to each other.

While we have assessed the readiness of our key suppliers and tested electronic interfaces with critical partners, we must anticipate that some external disruption could affect our operations. With this in mind, we have identified our critical business processes—such as postage payment, and the acceptance, processing, transportation, and delivery of mail—and weighed them against a catalog of "failure scenarios," essentially, external events that could interrupt our business processes.

This exercise resulted in the creation of business continuity plans—a series of strategies to help us work through disruptions to elements of our external support infrastructure, such as ground and air transportation, telecommunications, and utilities. The basic continuity plans were then shared with our field units for customization, as appropriate, to reflect specific local conditions. For example, in the event of an airport closure, field operations officials will identify the best alternative transportation and routing for mail to and from that area.

In developing continuity plans, the Postal Service has also worked very closely with its large customers to learn if they are changing their regular mailing plans. This could involve entering different mail volumes at different locations or at different times. Knowing this information will help us take the right steps to accommodate business mailers' needs. Similarly, through our work with the President's Council on Year 2000 Conversion, we have identified and planned for the mailing needs of other federal agencies, particularly in the area of benefit payments for millions of Americans.

We have also developed component contingency plans to provide "work arounds" for critical, internal systems. Generally, these are prescriptive and require no localization. Because of the uniformity of our equipment, the same plan fits the same component, no matter where it is located. They can also be extremely simple. For example, if equipment that makes sorting case labels is unavailable, the plan calls for writing the casing information on a blank label.

Neither business continuity plans nor component contingency plans reinvent the postal wheel. Rather, they represent the formalization of our everyday experience of coping with local, regional, and national disruptions to some element of our operations.

Contingency planning is something we do as a matter of course. On any given day, due to our sheer size and huge inventory of equipment, a local office may experience—and must overcome—problems that affect sorting, retail, or vending equipment. At the regional level, severe weather conditions often interrupt ground and air transportation or other critical support services, requiring our people to develop and implement alternative ways of keeping the mail moving.

Our Year 2000 continuity and contingency plans have been circulated throughout the organization, with testing and rehearsal of selected plans occurring through late summer and into the fall. We will also be conducting a large scale "dress rehearsal" in November to test our response readiness to potential year 2000 disruptions.

For the "dress rehearsal," field units will be presented with various problems and asked to select the appropriate response. Our goal is to prepare our people to make the right decisions in a challenging environment but one that does not result in disruption to the nation's mailstream.

The final element of our Year 2000 program is Recovery Management. Like contingency planning, recovery management builds on our experience in managing through—and around—the speed bumps and roadblocks we experience every day. In just the last two weeks, we have operated through hurricanes in the southeast and earthquakes in the southwest. The bottom line is that we manage recovery—somewhere—almost every day.

Recovery Management planning identifies the structure and processes our people will use to preempt, identify, report, track, and resolve Year 2000-related problems. At all levels of the organization, we will base our activities on an enhanced version of the reporting and response structures that we use to address problems every day. However, this will be overlaid with a structured reporting process to help us assess the overall status of the Postal Service—both nationally and regionally.

Key functional areas will operate command and control centers to provide the support and response capability required within their respective organizations. Here in Washington, our National Operations Center, which monitors system status nationwide, will operate around the clock from December 30 through January 4. It will be staffed by representatives of Information Systems, the Postal Inspection Service, Engineering, Operations, and Communications. Similar operations centers will be staffed at our area offices.

The National Operations Center models the President's Council on Year 2000 Conversion's Information Coordination Center in purpose and function. It will assess and report organizational status throughout the organization, and provide resource and decision support for issues that must be escalated to Headquarters level. It will also serve as the voice of the Postal Service, communicating with internal and external stakeholders, including employees, management, government, customers, and the media.

Postal Service representatives will also be on site at the Federal Government's Information Coordination Center. They will share status information about our organization that will contribute to a broader picture of the nation's overall status. Our representatives will also obtain critical information about national and international infrastructure issues that could affect postal operations, contributing to our ability to respond quickly and effectively.

In preparation for our "Day One" activities, we have also provided our operational and support organizations with useful and specific information that will help in their successful preparation for the transition to the year 2000. This includes a Year 2000 planning calendar that organizes preemptive and preparatory activities by action date, and information resources for communicating with customers and employees.

As I mentioned earlier, the Postal Service has had a very busy year. And, with only 63 days remaining until the new year, we will continue to be busy—testing and refining plans, sharing information, and working to protect the world's best—and largest—postal system.

The United States Postal Service exists for only one reason—to bind the nation together through universal mail service. Our efforts in preparing for the Year 2000 have only one goal—to deliver on that promise. The Postal Service will be ready!

Thank you very much. We will be pleased to answer any questions you may have.

#

Mrs. MORELLA. I won't ask you about whether those ponies are ready. But it's interesting, as I scrutinized the panel, that it was planned that we picked those five agencies that—I don't mean to prioritize as the most important, but have the greatest influence or effect on our American economy and our Nation: Social Security, Department of Defense, Department of Energy, Internal Revenue Service and the Postal Service. And I appreciate your being here. I think I'll try to ask each of you maybe one question and then see if it evolves into others.

First of all, as I mentioned, Mr. Dyer, I commend you on having started looking to Y2K and what needed to be done back in 1989. We have recognized your leadership in this regard. And yet what if the computers fail; what specific plans does Social Security Administration have to ensure that its millions of recipients receive their Social Security checks? I mean, you are very close to the people.

Mr. DYER. We are, of course, concerned, and we are committed to delivering those checks. The Supplemental Security Income checks go out before the end of the year. They'll be issued on Thursday. So they're before we turn over. The regular Title II or Social Security checks, they go out on Monday. We have worked very closely with the Federal Reserve, the Department of Treasury and the Postal Service to assure that we can get the direct deposit or the checks that go through mail there on time. We're positioning the checks and the tapes in advance. We worked through and tested it from beginning to end.

So we're very confident that the payments are going to go. If, however, some areas, checks do not reach it, we have fall-back plans. If it's with a financial institution with a direct deposit, where the bank fails to be able to push through the direct deposit, we would find another bank that could do the direct deposit, and if not, we would work out how to get a paper check to the individual.

If it's in terms of the paper checks, we're very confident because we've worked out contingency plans with the Postal Service, and, as you know, in hurricanes and other disasters, we've always been able with the Postal Service to be right there onsite and get the checks to the people.

Mrs. MORELLA. So we can tell the viewers, listeners, our constituents, do not worry, the check is in the mail or you will get the check.

Mr. DYER. You will get your check, or you will get your direct deposit in your bank.

Mrs. MORELLA. Exactly. And we will be continuing to watch to make sure that that you can continue that way, and feel confident that you will.

With regard to, Dr. Langston, the Department of Defense, it really is—you're really the largest Federal entity in terms of personnel and Y2K mission-critical systems. I think you have like 37 percent of all the mission-critical systems are within the Department of Defense. Consequently your mission-critical contingency plans or your contingency plans for all of your missions have got to be very detailed. I wonder how many personnel that you're planning to have ready on December 31st to implement the day 1 plan? And do you

have any idea what the cost might be to implement your day 1 plan? Have you estimated?

Mr. LANGSTON. I thought about both of those questions when you asked them earlier. In terms of our contingency planning personnel operations, as I mentioned earlier, we are, of course, on duty 24 hours a day, 7 days a week, around the world. That operation is actually just being augmented by folks that support the year 2000 systems. So in other words, we have compiled detailed lists of technical experts or operational experts that support any of the contingency plans; those names, telephone numbers, all the contact points have been established. We are establishing augmentation cells for the year 2000 to support any of our normal watch stations or command centers, if you will, in major command areas like our unified commanders, and like our Pentagon command center, and for the service command centers as well as the Joint Chiefs.

In terms of my—I do not have an actual number for you. My estimate is that we're operating—we will be operating 5 to 10 percent more personnel in a duty—nonduty status than we normally operate. In terms of how many—how much money we have spent to support contingency planning, we, of course, continue to report to OMB the expenditures for Y2K. Our most recent report, I believe, specified that we will spend by the time we're through with this transition phase about \$3.6 billion on the year 2000. My estimate, although I do not have this broken out exactly in the reports, is that approximately 25 percent of our effort has been toward consequence management, contingency planning or preparation other than the remediation and testing events that we have conducted.

Mrs. MORELLA. Do you think that money, that you could find that within your budget?

Mr. LANGSTON. Could we have found that money?

Mrs. MORELLA. Have you thought about finding that money within the budget that's already been allocated?

Mr. LANGSTON. Well, of that \$3.6 billion, all of it was DOD money with the exception of the \$1.1 billion augmentation budget that we were provided. We have been committed all along to doing whatever we had to do to find the money to support this. This has been Dr. Hamre and Secretary Cohen's No. 1 priority for the Department other than national security.

Mrs. MORELLA. So your financial planning has been done satisfactorily up to this point.

Mr. LANGSTON. Yes, ma'am.

Mrs. MORELLA. All right. I'm interested in how we connect with Russia and what we are doing to help Russia. I know you've got the command station that you mentioned in Colorado and in the Denver area. When will that U.S.-Russia strategic command be ready?

Mr. LANGSTON. It's actually ready now. And as I mentioned, we will have Russian people arriving on the 22nd of December and staying in this operational sense through the 15th. We have been conducting a series of meetings with Russia, both in Russia and in the United States. The most recent meeting was on the 18th through the 21st of October in Russia. And we will continue to interact with them as much as possible to do everything we can to prepare for this event.

Mrs. MORELLA. Have they been cooperating?

Mr. LANGSTON. Yes, ma'am. They have been very cooperative with the exception of the period of time through the Kosovo operations when we were, for political reasons, stopped for this activity.

Mrs. MORELLA. Do you have any interface with the other—as they call them, the NIS, the newly emerging States? That would be like Georgia, Armenia, Azerbaijan.

Mr. LANGSTON. We have not had extra activity associated with those folks. We have had a large host nation support interaction ongoing. We cooperate and work with the State Department on that, and we have also been working with all of our NATO allies in support of their preparations for these events. And our local base commanders, wherever they reside in foreign countries, are working with those local organizations to ensure the support or verify as much as possible how much support we will get through this period of time. That has been part of our host Nation support activity.

Mrs. MORELLA. You have a tremendous task, and I commend you and want you to know that we really want to help whenever we can and stay with it.

With regard to Mr. Gilligan and Energy, I'm curious. This afternoon I'm going to be going to the Nuclear Regulatory Commission for the swearing in of the new Director. And I'm just wondering how do you, Department of Energy, coordinate with the Nuclear Regulatory Commission to ensure that our nuclear power plants will be ready for the year 2000? I know that it's not within your jurisdiction, NRC specifically, but your interconnection?

Mr. GILLIGAN. The Nuclear Regulatory Commission, as you know, has the regulatory legal authority over the domestic nuclear power plants, and so they have been issuing guidance, and that guidance has been implemented within the plants. We have been monitoring those activities through two means: One, we have a relationship with the North American Electric Reliability Council, NERC, which has been assigned domestically for electricity and to coordinate the Y2K activities.

As the nuclear plants are part of our electricity generators, they are being monitored through the reporting activities, and those activities are then reported to us.

Second, we have established a relationship, we actually have an ongoing relationship, with the Nuclear Regulatory Commission. We have participation in their emergency operations facilities, and we are continuing to track their progress, and we expect that one of the key partnerships that we will have during the rollover will be with their command centers, as well as, we will have Nuclear Regulatory Commission participation at our energy sector desk in the Information Coordination Center.

Mrs. MORELLA. I think you also said in your statement that you have found that you are all 100 percent compliant?

Mr. GILLIGAN. For our mission-critical and health and safety systems, that's correct.

Mrs. MORELLA. That's great. How about your liaison with contractors, would you like to comment on that?

Mr. GILLIGAN. Sure. As you may know, the Department of Energy is structured where we have very heavy reliance on contrac-

tors. So of our roughly 120,000 employees, about 110,000 are contractors. And so we have an in-house, if you will, body of contractors, and it has been those contractors that we rely on day in and day out who have done the vast majority of our Y2K remediation activities. We have brought in external independent verification and validation contractors to help oversee the process to ensure that we were getting objectivity, and that's worked very well. We only have isolated incidents where we have brought in new contractors for the purpose of doing Y2K remediation at our sites.

Mrs. MORELLA. So you feel the selection of your validation crew is adequate for total assurance that the contractors are following through?

Mr. GILLIGAN. We believe that this was critical to our process, because of the potential danger of a contractor who does this work day in and day out potentially missing something, that we require the external and independent verification and validation. We defined a process for conducting that. We defined a reporting process that went through line management at each of our sites for each of our mission-critical and health and safety systems. So this became a very important part of our confidence building through the line management chain that our remediation activities had been done properly. And I'm pleased to report that we found very few discrepancies or items of concern in our independent verification and validation.

Mrs. MORELLA. I'm glad to hear that.

Mr. Turner's been very kind to let me continue to ask each of you a question, then I'll turn to him.

And, Mr. Cosgrave, you knew—you knew we were coming to you with regard to what I had posed to the first panel and that letter that was written to Bill Archer on October 15th that you reported that the quality of your computer systems' inventory currently poses a high risk to the Y2K effort. You addressed it a little bit in your statement, your oral statement. I just wondered if you would give us an update of the status to complete the inventory process. I wonder when it will be completed, why did it take so long. I mean, were there some glitches here that if could you go back you would have changed? And how would you adequately plan contingencies in the event of—given the fact that you're still determining the systems that you now have, how would you adequately plan contingencies in the event of a Y2K problem or failure?

Mr. COSGRAVE. Thank you for asking the question. Let me try to answer the questions. Let me try to hit them all. I need to first explain some background on this.

Tracking inventory in a large enterprise such as the Internal Revenue Service is a major problem for any large enterprise. It's significantly more difficult for us because of the highly decentralized nature of the way the Internal Revenue Service has historically operated and, frankly, because of the level of detail at which we are now trying to track this data.

Based on my 25 years of working in private industry, I don't think the problem is different for anybody else on the panel or anybody else in private industry. It is just made more difficult at the IRS by the highly decentralized nature of our operations. To give you an example of how complicated this is, we have recognized this

problem as a material weakness in the Internal Revenue Service dating back to 1984. So it has been recognized as a 15-year-old problem we still haven't been able to solve.

Specifically for Y2K purposes we are tracking about 800,000 items in our inventory, 800,000. To give you an example, we would track every PC, every piece of equipment, every piece of software that is on that equipment, and for Y2K purposes we have to track every release version of every piece of software that's on every computer. So it gets extremely detailed when you're up to 800,000 individual items.

However, maybe this is a good example of where Y2K has finally given us the push to solve a long-standing problem. In fact, prior to starting our Y2K program, we were probably in many cases at best 50 percent accurate in our inventories. I can report to you today that based on some of our most recent tests, we're now over the 90 percent level. However, there still are issues.

We have a three-step process in place right now to bring this together and make sure it's in place not only for January 1st, but also for October 1st, which was a critical date for establishing a year-end evaluation for the fiscal year for financial purposes. So we're working both those problems simultaneously for the financial records as well as for the Y2K inventory.

We are addressing the problem now with three specific actions. We're doing on-the-ground, wall-to-wall inventories in all our computing centers, all our service centers and 11 of our 33 districts. We, furthermore, are doing independent verification and validation of those results here at the national office for all our largest computers, our tier 1, tier 2 computers, and doing detailed comparisons between what's recorded from the inventory and what we have actually on the floor.

And then third, we have started the independent audit and readiness verification, which is also going out to all our computer centers, all our service centers, and, again, 13 of the 33 districts, different ones this time, to essentially make sure that we, in fact, can validate, get as close as 100 percent.

What's different now most importantly is that the CIO is now 100 percent responsible for the inventory. That was not the case prior to my arrival last July. The inventory responsibility was a decentralized responsibility, and as a result we were not able to adequately get our hands around this. Longer term the solution to this problem will clearly be automatic tracking, which we're in the process of implementing so that, in fact, we can automatically record everything that's on our network.

Mrs. MORELLA. Could—I know the people who are listening and watching would like to know could IRS computer problems result in more citizens being audited?

Mr. COSGRAVE. I'm not sure that that would be a concern. I think from the perspective of the individual person looking at this testimony, I would think their major concern would be probably around whether they're going to get their refund on time. So we're implementing special processes, much like the ones that Social Security described, to make sure that refund checks are processed on a timely basis. Of course, our process for sending out refunds would start toward the end of January rather than the beginning of Janu-

ary. So we have a little more ample time to make sure that everything is working properly. But we go through exactly the same processes that SSA described in working with FMS and the Postal Office to make sure that those checks get distributed. So I think probably that is the thing that your viewers would be most concerned about.

Mrs. MORELLA. Is there anything that the public should do to protect themselves against possible IRS computer failure?

Mr. COSGRAVE. What the public needs to do is what the tax preparers would recommend they do every year, and that is keep tax records at home. I mean, they will need tax records if, in fact, they are summoned in for an examination, and therefore they need to keep good, accurate records like they would any other year.

Mrs. MORELLA. Thank you. I'm going to ask unanimous consent that the letter from IRS sent to Chairman Archer be included in the record. Without objection, it will be so ordered. Thank you.

[The information referred to follows:]



COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

October 15, 1999

The Honorable Bill Archer
Chairman, Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for the opportunity to address the concerns raised in your letter dated September 15, 1999, about the readiness of the Internal Revenue Service (IRS) for the Year 2000 (Y2K). As I have stated before, the Y2K problem is one of my top priorities. We have devoted significant resources to this issue since 1996, and we continue to address the problem daily. While there is always an element of risk, and we do have some trouble spots in our effort towards becoming Y2K compliant, I am confident we will be prepared for the Year 2000. If problems surface when the clocks roll over into the new year, we will be prepared to deal with them before they begin to affect taxpayers.

Inventory

The quality of the IRS's inventory currently poses a high risk to the Y2K effort. We have taken significant actions to improve the accuracy of the inventory. The three most notable actions are the Wall-to-Wall Inventory, the Independent Validation and Verification (IV&V), and the Independent Audit and Readiness Verification (IARV).

Before I discuss these actions, I want to report that the results of the visits to the Atlanta and Philadelphia Service Centers and the Philadelphia and Pittsburgh field offices revealed both strengths and weaknesses in the inventory. The results verified that a large number of records for equipment that we removed from production remained in the inventory database. On a positive note, the results also indicated that we properly recorded most of the equipment in production. Specifically, we had recorded better than 91 percent of the items in production at the Atlanta and Philadelphia Service Centers in the database.

Wall-to-Wall Inventory. Each Service Center, each Computing Center, and selected District Offices will undergo a Wall-to-Wall Inventory prior to December 31, 1999. This effort involves reconciling the inventory in production versus the inventory database at each of the sites. We chose the District Offices that will have the greatest impact on taxpayers to undergo the Wall-to-Wall Inventory.

IV & V: We contracted with Northrop-Grumman to review our Commercial Off-the-Shelf products for Y2K compliance. They have performed their initial review of the 11,475 unique products currently in the inventory database and have completed their verification and validation process for almost 7,000 of these products. We are researching and tracking potential discrepancies detected by Northrop-Grumman's analysis to ensure we confirm and resolve errors.

IARV: We recently completed 26 IARV visits. We visited all Service Centers, all Computing Centers, and selected District Offices. The visits assessed each site's readiness for the Year 2000. Auditors examined the mini-computer and personal computer hardware, telecommunications equipment, commercial software, and custom developed applications in use at the sites. They also verified the equipment was Y2K compliant and correctly recorded in our national inventory database. They also ensured that sufficient policies and procedures were in place to ensure that the inventory is kept current and accurate.

Contingency Planning

As you mentioned in your letter, the GAO has acknowledged the significant progress we have made with our contingency plans that outline what we would do if systems fail. However, I want to emphasize that our returns processing systems, both paper and electronic, have been made Y2K compliant and have successfully completed initial End-to-End testing.

If our returns processing systems fail, our contingency plans do not provide alternate information systems to process returns or issue refunds but call for manually issuing refunds as a stopgap measure. When we would decide to issue manual refunds would depend on the time of year and the number of refund returns in our inventory. For example, a failure in January, when inventories are relatively low, would give us more time to invoke our contingency plan. At peak processing times, we would need to invoke our contingency plan within days of the event in order to process the largest number of manual refunds within the 45-day interest-free period.

Combined, the ten Service Centers can produce a maximum of 6,000 to 10,000 manual refunds daily. In a failure scenario, we would issue manuals to those taxpayers "most in need." Taxpayers "most in need" would meet the following criteria in priority order:

- Taxpayers meeting "hardship criteria," e.g., having an approved Form 911, Application for Taxpayer Assistance Order.
- Taxpayers filing refund returns who have adjusted gross incomes beginning with \$10,000 or less and increasing in increments of \$5,000 depending on the capability for issuing manual refunds.

End-to-End Testing

We have already conducted four successful End-to-End tests that have included applications, hardware, telecommunications, and third party products. We conducted the tests using current and Year 2000 dates. Additionally, we used these systems during the 1999 filing season, which was one of the most successful in recent history. The final End-to-End test will incorporate the changes we have made to our systems in preparation for the 2000 filing season. These systems have largely completed their standard filing season testing. Therefore, we anticipate that the final End-to-End test will run smoothly.

We are on schedule to complete the final End-to-End test in December. Some projects are behind schedule in development and systems acceptability testing and may not be ready at the *beginning* of the End-to-End test. These represent less than 10 percent of the projects that are a part of the test. However, we will be able to incorporate these projects into the End-to-End test without modifying the overall completion date.

Additionally, normal production startup activities use a procedure to "hub" all programs at one processing site before initiating the programs at all sites. This provides an additional opportunity to identify and correct problems before they are introduced to the full production environment.

Of course, we will assign significant resources to correct any problems that may be uncovered during End-to-End testing. Once corrected, we can re-test these systems during a small window of opportunity between the scheduled conclusion of the End-to-End test and January 1, 2000. We will monitor these systems, and any others that may be of concern, during the rollover weekend to ensure their correct startup and operation.

Penalties/Interest Abatement

We are studying how we will implement Penalty Relief for individuals and small businesses who attempt to file and pay in good faith but are prevented from doing so because of a Y2K problem beyond their control. We are preparing a report that addresses the following key issues:

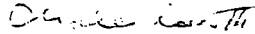
- Reasonable efforts taxpayers make to become Y2K compliant;
- Disaster relief provisions (declarations of disaster or emergencies by the President);
- Alternative methods of payment of outstanding liabilities;
- Penalty relief in the case of reasonable cause; and
- A communications strategy to taxpayers.

Funding Status

Because the IRS received the President's proposed FY2000 Century Date Change (CDC) budget of \$123.4 million, we will have the requisite funding to become Y2K compliant by December 31, 1999. We do not foresee additional CDC funding requests for FY 2001 and beyond, nor has any such funding request been made in the IRS' initial CDC budget submission to the Treasury Department.

I hope my answers to your queries bolster your confidence in the IRS' ability to fulfill its mission into the Year 2000 and beyond. I thank you again for the opportunity to discuss the IRS' Y2K efforts with you and appreciate your continued support. If you have any further questions, please contact me at (202) 622-9511 or Paul Cosgrave, Chief Information Officer, at (202) 822-6800.

Sincerely,



Charles O. Rossotti

Mrs. MORELLA. Now for our Postal Service. At the hearing we had back in February of this year, Mr. Lorentz, you stated that the Postal Service's contingency plan was itself. And you kind of implied that today, too; that is, there is no other organization that can deliver mail in the event of unforeseen computer failures. And you say that mail will be delivered. I wonder who can deliver the mail in the event of unforeseen computer problems? And what are your main contingency plan risks, and what have you done then to mitigate your risks?

Mr. LORENTZ. The answer to the first issue is that for our own computer systems, we have focused on the severe and critical systems. For severe and critical systems, 33 percent of the functionality has already been tested with the fiscal year turn. We have experienced no operational failures at all. We've had 17 anomalies where the wrong data appeared on a screen or perhaps printed on a piece of paper, but no operational failures whatsoever in the system so far. And as I mentioned previously, we have tested our mail processing equipment in many locations under full volume, so we're very confident that those systems have been mitigated. We are the ultimate contingency.

So how will the mail be delivered? It wasn't too many years ago that our sortation and delivery was done manually with little mechanization. We have not forgotten those tool sets. I think the major risk that we have that we've also addressed in our continuity plans is loss of major infrastructure capabilities, power, telecommunications, et cetera. We have detailed plans in place to mitigate that. We do that as a normal manner of course. We just did it in Florida. We just did it in North Carolina. We had to do it in L.A. We're used to working with without those capabilities. So we can do that just like anyone else. If it was a more of a general failure, that would be the highest risk.

Mrs. MORELLA. And you would probably take care of that by manually making sure the mail is—

Mr. LORENTZ. Absolutely.

Mrs. MORELLA [continuing]. Delivered. I thank you.

I now would like to turn to the distinguished ranking member, Mr. Turner, for his turn at any questioning or statements.

Mr. TURNER. Thank you, Madam Chairman.

You know, I've often wondered when we go through January 1st if we go through it with relatively minor disruption, if we want to look back and wonder if we avoided one of the greatest threats to our domestic tranquility and threats to national security that we've ever experienced in this country, or whether we'll look back and think, well, we dealt with one of the most overstated, overstudied, overdiscussed problems that cost us literally billions of dollars in both the public and private sector.

I thought it would be helpful in terms of trying to allow the general public to understand what all of this study, all these contingency plans, all these validation efforts have been about if I could ask each of you to give us an example of one specific problem that you did discover, that you did fix, and if you haven't fixed it, what would have been the significant consequence of the failure to have discovered it and fixed it?

And I'll give you a little time to think about that. I have a few other questions I want to address. I'll leave that for my last question for each of you, because I think if we could come up with a good example from each of you, it might help the public understand what all this effort and expenditure was really all about. You know, it's all well and good to hear we're checking our systems, we validate, we know there's not going to be a problem, but I think it's also helpful to know what problem was really found and fixed.

One long-term consequence, I think, of the effort that you've made that will have lasting value is in terms of our national security. We all know that we talk a lot about the threat of nuclear warfare, the threat of chemical warfare, the threat of biological warfare. But we also know that at the end of this century we also face the threat of cyber warfare. And I want to address this question to Dr. Langston because I think that it is important for us, having gone through the effort to address the Y2K problem, that once we hopefully successfully move through it, that we not take all of our contingency plans and throw them in the wastebasket. But recognize that they do perhaps have some long-term benefit in terms of being prepared for the threat of cyber warfare.

Dr. Langston, if you would, just address the implications of what you have done in the Department of Defense which would obviously be directly related to the issue I raised as well as what you might see as the benefits of the efforts that have been made all across the public and private sector with regard to preparation for cyber warfare.

Mr. LANGSTON. Thank you sir for that question. We currently operate, as I mentioned, with year 2000 as our highest priority in the Department short of military operations, and we also operate with cyber threat as our second highest priority for everything that relates to the movement of information within the Department. We have in this past year stood up what we call a Joint Task Force for Computer Network Defense, which has now been moved under the Unified Commander for CINC Space, signifying the importance of this operation. In other words, we believe that it is an operational four-star commander's importance level, level of importance for supporting and monitoring and preparing for computer network defense. That's an indication that our operational forces have realized that these computer networks are critical and integral part of all our war-fighting operations, and they include, of course, support operations, logistics, finance, personnel, as well as direct military mission operations.

So therefore, we plan to continue on through the preparation and development of cyber warfare defensive measures. We posture and are working right now on what we call an information assurance architecture, which is literally a defense in-depth architecture that will allow us to specify for all of our operational forces and systems how we want them to use the technologies of today and the technologies that emerge for information assurance.

In addition, we have already put policy in place—I'm talking about policy signed out by Dr. Hamre, the Deputy Secretary, to install key infrastructure. These are encrypted certificates that will allow us to understand who it is that is at the end of every computer transaction, both internal to our Department and external to

the Department, and to put these in place in the next 3 years. And in addition, we have taken a step to move toward using the new smart card technology, which are literally credit cards with a chip in them, as a part of this security network defense operation to allow these smart card chips to become hardware stanchions of these encrypted certificates to represent who we are.

So we take it all very seriously. We believe that the pressure that has been applied through both the executive branch and the congressional legislative branch for critical infrastructure protection is vitally important to all of us. And we work very hard with judicial department and State Department and others to help put in place these efforts and make them a major part of what we do.

Mr. TURNER. It seems obvious to me that our technological superiority which has caused us to be the world's greatest military force perhaps is also our greatest vulnerability.

What about my suggestion that the other agencies of government and perhaps the private sector are not simply putting all of their plans in the wastebasket, but remember that there is an ongoing national security threat to all of us that perhaps those plans would be useful in preparing for?

Mr. LANGSTON. Thank you for reminding me of that question. I meant to suggest as we went through our—what I call our chairman's contingency assessment where we took major systems off line from our operational forces, in every one of those events, the unified commanders came back and said to the chairman, this was a very useful exercise, it was money and energy well spent. It allowed us to update our contingency plans, and it reminded us that we need to refine and continue to exercise those plans.

We, of course, in the military have always had contingency plans and always had back-up plans for everything we do. But like any organization, it's easy to not exercise them as often as you might need to given the press of ongoing business. So we plan to continue to use the contingency plans as an operation. And, in fact, working with the GAO and recent legislation in the appropriations bill, we plan to follow on with our year 2000 data base to support the tracking of these information systems and the evolution of this entire information assurance architecture that I suggested.

Mr. TURNER. Let me ask the question that I posed at the outset, and starting with Mr. Dyer, could you cite for us one problem that was discovered that you fixed and share with us the consequence that may have resulted had you failed to fix it? When we started out this effort many months, years ago, we all heard there wasn't enough computer programmers available to fix all these problems. Some months ago we asked at one hearing whether or not that was still the case, and we learned that really wasn't a real problem. So, obviously we've been able to cope thus far with the available personnel. I still assume that it took many man-hours of computer programmers to check out these systems, and in the process they found some things that they fixed. If you would, Mr. Dyer, give us a good example from your agency of something you found and fixed.

Mr. DYER. As Madam Chairwoman said, we started back in 1989, so we've had a long time to do it. As we've been updating software over the years, we've been continuously doing it. I'll give you the

major problems that would have happened. If the software was not adjusted, when the software ran, the computers would get the dates and everything confused; which would have meant that the calculations for what our beneficiaries would have been paid for the month would be all wrong and, on top of that, would probably stop the messages from going through to actually print out the checks and send the direct deposits.

In terms of very small kinds of things, as we went through telecommunications systems and looked at them, what would have happened is that certain data that we would have been transmitting over satellites to move various things around the country would just not have happened.

Mr. TURNER. Dr. Langston, without breaching national security or revealing anything that might be top secret, could you give us an example of something that was found and fixed and the consequence of failure to do so?

Mr. LANGSTON. Yes, sir. An indication of how critical this has become for us is that many people in the early days of the year 2000 problem dismissed it as not a very significant or real problem. And as each of our folks, including our very senior managers and leaders, have gotten involved with it, they have all been very—become very serious about the importance of it as they've discovered what kinds of examples have come forward.

Let me just give you a couple of examples. In our finance and accounting systems, we have found that we would not have been able to move money between ourselves and our vendors our through the financial system, and we would not have been able to make payment to our retirees without fixing those systems.

In our medical equipment systems, we have found many examples of where we would have not been able to support the medical records or even the medical processes that distributed medical activity to the medical recipients. In a very vivid example, our communications switches, which are commercial switches, but which we purchase over long periods of time, often don't keep them up to date with the latest changes in the commercial switch market. We found over 120 switches that would have gone down during the Y2K period of time and literally taken down all of our telephones within the Department and therefore rendered us virtually without communications to support anything we've done.

And even in the weapons systems area, we have weapons planning systems that support the distribution of plans out to our weapons platforms, and there were Y2K problems in those systems that would have created a need for contingency backups.

Mr. TURNER. Thank you. Mr. Gilligan.

Mr. GILLIGAN. As you know, the Department of Energy has a range of missions, from nuclear missions to academic oriented research. The example that I would like to discuss is at one of our nuclear waste processing plants at our Savannah River site in Aiken, SC. We have a series of systems that are interconnected that provide for processing and treatment of nuclear waste, high level nuclear waste products, containerizing them and shipping them. In the course of the analysis and the inventorying of those systems, we found that many of the embedded processor chips that were involved with the process control of moving the waste from

one station to another, as well as those computers that monitored the exhaust stacks for possible increased levels of radiation, had Y2K related problems.

Those were, in many cases, easily fixed. In some cases, they redesigned new special-purpose computers in order to be able to fix the problems. And so—and those systems then were installed. They had to be installed during downtimes of the process so they would not disrupt operations. Now, many would fear that a possible Y2K failure would result in a nuclear accident.

That is not, in fact, the case. In all of those circumstances, what would have happened if we had not repaired those systems is that the processor would have failed, would have triggered automatic shut-down procedures. But the automatic shut-down procedures, while they protect against any nuclear release of contamination, they do cost money because we would have an approximately \$3 million a day impact in cost of lost opportunity if, in fact, those systems had not been prepared. That is an example where obviously there is high visibility because of the nuclear processing. We felt confident, even though these problems existed, they would not have caused a health and safety consequence; but they would have had a fairly significant financial impact if we had not repaired them prior to January 1st.

Mr. TURNER. Thank you. Mr. Cosgrave.

Mr. COSGRAVE. Mr. Turner, if I may, I would like to give you three quick examples, all stemming, frankly, from the neglect that allowed us to have an antiquated infrastructure that hadn't been addressed in a long time.

The first example, probably the most important, is we have replaced the entire submissions and remittent processing system that operates in our service centers for processing the tax returns when they come in. The system was, in many cases, 15- and 20-year-old hardware that, frankly, we couldn't even get replacement parts that were Y2K compliant to meet the needs. So we had no choice but to replace that entire system with modern technology. So we literally would not have been able to process tax returns.

The second example is with respect to security. We have been running a fairly old security environment that was decentralized like many things at the IRS, and it was very clear that we needed to bring that up to speed and up to date. So we have made a major improvement in our security environment as a result of the Y2K effort.

The third example, and probably the most dramatic to people listening in, is that when our revenue agents went out and visited taxpayers, they were often embarrassed because they were carrying with them either a PC that was of 286- or 386-type vintage. If you don't follow the Intel market, they were issued back in the early 1980's. Quite honestly, that is not adequate given what they are facing when they deal with the taxpayers today who quite often have much more sophisticated technology. So we have replaced all of those PCs with modern Pentium computers and now at least are on an even par with the taxpayers.

Mr. TURNER. Thank you. Dr. Lorentz.

Mr. LORENTZ. I guess I would answer the question two ways. The two specific examples I would give are: First of all, we identified

an accounts payable problem, one that if it hadn't been identified, if the process hadn't pointed it out to us, would have resulted in late or no payments at all going to some of our suppliers.

The second example is our air dispatch system. In that case, we have an automated system that literally takes the mail once it has been sorted and prepared and dispatches it to aircraft. A substantial portion of the mail is airborne now. So it would have given us an inability to do that in a mechanized way.

Those were two significant areas that were very constructive. The second answer to the question is that this has caused us to put process discipline in our business and we now have business owners of these issues, not just technology owners. So we literally have—we are going to leverage this in how we look at security.

Security is not a chief technology officer issue. It is a business issue. To give you an example in a more pedestrian way, we had the best close of our financial books that we have had in recent memory because we had significant configuration management in place. So the discipline that has been caused by going through Y2K preparation, as well as the retirement of unneeded systems, has given us a positive outcome.

Mr. TURNER. Thank you. I must say that listening to all of you, the direct and secondary benefits of the efforts seem to be very apparent. Thank you, Mr. Chairman.

Mrs. MORELLA. Thank you, Mr. Turner. Following up on the questions that you asked, I thought that was excellent, did any of you have any trouble with 9-9-99? Can we just very quickly, did you have any trouble?

Mr. LANGSTON. No, ma'am; but I would point out that in our testing efforts, we have found as many problems in the leap year rollover period which will occur the end of February as we have in the Y2K period, the rollover date.

Mrs. MORELLA. So you are preparing for that. I think that we all should—

Mr. LANGSTON. That is why our transition period includes that.

Mrs. MORELLA. Mr. Gilligan.

Mr. GILLIGAN. We had no problems on the 9th of September. We did, in fact though, have one system at the beginning of our fiscal year of October 1st that experienced a failure. This was a failure of a subportion of our procurement data tracking system. It was fixed within about a half hour, and the transactions were rerun and the permanent fix was done within about 24 hours. But it did give us clear indication that we need to have processes in place to be able to respond.

Mrs. MORELLA. OK. Mr. Cosgrave.

Mr. COSGRAVE. Our experience was very similar to what the Department of Defense is experiencing. I would reiterate the leap-year problem because we are focused on that as part of our testing as well.

Mr. LORENTZ. Not to our knowledge we didn't have any 9-9-99 problems. We did have a couple of cases where we printed the wrong dates, but it didn't do anything to the internal code.

Mrs. MORELLA. Several of you have already commented on the information computer security problem. Not only is it enormous with DOD, but obviously very important with all of you. I just won-

dered if you are taking precautions. Now, I heard what you said that is being done, Dr. Lorentz. You talked a little bit about it, Mr. Cosgrave. I wondered if the others might want to comment. Are you taking any precautions for this day 1 plan in terms of the information technology security?

Mr. DYER. We are quite concerned about security. We are going to be doing extra monitoring of all of our systems. We have a special team in place to concentrate totally on all of the security issues.

Mrs. MORELLA. Mr. Gilligan.

Mr. GILLIGAN. We have an organization called the Computer Incident Advisory Capability that is co-located at Lawrence Livermore Laboratory. They are our cyber-security investigation and response cell. They will be active as will their points of contact at all of our sites. We have established reporting procedures. They will be part of our emergency operations center contingent active through this rollover period.

Mr. LORENTZ. We have put in place all of the industry standard firewalls and virus protection on our case-hardened side. We have given specific special instructions to the field on what to look for in the intervention of viruses. The additional area that we are looking at both as far as the day 1 as well as the future, is more e-commerce exposure.

We have, so far, issued 150,000 digital certificates for the online stamp capability. We see potential exposure certainly in e-commerce along with everybody else. We are especially monitoring those aspects of the business. We are also participating in the cyber assurance effort as part of the Y2K council in partnership with other agencies.

Mrs. MORELLA. Thank you. I think you have all done a great job of sharing the experiences looking back, looking ahead, but more needs to be done of your agencies. I want to announce that—do you have any other questions or comments?

Mr. TURNER. No.

Mrs. MORELLA. It has been an excellent hearing. Please note that all of the members of the subcommittee again will get the full testimony. We would like your permission to be able to submit any further questioning to you from ourselves and other members of the subcommittee.

I am going to ask unanimous consent that Chairman Horn's opening statement be included in the record. If no objection, it will be so ordered.

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

Opening Statement
Chairman Stephen Horn (R-CA)
Subcommittee on Government Management,
Information, and Technology
October 29, 1999

This joint hearing of the House Subcommittee on Government Management, Information, and Technology, and the House Subcommittee on Technology will come to order.

Today, the subcommittees will hear testimony about the Federal Government's year 2000 computer contingency plans. This is our 23rd hearing on the year 2000 computer challenge during this first session of the 106th Congress.

For three years, we have been discussing the readiness of the executive branch's "mission-critical" computer systems. Our oversight objectives have been to ensure the seamless delivery of Federal military and civilian programs; that State and local governments will continue delivering vital Federal programs, such as Medicare and Medicaid, and Temporary Assistance for Needy Families; and, finally, that even if computers failure, Federal agencies can continue doing business.

Contingency plans are a part of daily life. If traffic is stalled, you take an alternate route, or ride the Metro. When storms threaten, you buy a couple of extra days' worth of food and check your supply of batteries.

Federal contingency and Day One plans provide the same type of insurance. This "insurance" provides that normal or, at least, limited business operations continue even if computers malfunction.

The Office of Management and Budget and the General Accounting Office have crafted guidelines for contingency and Day One planning. This framework is designed to help Federal agencies devise strategies to reduce potential year 2000 risks. The OMB required Federal departments and agencies to submit these plans on October 15th. Consequently, the agencies are in various stages of developing and testing their contingency and "Day One" plans.

I have often said that an organization is not "Year 2000 ready" until its computer systems are independently certified as compliant and its contingency plans are developed and rigorously tested. The Internal Revenue Service (IRS) recently reported to the House Ways and Means Committee that its computer systems inventory currently poses a high risk to IRS's Y2K effort. We want to know more about this "risk" and what effect it might have on the nation's taxpayers. Clearly, we need a candid discussion on IRS's contingency plans.

Many public and private organizations, including the IRS, will rely heavily on the U.S. Postal Service to deliver the mail if their electronic communications fail. Is the Postal Service prepared to handle such an increase in mail volume? What will the Postal Service do if it experiences Y2K-related problems?

Because each Federal agency is different, there is no single approach to contingency and Day One planning. Our witnesses today provide a cross-section of these departments and agencies, and their respective challenges.

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

Mrs. MORELLA. The next hearing of the House Y2K working group is going to be held next Thursday, November 4. It will be at 2 o'clock in the afternoon, room 2318 of this building. The hearing is going to be entitled "Y2K Myths and Realities; What Every American Needs to Know in the Remaining 50 days." it is now count down 63 today, but it will be 50 at that time. The hearing is designated to be the culmination of our over 3½ years and over 100 congressional hearings on the Y2K computer glitch.

I just want to thank the following people who have been involved in some way in putting this hearing together: The majority staff of the Government Reform Committee: J. Russell George, staff director and chief counsel; Matt Ryan, senior policy advisor; Bonnie Heald, the communications director and professional staff member; Chip Ahlswede, clerk; Rob Singer staff assistant; P.J. Caceres, an intern; Deborah Oppenheim, an intern; the Technology Subcommittee: Jeff Grove, staff director; Ben Wu, professional staff member; Joe Sullivan, staff assistant; minority staff of Government Reform: Trey Henderson, minority counsel; Jean Gosa, staff assistant; of the Technology Subcommittee minority staff: Michael Quear, professional staff assistant; Marty Ralston, staff assistant; the court reporters: Cindy Sebo and Randy Sandefer who has come on the scene here, too.

And so I thank all of them. I want to thank Congressman Turner for being with us for the entire hearing. I want very much to thank both of our panels. We appreciate it very much. Thank you very much.

The subcommittee is now adjourned.

[Whereupon, at 12:12 p.m., the subcommittee was adjourned.]

