S. HRG. 106–219

JOINT HEARING ON FEDERAL AGENCY Y2K SPENDING

HEARING

BEFORE THE

COMMITTEE ON APPROPRIATIONS

AND

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

SPECIAL HEARING

Printed for the use of the Committee on Appropriations and the Special Committee on the Year 2000 Technology Problem

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

58–306 cc WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0–16–059709–9

COMMITTEE ON APPROPRIATIONS

TED STEVENS, Alaska, *Chairman*

THAD COCHRAN, Mississippi
ARLEN SPECTER, Pennsylvania
PETE V. DOMENICI, New Mexico
CHRISTOPHER S. BOND, Missouri
SLADE GORTON, Washington
MITCH MCCONNELL, Kentucky
CONRAD BURNS, Montana
RICHARD C. SHELBY, Alabama
JUDD GREGG, New Hampshire
ROBERT F. BENNETT, Utah
BEN NIGHTHORSE CAMPBELL, Colorado
LARRY CRAIG, Idaho
KAY BAILEY HUTCHISON, Texas
JON KYL, Arizona

ROBERT C. BYRD, West Virginia
DANIEL K. INOUYE, Hawaii
ERNEST F. HOLLINGS, South Carolina
PATRICK J. LEAHY, Vermont
FRANK R. LAUTENBERG, New Jersey
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
HARRY REID, Nevada
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
BYRON L. DORGAN, North Dakota
DIANNE FEINSTEIN, California
RICHARD J. DURBIN, Illinois

STEVEN J. CORTESE, *Staff Director*
LISA SUTHERLAND, *Deputy Staff Director*
JAMES H. ENGLISH, *Minority Staff Director*

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

ROBERT F. BENNETT, Utah, *Chairman*
CHRISTOPHER J. DODD, Connecticut, *Vice Chairman*

JON KYL, Arizona
GORDON SMITH, Oregon
SUSAN M. COLLINS, Maine
TED STEVENS, Alaska (ex officio)

DANIEL PATRICK MOYNIHAN, New York
ROBERT C. BYRD, West Virginia (ex officio)

ROBERT CRESANTI, *Staff Director*
WILKE GREEN, *Minority Staff Director*

CONTENTS

JOINT HEARING ON FEDERAL AGENCY Y2K SPENDING

TUESDAY, JUNE 22, 1999

U.S. SENATE,
COMMITTEE ON APPROPRIATIONS,
SPECIAL COMMITTEE ON THE
YEAR 2000 TECHNOLOGY PROBLEM,
Washington, DC.

The committees met at 9:35 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Robert F. Bennett (chairman of the Special Committee on the Year 2000 Technology Problem) presiding.

Present: Senators Bennett, Stevens, and Gorton.

GENERAL ACCOUNTING OFFICE

STATEMENT OF HON. DAVID M. WALKER, COMPTROLLER GENERAL

ACCOMPANIED BY JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS

OFFICE OF MANAGEMENT AND BUDGET

STATEMENT OF JACOB J. LEW, DIRECTOR

OPENING STATEMENT OF HON. ROBERT F. BENNETT

Chairman BENNETT. We welcome you to this morning's hearing, which is a joint hearing of the Senate Appropriations Committee and the Senate Special Committee on the Year 2000 Technology Problem. Senator Stevens has asked that I chair the committee, and I am grateful to him for his courtesy.

We want to welcome our witnesses for coming today as well. The topic for today's hearing is oversight of spending on the year 2000 technology problem within the Federal Government. Let me start out by noting that questioning Government spending on Y2K has been likened in some circles to questioning a firefighter on the use of water during a fight against a fire in a burning building, and I agree with that to a certain extent.

I think it would be a tragedy if we get to the year 2000 and have serious problems. To have them traced to a lack of money and say, "well, we knew what to do, we had the plans in place to do them, but we just did not have the money." I certainly do not want anyone to accuse the Congress of being complicit in a situation like that. Ensuring the uninterrupted flow of critical Federal services is too important.

Our purpose here today is not to assail the Federal agencies or the administration for the amount or manner of Y2K spending. We

recognize that the biggest roadblock we face toward getting this problem under control, the biggest scarcity we have, is time, not money.

However, there is always the possibility within the Federal Government that money that is appropriated for good and proper purposes ends up being diverted some place else. We have a responsibility to ensure that the taxpayer dollars have been spent for the purpose for which they were appropriated, and at the same time that there will be sufficient funds left for unexpected Y2K costs that will shortly crop up this year and next.

The appropriations that were made, were made with the assumption that there would be some left over after we get to January 2000 to take care of problems. We simply do not know how much needs to be left over, but it would be irresponsible to say, well, this money is available, let's just go ahead and spend it.

Now, here is what we do know. According to the General Accounting Office (GAO), Federal spending on Y2K readiness is currently estimated to be $8.7 billion, and that is up from $2.3 billion that was estimated in February of 1997. I remember when that estimate was made, members of our committee were highly skeptical that it could be achieved for that, so we are now more than three times that original estimate. We may see an escalation in the $8.7 billion. It may continue up after January 1, 2000.

Now, we have also learned that many Government agencies are not tracking their Y2K costs, and this includes costs funded from the $3.35 billion emergency supplemental appropriation. That breaks down to $1.1 billion for defense, and $2.25 billion for nondefense. We need to determine if these funds are being used appropriately and, if not, we should determine where additional oversight is necessary.

The charts displayed here show the growth in Federal agencies' Y2K cost estimates and the status of emergency supplemental funding for nondefense agencies. That second chart is a little hard—not a little hard, it is impossible to read, except when you have a hard copy of it in front of you. We tried to simplify it but we were unable to because the information on it is vital.

The charts indicate that we have only $450 million left through September 30, 2001, the life of the fund. That is one of the reasons for this hearing. We are concerned about whether there will be money left to clean up problems that come after the year 2000 turns, so we must determine if there are adequate resources available to meet the future Y2K demands, and we suspect that more and more will be spent for Federal agencies' contingency plans.

Now, unfortunately the current pace of contingency planning presents us with one of our blind spots as far as congressional oversight is concerned, because many Government agencies missed the June 15 deadline for submitting contingency plans. This failure not only deprives us of any confidence we might have in their ability to handle the emergencies, but it also prevents the Office of Management and Budget (OMB), GAO, and the Congress from estimating how much these contingency plans may cost if they are required.

So with time running out, contingency planning for Y2K becomes very important. As we explore the flow of funding to the Federal

agencies, a lack of contingency planning is not a blind spot we can afford to have.

So with that, Senator Stevens, if you have an opening comment we will call upon you now.

[The statement follows:]

PREPARED STATEMENT OF SENATOR ROBERT F. BENNETT

Good morning. I would like to thank Chairman Stevens for presiding over this joint hearing of the Senate Appropriations and Y2K committees. I would also like to thank our witnesses for coming today.

The topic of today's hearing is federal Y2K spending. Before proceeding, I think it is important to note that, in some circles, questioning government spending on Y2K is likened to questioning a firefighter on his use of water on a burning building. I agree with that statement to an extent. In fact, I believe we should continue to make available the necessary resources to ensure that government continues to function on January 1, 2000 and beyond. We don't want the lack of money to be a reason why the federal government is not prepared for Y2K—ensuring the uninterrupted flow of critical federal services is simply too important.

Therefore, my purpose here today is not to assail the federal agencies or the administration for the amount or manner of Y2K spending. The biggest roadblock to Y2K readiness at this point—with only 192 days left—is the scarcity of time, not money.

Having said that, we have a responsibility to ensure that taxpayer dollars are not being spent frivolously, and that there will be sufficient funds left for the continued unexpected Y2K costs that will surely crop up later this year, and next. But the truth is, we simply don't know enough to say exactly how much will be needed for the remainder of this year and future years.

Here is what we do know: According to GAO, federal spending on Y2K readiness is currently estimated to be $8.7 billion—up from $2.3 billion in February 1997—and may continue upward after January 1, 2000. We have also learned that many government agencies are not tracking Y2K costs—this includes costs funded from the $3.35 billion emergency supplemental appropriation. We need to determine if these funds are being used appropriately. If not, we should determine whether additional oversight is necessary.

We must determine if there are adequate resources available to meet future Y2K funding demands. In particular, we suspect that more and more will be spent for federal agencies' contingency plans. Unfortunately, the current pace of contingency planning presents us with another blind spot, as far as congressional oversight is concerned. Many government agencies missed the June 15 deadline for submitting contingency plans. This failure not only deprives us of any confidence we might have in their ability to handle Y2K-induced emergencies, but also prevents OMB, GAO and the Congress from estimating how much contingency plans may cost.

With time running short, contingency planning for Y2K becomes very important. As we explore the flow of funding to the federal agencies, a lack of contingency planning is not a blind spot we can afford to have. Thank you very much.

STATEMENT OF HON. TED STEVENS

Chairman STEVENS. Well, thank you very much, Senator Bennett. I welcome the chance to jointly review this problem with you. The emergency supplemental funding is what worries me, and I hope that we are keeping track of not only what has been spent, but what the demand will be between now and the turn of the century. It does appear to me that we have a little glitch in terms of contingency planning. I do want to go into that with our witnesses this morning. I do not have an opening statement.

I appreciate these charts. They are a little busy, but they contain a great deal of information. I do not know if we have copies we could provide to the press out there so they can understand what we are talking about.

Chairman BENNETT. Yes, indeed.

Chairman STEVENS. Thank you very much.

Chairman BENNETT. Thank you, and everyone should recognize that we would not be in the good position we are with respect to funds for the year 2000 if it were not for Senator Stevens and his very early recognition of this problem and his willingness to carve out of the appropriations bill these funds. Any other appropriations chairman might have taken the position of, "well, let's wait and see." Senator Stevens recognized early on that there is no time to wait and see, and we are in the good position we are because of Senator Stevens.

PREPARED STATEMENT OF SENATOR BYRD

Chairman STEVENS. Mr. Chairman, Senator Byrd is detained, and I would like to have his statement placed in the record, and he does have some questions he would like to submit for the record.

Chairman BENNETT. That will be placed in the record, and we will be happy to forward his questions and receive them at such time as he might be available.

[The statement follows:]

PREPARED STATEMENT OF SENATOR ROBERT C. BYRD

Thank you, Mr. Chairman, for calling this joint hearing of the Appropriations Committee and the Special Committee on the Year 2000 (Y2K) Technology Problem to examine budgeting efforts to ensure the Y2K readiness of the executive branch. You have provided important leadership on this issue. As an Ex-Officio Member of the Special Committee on the Year 2000 Technology Problem, I also thank Chairman Bennett and Senator Dodd for their good work on this vexing problem. You have both worked diligently to raise awareness about this issue and to monitor the progress our nation is making toward meeting the immovable deadline of midnight, December 31.

Our nation, indeed, the entire world, is increasingly reliant on technology. In the case of the federal government and its responsibilities in areas such as defense, emergency management services, telecommunications, and benefit programs, Y2K readiness is critical. Congress has recognized and responded to the importance of this issue by providing considerable funds to bring federal systems into compliance.

The costs are substantial. GAO estimates that federal Y2K costs as of May 1999 total $8.7 billion, a dramatic increase from the $2.3 billion cost estimated in early 1997. In response to emergency needs cited by federal agencies, last year Congress provided $3.35 billion in emergency funding through the Omnibus Consolidated and Emergency Supplemental Appropriations Act. Of the $3.35 billion, $2.25 billion was provided for non-defense agencies and $1.1 billion for Department of Defense (DOD). Thus far, a substantial portion of these emergency funds have been allocated to federal agencies by the Office of Management and Budget (OMB). It is important that these Committees provide oversight of this spending.

As December 31, 1999, draws near, we must make every effort to ensure that the federal government is Y2K ready. As appropriators, we have a responsibility to ensure that the funds provided for Y2K conversion are in fact achieving federal Y2K readiness and that these funds are accounted for carefully. We must also explore whether additional resources will be necessary to finish the job, to implement contingency plans, and to meet any outstanding needs. I look forward to receiving the testimony of our witnesses this morning as we delve into these important issues.

Chairman BENNETT. Our witnesses this morning are Hon. David Walker, who is the Comptroller General of the U.S. General Accounting Office, and Hon. Jacob Lew, who is the Director of the Office of Management and Budget. Between the two of you, you probably represent more expertise on the budget and the cash flow of the Federal Government than any other two individuals available, and we are grateful to you for your willingness to appear here and look forward to hearing from you both.

We will start, Mr. Walker, with you.

STATEMENT OF HON. DAVID M. WALKER

Mr. WALKER. Thank you, Mr. Chairman. Good morning, Chairman Bennett, Chairman Stevens. Thank you for inviting me to testify today on Y2K costs and to discuss more broadly the implications of Y2K on future information technology activities.

Since our February 1997 designation of the year 2000 problem as a high risk area for the Federal Government, action to address the Y2K threat has intensified. In response to a growing recognition of the challenge, as well as urging from congressional leaders, the administration has strengthened the Government's Y2K preparations.

For example, OMB has now established 43 high impact program areas as Government priorities. This list includes such programs as Social Security, food stamps, and Medicare. It does not, however, include direct national security and revenue collection activities. Many congressional committees have been extremely diligent in addressing the year 2000 challenge by holding agencies accountable for demonstrating progress, and by heightening public appreciation of the problem.

In particular, work done by the Senate Special Committee on the Year 2000 Technology Problem has fostered a greater understanding of this issue and focused attention on much-needed actions. Despite the improvements in the Government's Y2K approach, significant challenges remain. In particular, through year 2000 testing is essential. Further, adequate business continuity and contingency plans must be successfully completed and tested.

As shown by this chart, Mr. Chairman, the total estimated Y2K costs for the 24 major Federal agencies have more than tripled during the last 2 years. A total of about $8.7 billion as of the end of last month. Within this $8.7 billion, Federal agencies have reported that their year 2000 costs for fiscal years 1996 to 1998 were over $3 billion. Some agencies told us that they reported these based on actual costs, while others reported some costs as actuals, and others as estimates. Still others included total estimates, and did not maintain actual costs for Y2K, other than for the emergency supplemental.

With agencies' estimates of Y2K costs increasing dramatically, and with limited time remaining to complete needed actions, many agencies have requested emergency funds in fiscal year 1999. According to their justification submissions to the Congress and OMB, three categories of reasons emerge to explain organizations' requests for emergency funds: First, new requirements that had not been planned for fiscal 1999; second, cost increases to complete ongoing Y2K activities; and, third, the unavailability of regular appropriations for planned Y2K work.

New requirements included outreach, independent verification validation, as well as decisions to replace personal computers and network hardware and software for a variety of reasons, including to assure Y2K compliance.

In May 1999, the 24 major departments and agencies estimated their fiscal year 2000 costs for Y2K activities at about $981 million, almost a ninefold increase from the original year 2000 estimate of about $111 million provided in February 1997.

Determining the extent of continued Y2K cost estimation is difficult because of many uncertainties. For example, 10 agencies reported that they have not completed work on their mission-critical systems as of mid-May 1999. Key factors that could fuel additional cost increases include agencies determining that they must implement business continuity and contingency plans, or if there are any other anticipated events that occur due to the Y2K problem that must be addressed.

For example, in August of 1998, the Health Care Financing Administration (HCFA) estimated that it would need between $300 million and $500 million to handle emergency contingency situations that could result from the Y2K problem. HCFA reported that the types of activities that these funds would be needed for included unforeseen software, hardware, and telecommunications failures, increased paper claims due to provider or billing companies' inability to transmit electronically, and claims reprocessing to correct erroneous repayments.

The Health and Human Services (HHS) reported to us that it requested about $165 million for Y2K activities in its fiscal year 2000 budget request. This amount, however, excluded any amounts for the implementation of HCFA contingency plans should those plans prove to be necessary.

Other agencies could also have higher costs if business contingency and continuity plans need to be implemented. OMB's review of agency contingency plans should therefore consider whether agencies have provided information on the cost of implementing contingency plans if that should be required. If not, OMB needs to gather this information quickly so that it can share with the Congress what impact this would have on potential future funding needs.

Additional costs could also be incurred if some States do not complete their year 2000 work on systems that support critical Federal programs such as food stamps and Medicaid. Importantly, 10 of OMB's designated high impact programs rely on State-level implementation. Information indicates that some State systems are not scheduled to be compliant until the last quarter of 1999.

If States do not complete their year 2000 remediation in time, or if those remediation efforts fail, the States would have to implement their business continuity and contingency plans, which could encompass Federal Government assistance because of the cost reimbursement mechanisms under those programs.

While making systems ready for year 2000 has been an enormous job, other program and information technology needs have not disappeared. In fact, they have grown, and continue to grow. In particular, because of the year 2000 problem, agencies have delayed implementation of regulatory requirements and planned information technology enhancements. There is a pent-up demand and growing backlog of such initiatives which may have significant implications for future funding level requests.

The total Government-wide volume of program and information technology activities delayed by Y2K is not known. Therefore, the potential demand for additional information technology resources in the future is difficult to predict. However, the cost of these delayed activities could be significant. Accordingly, OMB will need to

work with the agencies to determine the magnitude of these pent-up demands in order to make informed management and funding decisions in the future.

In addition to these demands, increased resources will likely be needed for another key issue that has garnered increased attention, namely information security. As we reported in September 1998, the expanded amount of audit evidence that has become available since mid-1996 describes widespread and serious weaknesses to adequately protect Federal assets, sensitive information, and critical operations.

The computer security issue, which is already on our high risk list, will follow on the heels of the Y2K challenge. Computer security issues have a range of potential national security, economic security, and personal privacy implications.

There has importantly been a silver lining to the Y2K challenge. The Government organizations' experiences in becoming prepared for the year 2000 hold valuable lessons about how information technology can best be managed. For many agencies, the threat posed by the year 2000 problem was a much-needed wake-up call. Because of the urgency of the issues, agencies could not afford to carry on in the same manner that resulted in a decade of poor information technology planning and program management.

Earlier this year, we reported that the year 2000 provided the opportunity to institutionalize valuable lessons, such as the importance of consistent and persistent top management attention to be accompanied by reliable processes and reasonable controls.

Another benefit of the year 2000 effort was the establishment of much-needed information technology policies in such areas as configuration management, quality assurance, risk management, project scheduling and tracking, and metrics. Beyond individual agencies, the year 2000 problem holds lessons in overseeing and managing information technology on a Government-wide basis. In particular, actions taken by the Congress and the executive branch have demonstrated that effective oversight and guidance can have a positive influence on major information technology efforts.

In conclusion, Mr. Chairman, it is clear that Y2K expenditures have been significant, sometimes unpredictable, and constantly growing. Further, Y2K cost growth may continue, especially if business and continuity contingency plans must be put into operation, or if State-administered Federal program system efforts are not completed.

In addition, pent-up demand exists for information technology enhancements and security activities. OMB needs to take steps to estimate the nature and extent of these pent-up demands, as well as the contingency expenditures that could be incurred related to Y2K.

On the positive side, while correcting the Y2K problem has been and continues to be costly, the experiences of individual agencies and the Government as a whole in meeting this challenge have provided renewed and needed focus on information systems. As we attempt to meet future information technology and security challenges, these lessons must not be lost.

PREPARED STATEMENT

This completes my summary statement, Mr. Chairman. I would be happy to answer any questions at the appropriate time. Thank you.

Chairman BENNETT. Thank you very much. We appreciate your statement. Your full statement will be made a part of the record.

[The statement follows:]

PREPARED STATEMENT OF DAVID M. WALKER

Messrs. Chairmen and Members of the Committees: We are pleased to be here today to present information on Year 2000 (Y2K)[1] costs and funding and to discuss more broadly what implications the government's necessary short-term focus on preparing for the year 2000 will have on future information technology activities. In 1997, we designated the Year 2000 computing problem as a high-risk area because computer failures could disrupt functions and services that are critical to our nation.[2] After providing a brief summary of the issues and background information, my testimony today will highlight (1) estimated Y2K costs and agency processes to track costs to date, (2) planned uses of emergency funding, (3) Y2K costs for fiscal year 2000 and beyond, (4) agency program and information technology initiatives delayed by Y2K activities, and (5) lessons learned from Y2K efforts that can be applied to other information technology activities.

RESULTS IN BRIEF

Meeting the Year 2000 challenge has been necessary but expensive, with estimated federal costs rising from $2.3 billion in February 1997 to $8.7 billion as of last month. From February through May 1999, the estimated cost rose $1.2 billion. With respect to Y2K costs incurred through fiscal year 1998, the 24 major federal departments and agencies reported costs exceeding $3 billion. While some agencies reported actual costs incurred through 1998, others reported estimates. In fiscal year 1999, agencies have requested emergency funds and plan to spend much of these funds on renovation, validation, and implementation activities, along with replacing personal computers and network hardware and software. Beyond fiscal year 1999, estimated Y2K costs have continued to climb, now reaching over $1 billion. Determining the extent of continued Y2K cost escalation is difficult because of many uncertainties. One major unknown is whether agencies will have to implement their business continuity and contingency plans. Such plans, if triggered, could entail substantial costs. Agencies' high-level business continuity and contingency plans were due to the Office of Management and Budget (OMB) by June 15. OMB's review of these plans should consider whether agencies provided estimated business continuity and contingency plan costs. If not, OMB needs to require that this information be provided expeditiously so that it can provide the Congress with information on potential future funding needs. We intend to review the plans submitted to OMB and advise the Congress of potential funding ramifications.

Another less direct but undeniable issue associated with the Year 2000 challenge has been the postponement of many program and information technology initiatives so that resources could be dedicated to Y2K. Such demands—including system enhancements and computer security—have not vanished; in fact, they have grown. On the positive side, however, the government will likely approach these future information technology challenges better prepared, having gained much valuable information from experiences in meeting the Y2K challenge. For example, this was the motivator that resulted in many agencies' taking charge of their information technology resources in much more active ways, from inventorying and prioritizing systems to implementing reliable processes and better controls. Such lessons should not be lost on future information technology projects.

---

[1] The Y2K problem is rooted in how dates are recorded and computed. For the past several decades, computer systems typically used two digits to represent the year, such as "99" for 1999, in order to conserve electronic data storage and reduce operating costs. In this format, however, 2000 is indistinguishable from 1900 because both are represented as "00". As a result, if not modified, systems or applications that use dates or perform date- or time-sensitive calculations may generate incorrect results beyond 1999.

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

BACKGROUND

With close to half of all computer capacity and 60 percent of Internet assets, the United States is the world's most advanced and most dependent user of information technology.[3] Such systems perform functions and services critical to our nation; disruption could create widespread hardship, including problems in key federal operations ranging from national defense to benefits payments to air traffic management. Accordingly, the upcoming change of century is a sweeping and urgent challenge for public- and private-sector organizations alike, in this country and around the world.

Since our February 1997 designation of the Year 2000 problem as a high-risk area for the federal government, action to address the Y2K threat has intensified. In response to a growing recognition of the challenge and urging from congressional leaders and others, the administration strengthened the government's Year 2000 preparation. In February 1998, the President took a major step in establishing the President's Council on Year 2000 Conversion. The President also (1) established the goal that no system critical to the federal government's mission experience disruption because of the Year 2000 problem and (2) charged agency heads with ensuring that this issue receive the highest priority attention. Further, the Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies, (2) acting as chief spokesperson in national and international forums, (3) providing policy coordination of executive branch activities with state, local, and tribal governments, and (4) promoting appropriate federal roles with respect to private-sector activities.

Among the initiatives the Chair of the Council has implemented in carrying out these responsibilities are attending monthly meetings with senior managers of agencies that are not making sufficient progress, establishing numerous working groups to increase awareness of and gain cooperation in addressing the Y2K problem in various economic sectors, and emphasizing the importance of federal/state data exchanges. In addition, on June 14, 1999, the President ordered the creation of an Information Coordination Center—consisting of officials from executive agencies—to assist the Chair of the Council in addressing Year 2000 conversion problems both domestically and internationally. Among its duties, the Information Coordination Center is to assist in making preparations for information sharing and coordination within the federal government and key components of the public and private sectors.

Many congressional committees have been extremely diligent in addressing the Year 2000 challenge by holding agencies accountable for demonstrating progress and by heightening public appreciation of the problem. By holding numerous hearings on important topics such as health care, the food sector, electric power, and financial services and in issuing a major report[4] on the impact of the Year 2000 problem, the Senate Special Committee on the Year 2000 Technology Problem has fostered a greater understanding of the problem and focused attention on actions needed.

OMB, for its part, has taken more aggressive action on Year 2000 matters over the past year and a half and has been responsive to our recommendations. For example, in its quarterly report issued in December 1997, OMB accelerated its milestone for agencies to complete the implementation phase of Y2K conversion by 8 months, from November to March 1999. OMB has also tightened requirements on agency reporting of Year 2000 progress. It now requires that beyond the original 24 major departments and agencies that have been reporting, 9 additional agencies (such as the Tennessee Valley Authority and the Postal Service) report quarterly on their Year 2000 progress, and that additional information be reported from all agencies. Additionally, in response to our April 1998 recommendation,[5] on March 26, 1999, OMB issued a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs, including those delivering critical benefits such as social security, food stamps, and Medicare; ensuring adequate weather forecasting capabilities; and providing federal electric power generation and delivery. (OMB later added a 43rd high-impact program—the National Crime Information Center.) Further, OMB has clarified instructions for agencies relative to preparing business continuity and contingency plans, and required agencies to submit

---

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

[4] *Investigating the Impact of the Year 2000 Problem* (United States Senate, Special Committee on the Year 2000 Technology Problem, February 24, 1999).

[5] *Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships* (GAO/AIMD–98–85, April 30, 1998).

high-level versions of these plans just last week, on June 15. We intend to review the plans submitted to OMB and advise the Congress of our results.

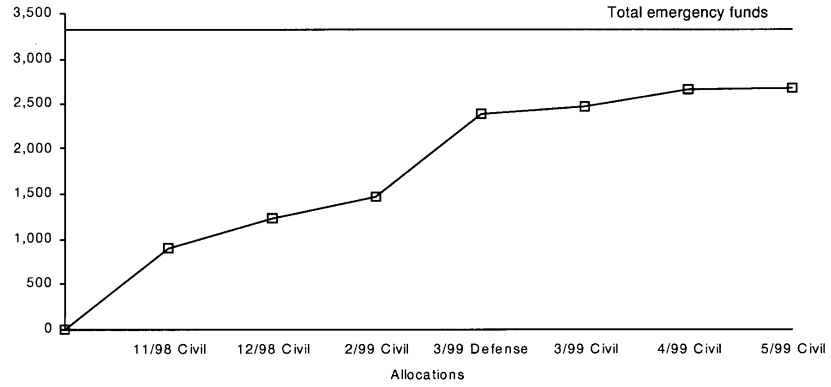
As you know, we have been very active in working with the Congress as well as federal agencies to both strengthen agency processes and to evaluate their progress in addressing these challenges. To help agencies mitigate their Year 2000 risks, we produced a series of Year 2000 guides on enterprise readiness, business continuity and contingency planning, and testing.[6] In addition, we have issued over 100 reports and testimony statements detailing specific findings and have made dozens of recommendations related to the Year 2000 readiness of the government as a whole and of a wide range of individual agencies.

Fortunately, the past 2 years have witnessed marked improvement in preparedness as the government has revised and intensified its approach to this problem. Nevertheless, significant challenges remain. In particular, complete and thorough Year 2000 testing is essential to providing reasonable assurance that new or modified systems will be able to process dates correctly and not jeopardize agencies' abilities to perform core business operations. Moreover, adequate business continuity and contingency plans must be successfully completed and tested throughout government.

The Congress Appropriated Emergency Year 2000 Funding

To address Y2K resource needs, last year the Congress appropriated $2.25 billion for civilian agencies[7] and $1.1 billion for the Department of Defense for emergency expenses related to Year 2000 conversion of federal information technology systems. Through May 1999, OMB made six separate allocations totaling about $1.724 billion[8] to civil agencies (77 percent of the $2.25 billion in civilian emergency funds) and one allocation of $935 million to the Department of Defense (85 percent of its emergency funds). Figure 1 illustrates the cumulative amount of emergency funds allocated to nondefense organizations and the Department of Defense, and that about $661 million remains.

Figure 1: Emergency Supplemental Funds Allocated to Agencies (Dollars in Millions)



Note: This chart does not include the amount set aside for the legislative and judicial branches ($29.9 million).

Source: OMB.

Figure 2 illustrates the entities that received the largest allocations.

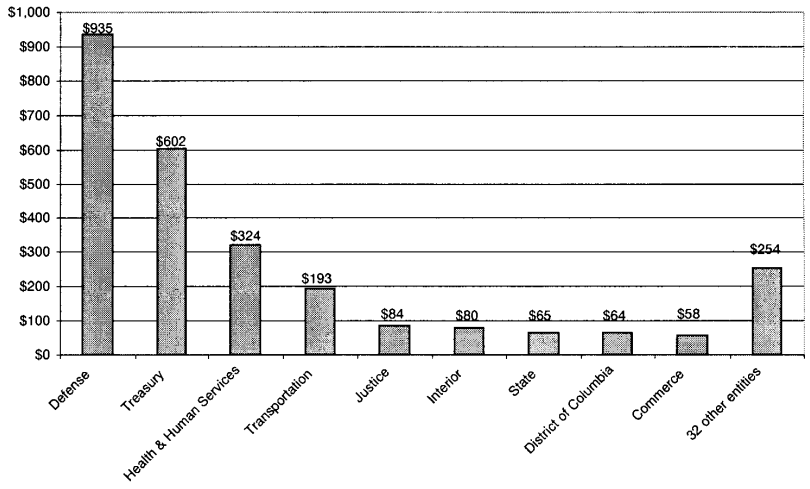
---

[6] *Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD–10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997), *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), and *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD–10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998).

[7] As part of the $2.25 billion for civilian departments and agencies, $16.873 million and $13.044 million were designated for the legislative and judicial branches, respectively.

[8] This amount does not include $13.65 million that OMB allocated to the Department of Energy but did not transfer to the department because, according to OMB, the House Appropriations Committee did not consider the planned use of these monies an appropriate use of emergency funding.

Figure 2: Entities With the Largest Emergency Funding Allocations as of May 1999 (Dollars in Millions)



Note: Appendix I lists all of the entities that received emergency funding allocations.

Source: OMB.

Regarding Y2K costs and funding, the House Majority Leader asked us to (1) identify agency-reported Year 2000 costs through fiscal year 1998 and the agencies' processes used to track these costs, (2) determine the reported status of fiscal year 1999 obligations for Year 2000 activities, (3) identify estimated Year 2000 costs for fiscal year 1999 and the planned uses of the emergency allocations, and (4) identify the Year 2000 costs for fiscal year 2000. In addressing these questions, we requested documentation of actual and planned costs from 29 federal agencies that provide quarterly Y2K compliance information to OMB, plus an additional 12 organizations that had received emergency funding. We provided a report to the House Majority Leader on this information in April 1999.[9]

In my testimony before the Senate Committee on Appropriations in January,[10] Chairman Stevens, you asked me to return and discuss these costs issues further. Accordingly, to prepare for this testimony, we updated the information in our April report to include (1) the latest cost estimates from the 24 major departments and agencies and (2) information on releases from the emergency fund subsequent to our prior work.[11]

ESTIMATED YEAR 2000 COSTS CONTINUE TO ESCALATE

As figure 3 indicates, the total estimated costs of ensuring that the computer systems of the 24 major federal agencies perform as expected beyond 1999 more than tripled during the last 2 years—to a total of about $8.7 billion as of last month—up $1.2 billion in the past 3 months alone.

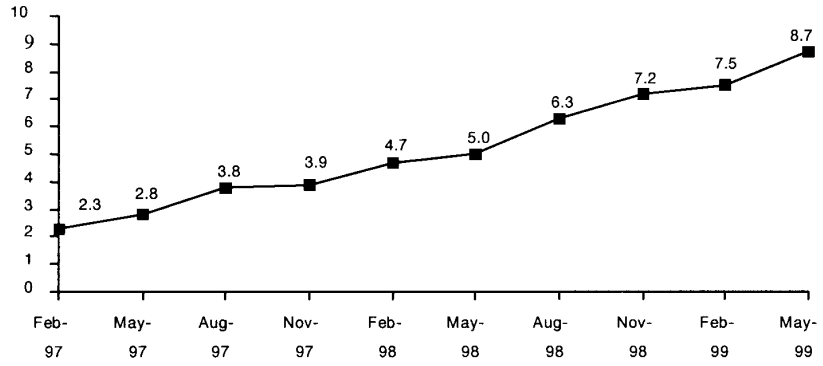
---

[9] *Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds* (GAO/AIMD–99–154, April 28, 1999).

[10] *Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain* (GAO/T–AIMD–99–49, January 20, 1999).

[11] Seven additional agencies received emergency allocations subsequent to our prior work and, therefore, were not included in our April 1999 report.

Figure 3: Estimated Total Reported Year 2000 Costs of the 24 Major Federal Departments/Agencies, February 1997 Through May 1999 (Dollars in Billions)



Note: The August 1998 through May 1999 figures are totals of all individual submissions from the 24 major departments and agencies. In its summary of agency reports, OMB decreased total estimated Year 2000 costs for the 24 major agencies by about $900 million in August 1998, $800 million in November 1998, $779 million in February 1999, and $688 million in May 1999. For the August 1998 costs, OMB did not include all costs in its estimate because, for example, it was still reviewing some of the estimates provided by the agencies. For the November 1998 and February 1999 costs, OMB did not provide explanations in its report for all of the discrepancies between the agency reports and their total estimated Y2K cost figure. However, the OMB reports covering the November 1998 and February 1999 periods did not include $81.3 million and $91.7 million in Transportation and Treasury costs, respectively, that they stated were non-Y2K costs funded from emergency supplemental funds. In OMB's report covering the May 1999 period, it revised the amount of Transportation's non-Y2K costs funded from emergency supplemental funds to $52 million, but Treasury's amount remained the same.

Source: February 1997 data are from OMB's report *Getting Federal Computers Ready for 2000*, February 6, 1997. May 1997 through May 1998 data are from OMB's quarterly reports. The August 1998 through May 1999 data are from the quarterly reports of the 24 major departments and agencies.

Among the agencies that had substantial increases from February 1997 through May 1999 were the Department of Defense—$969.6 million to $3.66 billion (277 percent increase), the Department of the Treasury—$318.5 million to $1.9 billion (497 percent increase), and the Department of Health and Human Services (HHS)—$90.7 million to $1.111 billion (1,125 percent increase).

Several Agencies Did Not Separately Track Actual Year 2000 Costs for Fiscal Years 1996 Through 1998

Reported Year 2000 costs incurred each year from 1996 through 1998 for the 24 major departments and agencies have also grown dramatically. Reported fiscal year 1996 costs were about $72 million,[12] fiscal year 1997 costs were about $830 million, and fiscal year 1998 costs were over $2.7 billion. These reported costs, however, still represent less than half of the total Year 2000 costs of $8.7 billion estimated last month by the 24 major departments and agencies.

While federal agencies reported that their Year 2000 costs from fiscal years 1996 through 1998 were over $3 billion, some agencies reported actual costs while others reported some costs as actual and others as estimates; still others reported just estimates. In particular, at the time of our report,[13] of the 24 major departments and agencies, 7 reported that their fiscal years 1996 through 1998 costs were actual (3 used financial management systems while 4 used reports from component entities to track costs), 5 reported that some costs were actual while others were estimates (e.g., contract costs were actual while labor costs were estimates), 9 reported that

[12] One agency also reported Year 2000 costs that were prior to fiscal year 1996.
[13] GAO/AIMD–99–154, April 28, 1999.

they did not separately track actual costs for fiscal years 1996 through 1998, and 3 did not provide information on cost tracking.

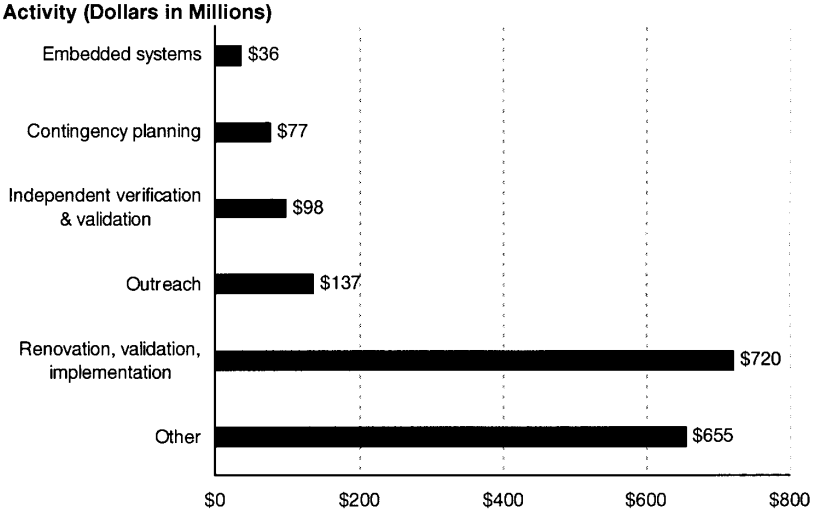
With respect to the nine major agencies that reported not separately tracking actual costs for fiscal years 1996 through 1998, at least three cited as a reason that they were not required to do so. For example, the Department of the Interior reported that aside from the 1999 Y2K Supplemental Funding, the Department has never tracked Y2K funding separately from other appropriated funds, as there has never been any requirement to do so. With respect to tracking of actual costs associated with the emergency funding, five of the nine agencies that reported estimated costs for fiscal years 1996 through 1998 reported that they were tracking, or planned to track, actual costs associated with the emergency funding allocation (the other four agencies did not address whether they were tracking these funds or had not received emergency allocations).

While agencies may not be required to track actual costs of Y2K activities, we believe that the criticality of Year 2000 activities and the significance of the costs—hundreds of million of dollars in some cases—indicate that prudent management practices warrant cost tracking. Specifically, our enterprise readiness guide [14] states that agencies' Year 2000 program management staff should be able to track the cost and schedule of individual Year 2000 projects.

EMERGENCY FUNDS TO BE USED FOR A VARIETY OF PURPOSES

With agencies' estimates of Y2K costs increasing dramatically and with limited time remaining to complete needed actions, many agencies requested emergency funds in fiscal year 1999. Thirty-nine civilian agencies and the District of Columbia have requested—and received—emergency funding for a variety of uses, as shown in figure 4.

Figure 4: Civil Agencies' Proposed Uses for Year 2000 Emergency Funds by Type of Activity (Dollars in Millions)



Note: The other category primarily includes funds for replacement of personal computers and network hardware and software. In their justifications, some organizations said the personal computers and network hardware and software could not be upgraded to be Y2K compliant, and in other cases they determined that it would not be economical to upgrade obsolete equipment. In addition, the total amount in this chart does not equal the total amount allocated because the justification data from two organizations did not equal the total allocations reported by OMB.

Source: GAO analysis based on agency justifications.

In its response to our request, the Department of Defense reported that it is targeting almost $525 million for testing, about $262 million for contingency planning, and $148 million for operational evaluations.

[14] GAO/AIMD–10.1.14, September 1997.

According to their justification submissions to the Congress and OMB, three categories of reasons emerged to explain organizations' requests for emergency funds: (1) new requirements that had not been planned for fiscal year 1999, (2) cost increases to complete ongoing Y2K activities, and (3) the unavailability of regular appropriations for planned Y2K work.

New requirements included outreach and independent verification and validation (IV&V) (cited by 24 organizations), and decisions to replace personal computers and network hardware and software (cited by 23 organizations)—activities not initially in agencies' fiscal year 1999 plans. For example, the Department of Commerce requested about $32 million for IV&V and $25 million for outreach activities not previously anticipated.

Costs for ongoing Y2K activities also increased for 25 organizations, beyond the fiscal year 1999 projections on which budget requests were based. For instance, HHS' Health Care Financing Administration (HCFA) requested over $28 million for IV&V activities because such work had increased beyond the level planned for fiscal year 1999. The Department of Energy requested just under $14 million to accelerate renovation, validation, and implementation.

Finally, in several cases, agencies reported that their budget requests were reduced and Year 2000 emergency funding was utilized to help make up the difference, even though not all of the activities in the original budget request were Y2K-related. While no legislative or statutory requirements explicitly provide for the use of emergency funds as an alternative to general appropriations, the House-Senate conference report on Treasury and Department of State appropriations for fiscal year 1999 acknowledges the need for additional monies to achieve Y2K compliance, and part of the Treasury and General Government Appropriations Act permits use of Treasury funds to achieve Y2K compliance until * * * supplemental appropriations are made available * * *.

COSTS FOR FISCAL YEAR 2000 AND BEYOND

In May 1999, the 24 major departments and agencies estimated their fiscal year 2000 costs for Y2K activities at about $981 million—almost a nine-fold increase from the original fiscal year 2000 estimate of about $111 million provided in February 1997. In addition, in their May 1999 quarterly reports to OMB, three agencies estimated that they would incur about $127.4 million in Year 2000 costs beyond fiscal year 2000.[15] During our work for the House Majority Leader, we asked agencies whether they expected to have Year 2000 costs beyond those projected in their budgets. HHS was the only agency that identified a specific need: it reported that it had begun to identify possible Y2K needs of grantees.

Determining the extent of continued Y2K cost escalation is difficult because of many uncertainties; 10 agencies reported that they had not completed work on their mission-critical systems as of mid-May 1999, many agencies are still planning or undergoing end-to-end testing to ensure that data can be properly transferred and processed among systems, and much work with states and other partners remains. Key factors that could fuel additional cost increases include agencies' determining that they must implement business continuity and contingency plans, or the occurrence of other, unanticipated events due to the Y2K problem that must be addressed. In August 1998, HCFA estimated, for example, that it would need between $311.2 million (most likely scenario) and $536.7 million (pessimistic scenario) to handle emergency situations that could result from the Y2K problem. HCFA reported that the types of activities that these funds would be needed for included (1) unforeseen software, hardware, and telecommunications failures, (2) increased paper claims due to provider or billing companies' inability to transmit electronically, and (3) claims reprocessing to correct erroneous payments. HHS' August 1998, November 1998, February 1999, and May 1999 quarterly reports to OMB included the $311.2 million in contingent HCFA costs in its Year 2000 cost estimate. HHS reported to us that it had requested about $165 million for Y2K activities in its fiscal year 2000 budget request—the amount it estimated that it needed to fund other Year 2000 activities, excluding the implementation of HCFA contingency plans. Consistent with this, OMB has not included HCFA's contingency costs when reporting Y2K costs.

Other agencies could also have higher costs if business continuity and contingency plans need to be implemented. For example, the Department of Education's May 1999 quarterly report stated that it planned to estimate the cost to implement its

[15] The vast majority of these costs were reported by the Department of the Treasury, which reported that the Internal Revenue Service's Y2K costs after fiscal year 2000 would be about $125 million.

contingency plans in the next few months and that these estimates would be likely to increase its fiscal year 2000 and overall Y2K cost estimates. Similarly, the Office of Personnel Management's May 1999 quarterly report said that it would continue to evaluate the need for additional Y2K-related funding for business continuity and contingency plan implementation and will advise OMB of those requirements.

Our guide on business continuity and contingency planning calls on agencies to assess the cost and benefits of identified alternatives.[16] In its May 13 memo requiring agencies to submit high-level business continuity and contingency plans on June 15, OMB stated that agencies should follow our guide in preparing these plans. Accordingly, OMB's review of these plans should consider whether agencies provided estimated business continuity and contingency plan costs. If not, OMB needs to require that this information be provided expeditiously so that it can provide the Congress with information on potential future funding needs.

Additional costs could also be incurred if some states do not complete their Year 2000 work on systems that support federal programs, such as food stamps and Medicaid. Recent information indicates that some state systems are not scheduled to be compliant until the last quarter of 1999. For example, according to OMB's latest quarterly report dated June 15, 1999, three states or U.S. territories did not expect to complete testing of their food stamp systems and four states or U.S. territories did not expect to complete testing of their Medicaid eligibility systems until the last quarter of 1999. Because these deadlines are so close to the turn of the century, the risk of disruption to these states' and territories' programs substantially increases, especially if delays occur or if unexpected problems arise.

If states do not complete their Year 2000 remediation in time, or if those remediation efforts fail, the states would have to implement their business continuity and contingency plans, which could encompass federal government assistance. An example of such assistance is the Department of Labor's April 2, 1999, emergency funding request of $274,000 to design and develop a prototype PC-based system to be used in the event that a state's unemployment insurance system is unusable due to a Y2K-induced problem. In addition, many state-administered federal programs, such as Medicaid and child support enforcement, require the federal government to reimburse states for a percentage of their administrative costs, which would be expected to increase in the event that business continuity and contingency plans are implemented.

PROGRAM AND INFORMATION TECHNOLOGY INITIATIVES DELAYED BY Y2K

While making systems ready for the year 2000 has been an enormous job, other program and information technology needs have not disappeared; in fact, they continue to grow. In particular, because of the Year 2000 problem, agencies or the Congress have delayed implementation of regulatory requirements and planned information technology initiatives. In addition, many agencies have implemented or plan to implement moratoriums on software changes until some time after the rollover to the new century. For example:

—In July 1998, HCFA notified the Congress of its intention to delay implementation of certain provisions of the Balanced Budget Act of 1997 that would have required changes to systems on which Year 2000 modifications were being made. As of June 16, 1999, HCFA had delayed work on seven provisions, in whole or in part, associated with this act in order to meet the Year 2000 challenge. In addition, HCFA reported that it had delayed another information technology initiative because it would have caused an unacceptable resource drain from the Year 2000 effort. According to a HCFA official, the agency is in the process of carefully examining all of the work associated with the Balanced Budget Act of 1997 provisions and the other initiative in order to make decisions as to the order and time frames in which each will be accomplished after the Y2K effort.

—As we reported last year, the level of effort required for the Internal Revenue Service (IRS) to make its information systems compliant is without precedent.[17] Accordingly, as the Senate was debating the IRS Restructuring and Reform Act of 1998, the IRS Commissioner provided the Joint Committee on Taxation with a listing of 28 provisions that given their effective dates, could affect IRS' ability to complete its Y2K work as planned. The final act extended the effective dates for 13 of the 28 provisions about which IRS had expressed concern.

---

[16] GAO/AIMD–10.1.19, August 1998.

[17] *Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts* (GAO/GGD–98–158R, August 4, 1998).

—Some agencies have delayed planned information technology initiatives in order to concentrate on their Year 2000 efforts. In December 1998 we reported that the Department of Housing and Urban Development suspended systems integration work on three mission-critical systems so that the department could focus its resources on completing Y2K renovations.[18] Also, in September 1998, the Department of State imposed a moratorium on non-Year 2000-related system development projects to focus scarce resources on Y2K remediation.

—A backlog of system modifications will have to be addressed subsequent to the change of century. In response to our January 1999 suggestion,[19] OMB issued a memorandum in May stating that agencies should follow a policy that allows system changes only where absolutely necessary because such changes can introduce additional risk into systems that have already been certified as Y2K compliant and could divert resources from other Year 2000 efforts. Accordingly, at least six agencies have established, or plan to establish, moratoriums or restrictions on system changes during parts of 1999 and early 2000.

The total governmentwide volume of program and information technology activities delayed by Y2K efforts is not known; therefore, the potential demand for additional information technology resources in the future is difficult to predict. However, the costs of these delayed activities could be significant. Accordingly, OMB will need to work with the agencies to determine the magnitude of these pent-up demands in order to make informed funding decisions in the future.

In addition to these demands, increased resources will likely be needed for another key issue that has been garnering increased attention—information security. This issue has many dimensions, ranging from national security to economic disruption to privacy considerations. As we reported in September 1998, the expanded amount of audit evidence that has become available since mid-1996 describes widespread and serious weaknesses in adequately protecting federal assets, sensitive information, and critical operations.[20] These weaknesses place critical government operations, such as national security, tax collection, and benefit payments, as well as assets associated with these operations, at great risk of fraud, disruption, and inappropriate disclosures. Further, as we testified in September 1998, the Year 2000 crisis is the most dramatic example yet of why we need to protect critical computer systems because it illustrates the government's widespread dependence on information systems and our vulnerability to their disruption.[21]

Because of the longer-term danger of malicious attack from individuals or groups, it is important that the government design long-term solutions to this and other security risks. Accordingly, in response to recommendations by the President's Commission on Critical Infrastructure Protection, Presidential Decision Directive 63 was issued in May 1998, which, among other provisions, required federal agencies to develop plans for protecting their own critical infrastructure, including cyber-based systems. These plans are currently undergoing review by the Critical Infrastructure Assurance Office, which was established by the Presidential Directive.

LESSONS LEARNED FROM THE GOVERNMENT'S YEAR 2000 EFFORTS CAN BE APPLIED TO FUTURE INFORMATION TECHNOLOGY ACTIVITIES

Throughout government—and likely in the private sector as well—organizations' experiences in addressing Y2K hold valuable lessons about how information technology can best be managed. For many agencies, the threat posed by the Year 2000 problem was a much-needed wake-up call. Because of the urgency of the issue, agencies could not afford to carry on in the same manner that had resulted in over a decade of poor information technology planning and program management. Accordingly, lessons learned from the Year 2000 challenge should be applied to agencies' implementation of the Clinger-Cohen Act of 1996 which, in part, seeks to strengthen executive leadership in information management and institute sound capital investment decision-making to maximize the return on information systems investments. Indeed, the Department of Defense has reported that its response to the Year 2000 problem has become an example of an enterprisewide approach to information technology management advocated by the Clinger-Cohen Act of 1996. It is important that agencies institutionalize the processes that they have established to contend

---

[18] *HUD Information Systems: Improved Management Practices Needed to Control Integration Cost and Schedule* (GAO/AIMD–99–25, December 18, 1998).

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

[20] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD–98–92, September 23, 1998).

[21] *Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets* (GAO/T–AIMD–98–312, September 23, 1998).

with the Year 2000 problem so that future information technology initiatives benefit from this massive effort.

Year 2000 programs provided agencies with the incentive and opportunity to assume control of their information technology environment. In many instances, it forced agencies to inventory their information systems, link those systems to agency core business processes, and jettison systems of marginal value. For example, in response to recommendations in our August 1998 report, the Department of State is in the process of identifying its core business functions and determining the relative importance of each function.[22]

Earlier this year we also reported[23] that the Year 2000 problem provided the opportunity to institutionalize valuable lessons, such as the importance of consistent and persistent top management attention, accompanied by reliable processes and reasonable controls. More specifically, complete and accurate inventories of information systems can facilitate remediation, testing, and validation activities. Information gained from identifying and prioritizing mission-critical systems can further be used to identify and retire duplicative or unproductive systems, and work that has been done to identify and establish controls over data interfaces can help prevent data exchange problems in the future. Similar lessons have been learned at the state level, according to three state Year 2000 project managers. Other critical success factors cited by one of these project managers that could be used in future information technology initiatives are the need to measure performance, outline responsibilities, and ensure accountability.

Another benefit of the Year 2000 effort was the establishment of much-needed information technology policies. Our Year 2000 enterprise readiness guide[24] called on agencies to develop and implement policies, guidelines, and procedures in such critical areas as configuration management, quality assurance, risk management, project scheduling and tracking, and metrics. Several agencies have implemented such policies. For example:

—In April 1999, we reported that according to Postal Service officials, the service is implementing improved processes for documenting software, testing, quality control, and configuration management.[25]

—As part of its Year 2000 effort, HCFA has implemented policies and procedures related to configuration management, quality assurance, risk management, project scheduling and tracking, and performance metrics for its internal systems.

—As we testified in February, the Customs Commissioner has committed to leveraging the agency's Year 2000 experience by extending the level of project management discipline and rigor being employed on the year 2000 to other information technology programs and projects.[26]

Beyond individual agencies, the Year 2000 problem holds lessons in overseeing and managing information technology on a governmentwide basis. In particular, actions taken by the Congress and the Chief Information Officers Council have demonstrated that effective oversight and guidance can have a positive influence on major information technology efforts. Congressional oversight played a crucial role in focusing OMB and agency attention on the Y2K problem. In addition, congressional hearings on international, national, governmentwide, and agency-specific Year 2000 problems exposed the threat that this problem poses to the public. The Chief Information Officers Council has proved useful in addressing governmentwide issues through its Year 2000 Committee; this committee and its subcommittees have dealt with important issues such as best practices, telecommunications, and data exchanges. Continued oversight and guidance from the Congress and the Chief Information Officers Council will be essential to ensuring the future effectiveness of information technology initiatives.

Another lesson that could be adopted in the future is the use of public/private partnerships. To address the Year 2000 problem from a national perspective, the President's Council on Year 2000 Conversion adopted a sector-based focus and has been initiating outreach activities since it became operational last spring. As a re-

---

[22] *Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program* (GAO/AIMD–98–162, August 28, 1998).

[23] *Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement* (GAO/T–AIMD–99–93, February 25, 1999) and *Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed* (GAO/T–AIMD–99–101, March 2, 1999).

[24] GAO/AIMD–10.1.14, September 1997.

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

[26] *Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program* (GAO/T–AIMD–99–85, February 24, 1999).

sult, the Council and federal agencies have partnered with private-sector organizations, such as the North American Electric Reliability Council, to gather information critical to the nation's Year 2000 efforts and to address issues such as contingency planning. In addition, the Chair of the Council has formed a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on crosscutting issues, information-sharing, and appropriate federal responses to potential Year 2000 failures. Other major information technology areas, such as information security, could benefit from such an approach.

In summary, it is clear that Year 2000 expenditures have been significant, sometimes unpredictable, and growing. Emergency supplemental funds are planned for a variety of purposes, including renovation, validation, and implementation of individual systems and the independent verification and validation of these systems. Moreover, Y2K cost growth may continue, especially if business continuity and contingency plans must be put into operation or if state-administered federal program remediation efforts are not completed. While correcting the Y2K problem has been and continues to be costly, the experiences of individual agencies and the government as a whole in meeting this challenge have provided a renewed and needed focus on information systems. We have come to realize how much we depend on them, and have been reminded of how they must be well-managed. As we attempt to meet future information technology and security challenges, these lessons should not be lost.

Messrs. Chairmen, this completes my statement. I would be happy to respond to any questions that you or other members of the Committees 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 willemssenj.aimd@gao.gov. Individuals making key contributions to this testimony included Michael Fruitman, James Hamilton, James Houtz, Linda Lambert, Michael Tovares, and Daniel Wexler.

APPENDIX I.—*Organizations Receiving Emergency Allocations (as of May 1999)*

[In thousands]

Organization	*Amount allocated*
Department of the Treasury	$602,223
Department of Health and Human Services	323,858
Department of Transportation	192,789
Department of Justice	84,396
Department of the Interior	80,347
Department of State	64,918
District of Columbia	64,049
Department of Commerce	57,920
General Services Administration	48,407
Department of Agriculture	46,168
Executive Office of the President—Office of Administration	29,791
Department of Energy [1]	23,840
Department of Labor	17,792
Department of Housing and Urban Development	12,200
Agency for International Development	10,200
United States Information Agency	9,562
Federal Communications Commission	8,516
Securities and Exchange Commission	8,175
Federal Emergency Management Agency	7,352
National Archives and Records Administration	6,662
Small Business Administration	4,840
Smithsonian Institution	4,801
Department of Education	3,846
Federal Trade Commission	2,599
Office of Personnel Management	2,428
Overseas Private Investment Corporation	2,100
United States Holocaust Memorial Council	900
Corporation for National and Community Service	800
Executive Office of the President—Office of the U.S. Trade Representative	498
Export-Import Bank of the United States	400
Railroad Retirement Board	398
National Capital Planning Commission	381

Organization	*Amount allocated*
Commodity Futures Trading Commission	356
Selective Service System	250
Federal Labor Relations Authority	243
African Development Foundation	137
Office of Special Counsel	100
Merit Systems Protection Board	66
Architectural and Transportation Barriers Compliance Board	60
Marine Mammal Commission	38
Total civil agencies	1,724,406
Department of Defense	935,000
Total allocations	2,659,406

[1] This amount does not include $13.65 million that was allocated to the Department of Energy but was not transferred.

Source: OMB.

STATEMENT OF JACOB J. LEW

Chairman BENNETT. Mr. Lew, let's go to you now.

Mr. LEW. Thank you, Mr. Chairman, Senator Stevens. I am delighted to be here with you this morning. I appreciate the invitation to testify on the progress the Federal Government has made in addressing the year 2000 problem.

As you well know, this is a problem that potentially has enormous implications for our Nation. I am very pleased we have been able to work together, and I want to thank Senator Stevens in particular for the cooperation on working to make sure that the funding was in place to make sure that Y2K, as the President has said, will be remembered as the last headache of the 20th Century and not the first crisis of the 21st.

I would like to address three topics today: First, the Federal progress in addressing the Y2K challenge; second, Federal agency costs and funding for these efforts; and third, the next steps to assure that Federal programs that people depend on will not be disrupted.

As you know, last week I sent both committees OMB's ninth quarterly report on Federal agency progress in addressing the Y2K problem. That report shows that Federal agencies continue to make excellent progress in addressing the challenge.

Ninety-three percent of the Federal Government's mission-critical systems are now compliant, which is an increase from 79 percent reported in February. Fourteen of the 24 major Federal departments and agencies now report that they have 100 percent of their mission-critical systems Y2K-compliant, and 9 are over 90 percent.

This progress is attributed to the hard work of thousands of Federal employees and contractors and, I might add, to the rapid and timely availability of funding through the contingent emergency reserve. I would like to thank the committees for ensuring Federal agencies have had adequate funds to address Y2K remediation to date.

While much work remains to be done, we fully expect that all of the Government's mission-critical systems will be Y2K-compliant before January 1, 2000. For some time, fixing the Y2K problem has been the agency's number one information technology priority. Additionally, agencies are minimizing any kind of changes to their

systems that are not related to Y2K in order to ensure that they will be able to maintain the schedules that they have set.

Based on guidance that we sent out just last month, agencies are using change management processes to ensure that any new IT requirement changes and system changes are minimized while they are completing dealing with the Y2K problem. This effort will ensure that agencies set realistic goals for the completion of their work, and will enable them and us to measure their progress against their own goals. As I said, we are confident that every mission-critical system will be ready for the year 2000.

As you know, last September, the administration requested a fiscal year 1998 supplemental appropriation for $3,250 million in contingency emergency funding to address urgent emerging needs related to Y2K activities. The 1999 omnibus bill provided contingent funding of $2.25 billion for nondefense activities and $1.1 billion for defense-related activities. OMB is responsible for allocating the nondefense contingent emergency reserve and for working with the Department of Defense (DOD) on its share as well.

To date, $1,768 million has been allocated from the nondefense reserve, and $14 million has been returned to the reserve at the request of the House Appropriations Committee. Therefore, $486 million remains in the reserve for unforeseen requirements. Of the $1.1 billion provided for defense-related activities, $935 million has been released, and $165 million remains in the reserve.

OMB has worked with the agencies on an ongoing basis to evaluate the total Y2K requirements and to determine how to best utilize available nondefense funding for Y2K. First, OMB made certain that agencies received funding for activities that were requested in the President's fiscal year 1999 budget, but were directed to be funded from the contingent emergency reserve.

As you know, there were a number of specifically mentioned items. Since then, agencies have been asked to forward requests for contingent emergency funding on an as-needed basis. These requests were then reviewed by OMB to ensure that the requested funding meets the criteria for release. First, that the funding is Y2K-related, and is the most cost-effective option to facilitate compliance; second, that it addresses an unforeseen need, not one accounted for within existing agency plans; and, third, that it cannot be accommodated within appropriated levels for fiscal year 1999. Finally, that they cannot be addressed using unobligated balances of already-released Y2K funds.

Once the funds are allocated, OMB tracks the Y2K-related expenditures to confirm that appropriate progress is being made, and that each agency can cogently explain its cost levels and cost changes. All agencies that received emergency funding have forwarded data on obligations to date to OMB, and this data has informed our consideration of subsequent emergency requests.

In the first OMB quarterly report issued in February 1997, we estimated that the cost of Y2K compliance would be $2.3 billion. Initially, it was thought that fixing the problem would primarily involve mainframe computers and legacy applications. However, as we and others learned in the course of remediation, the problem is far more complex, involving desktop personal computers, embedded chips, and telecommunications components.

Cost increases from the first to the fourth OMB quarterly report—that would be through March 1998, totalling $2.4 billion—resulted from better understanding of the scope of the problem and increasing agency attention to the cost estimates.

Since the broader universe of Y2K remediation was clearly established, costs have remained within a much more predictable band. From the fourth OMB quarterly report in March 1998, to the ninth OMB quarterly report just this month, cost reports reported change by 4.7 percent of the 3-year total. Of this, estimates for defense have changed by 3.6 percent of the 3-year total.

The increase in fiscal year 1999 funding, $2.8 billion between the fourth and ninth OMB quarterly reports, has reported activities that have been subjected to a rigorous policy review. Most of the cost increases can be attributed to specific activities, remediation of information technology systems, testing to ensure that systems are Y2K compliant, replacement of embedded computer chips, and creation and verification of business continuity plans.

Fiscal year 2000 costs, which have increased by $509 million over the same period, are primarily for Y2K project offices to manage and monitor the transition into 2000, as well as for retesting and recertifying contingency plans. The details of agency spending plans continue to be made available for your review as the process moves forward.

Most of the work on fixing mission-critical systems is completed, so OMB will focus its system-readiness on ensuring the readiness of individual systems. In addition, OMB and the agencies are beginning to focus on two new priorities: ensuring the readiness of Federal programs, particularly 43 high-impact programs that we have identified, and planning for business continuity and contingencies.

We must make sure that the Federal programs, particularly those that have a direct and immediate effect on health, safety and well-being of the public, function smoothly. As I have just related to you, we are confident that the mission-critical systems will be ready, but because Federal programs partner with other entities. It is critically important that all partners are working together to ensure that the programs they support will be ready.

The critical task is to make sure that not just systems but the programs they support will be ready. Accordingly, I have asked agencies to take this additional step.

OMB has also identified 43 high-impact, federally supported programs, and directed Federal agencies to take the lead on working with others to ensure that programs critical to health, safety, and well-being will provide uninterrupted service. Agencies have also been asked to help partners develop year 2000 plans if they have not already done so to ensure that these programs will operate effectively.

Agencies are reporting to us monthly, and will demonstrate the readiness of each program by September 30, 1999. 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.

Agencies have identified their core business functions and are using this as a basis for developing business continuity and contin-

gency plans which will ensure that these core business functions will operate smoothly no matter what kinds of glitches occur in agency systems or with agency partners.

Let me make it clear, we do not anticipate disastrous consequences as a result of the year 2000 computer problem in Federal systems. However, it is possible there will be problems that result in minor disruptions to the way agencies operate. Agencies are prioritizing functions and systems and work-arounds and backup plans are being established as contingencies.

On May 13, I issued guidance on this subject, asking all agencies, including small and independent agencies, to submit to OMB by June 15 their business continuity and contingency plans. These plans are an increasingly important component of agency progress. Like a good insurance policy, a sound plan is important no matter how well you are taking care of your system. I have directed agencies to use the GAO guidance in preparing their plans.

Additionally, many agencies are working closely with their inspectors general and their expert contractors in the development and testing of these plans. OMB is reviewing the high-level business continuity and contingency plan (BCCP) of agencies and will provide feedback and guidance to the agencies on an individual basis.

In conclusion, during the 192 days remaining before the year 2000, we plan to complete work on the remaining mission-critical systems and on other Federal systems. We will conduct end-to-end testing with the States and other key partners, placing special emphasis on the readiness of programs that have a direct and immediate impact on public health, safety, and well-being.

We will complete and test business continuity and contingency plans as insurance against any disruptions related to Y2K failures. We will promote Y2K awareness with State, local, and tribal governments with the private sector and with other nations.

PREPARED STATEMENT

Again, I want to thank you for the opportunity for allowing me to share this information with you. The administration continues to treat this challenge with the high level of attention that it deserves. We have enjoyed the cooperative relationship that we have had with this committee and with the Appropriations Committee to work together on this problem.

Thank you.

[The statement follows:]

PREPARED STATEMENT OF JACOB J. LEW

Good morning, Chairman Stevens, Chairman Bennett, Senator Byrd, and Senator Dodd. I am pleased to appear before the Committees to discuss the Federal Government's progress in addressing one of the most complex management challenges it has ever faced, the year 2000 problem. The Federal Government is not alone in addressing this challenge, as the Senate wisely recognized last year when it formed the Senate Special Committee on the Year 2000 Technology Problem. This is a problem with potentially enormous implications for our Nation. Every sector of our economy and all organizations large and small must work together so that we can, as the President said in his State of the Union Address, make sure that the Y2K computer bug will be remembered as the last headache of the 20th century, not the first crisis of the 21st.

Today, I would like to address three topics. First, I will describe Federal progress in addressing the Y2K challenge. Second, I will discuss Federal agency costs and funding for these efforts. Third, I will describe our next steps to assure that Federal programs that people depend upon will not be disrupted. These next steps include focusing on completion of individual systems, ensuring the readiness of Federal programs, and completion of business continuity and contingency plans.

FEDERAL PROGRESS

As you know, the Federal Government has been working for more than three years on this problem. Last week I sent to Congress OMB's ninth quarterly report on Federal agency progress in addressing the Year 2000 problem. That report shows that Federal agencies continue to make excellent progress in addressing this challenge. In particular, it shows that 93 percent of the Federal Government's mission critical systems are now compliant, an increase from 79 percent reported in February.

Fourteen of the 24 major Federal departments and agencies now report that 100 percent of their mission critical systems are Y2K compliant. These agencies are: the Departments of Education, Housing and Urban Development, Interior, Labor, State, and Veterans Affairs; the Environmental Protection Agency, the Federal Emergency Management Agency, the General Services Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Office of Personnel Management, the Social Security Administration, and the Small Business Administration.

In addition, two agencies, Commerce and NASA, report that 99 percent of their mission critical systems are compliant and that they expect to be finished soon. Three agencies, the Departments of Agriculture, Energy, and Health and Human Services, are between 96 and 97 percent compliant. Four agencies report that between 90 and 94 percent of their mission critical systems are compliant, including the Departments of Justice and Transportation at 92 percent. The Department of Defense reports that 87 percent of its systems are compliant, while the U.S. Agency for International Development has completed implementation of three of its seven mission critical systems.

From a base of 6,190 mission critical systems at this time, 410 mission critical systems remain to be finished, down from 1,354 in the last report. The compliant systems include those that have been repaired or replaced as well as systems that were already compliant. Of the mission critical systems that remain to be finished, 87 (82 percent) are being repaired, 35 (10 percent) are being replaced, and 24 (eight percent) are being retired. We are monitoring the completion of each remaining system through monthly reports from the agencies.

This progress is a tribute to the hard, skillful, and dedicated work of thousands of Federal employees and contractors. Moreover, the rapid availability of funds through the contingent emergency reserve has been key to ensuring progress. I would like to thank the Committees for ensuring that Federal agencies will not fail to meet the Year 2000 deadline because of lack of adequate funding.

While much work remains to be done, we fully expect that all of the Government's mission critical systems will be Y2K compliant before January 1, 2000. For some time, fixing the Year 2000 problem has been the agencies' number one information technology (IT) priority, as other IT projects are being delayed until the Y2K work is done. This action has been managed throughout OMB's budget process.

Additionally, agencies are minimizing any kind of changes to their systems unrelated to Y2K in order to ensure that they will be able to maintain the schedules they have set for completion of their work. Changes not only divert resources from fixing the Y2K problem, but may also undo Y2K fixes. Based on guidance I issued on May 14, 1999, "Minimizing Regulatory and Information Technology Requirements," (M–99–17), agencies are using change management processes to ensure that new IT requirements or changes to IT systems are minimized.

Again, this effort will ensure that agencies set realistic goals for the completion of their work and will enable them—and us—to measure their progress against their own goals. Agencies are working hard to finish fixing their systems, and we are confident that every mission critical system will be ready for the year 2000.

Y2K COSTS AND FUNDING

First and foremost, I want to recognize that the transition into the Year 2000 has posed a unique challenge. Formulating the Federal response has required a great deal of attention, hard work, and flexibility. In advance of my more detailed comments on this subject, let me thank you for all of your work and leadership in helping to ensure that sufficient funds are available in a timely manner to address Y2K remediation. As we have scrutinized agency requests and funded the most critical

ones, the utility of this funding mechanism has been proven many times. Simply put, without such a fund, many Federal agencies would not be nearly as far along in their efforts as they are today.

I would also like to emphasize that the Administration's strategy for monitoring Government-wide progress on Y2K has been predicated on agency accountability. We have systematically monitored agency progress using a range of performance measures—compliance of mission critical systems, status of mission critical systems being repaired, progress on high impact programs, etc., as well as agency Y2K cost estimates. These measures are linked, and together provide the most accurate picture of the Government's overall readiness. On a quarterly basis (or more frequently, if needed), agencies have been required to update OMB on their Y2K progress and to explain all significant changes in these measures.

We have tried to strike the appropriate balance to ensure agency accountability without diverting vital resources from Y2K compliance activities to reporting requirements. In addition, the Administration has tried to be as forthright as possible in sharing information about Y2K readiness. OMB has directed that agency quarterly reports and detailed spending plans be forwarded to Congress, and we have appreciated your input as we have worked together to address the challenge posed by Y2K.

As you know, last September the Administration requested an fiscal year 1998 supplemental appropriation for $3.25 billion in contingent emergency funding to address urgent, emerging needs associated with Y2K conversion activities. This request was consistent with Senate action to that point. The Omnibus bill provided contingent emergency funding of $2.25 billion for non-defense activities and $1.1 billion for defense-related activities for Y2K computer conversion. As you also know, OMB is responsible for allocating the non-defense contingent emergency reserve. To date, $1.768 billion has been allocated from the non-defense reserve, and $14 million has been returned to the reserve at the request of the House Appropriations Committee. Therefore, $496 remains in reserve for unforeseen requirements. Of the $1.1 billion provided for defense-related activities, $935 million has been released and $165 million remains in reserve.

In order to determine how to best utilize all available non-defense funding for Y2K—both base appropriations and emergency funding—OMB has worked with agencies on an ongoing basis to evaluate total Y2K requirements. First, OMB made certain that agencies received funding for activities that were requested in the President's Fiscal Year 1999 Budget, but were directed to be funded from the contingent emergency reserve. Since then, agencies have been asked to forward requests for contingent emergency funding on an as-needed basis. These requests are then reviewed by OMB examiners from both the Resource Management Offices (RMOs)—liaisons to the individual agencies—and analysts from our Information Policy and Technology Branch. In combination, they review these requests to ensure that requested funding is:

—Y2K-related and is the most cost-effective option to facilitate compliance.
—Addresses an unforeseen need, not one accounted for within existing agency plans.
—Cannot be accommodated within appropriated levels for fiscal year 1999.
—Cannot be addressed using unobligated balances of Y2K emergency funding.

In some cases, funds have also been requested to support outreach to non-Federal entities in support of the efforts of the President's Council on Year 2000 Conversion.

Once reviewed and discussed with the affected agency, OMB staff make recommendations to OMB policy officials. These levels are then finalized and included in an emergency release. As you know, pursuant to last Omnibus Act, detailed information on each affected agency's spending plan, as well as an account-by-account breakdown of the request as a whole, is provided to your and other Committees. The funds in the release are not made available to the agencies until 15 days after the transmittal.

Once the funds are allocated, each Resource Management Office has been tasked with tracking the Y2K-related expenditures for the agencies it oversees, including emergency expenditures. At a minimum, the RMOs review the agency quarterly report to confirm that appropriate progress is being made and that each agency can cogently explain its cost levels and cost changes. Then, depending on an agency's status, RMOs have used different methods to track Y2K-related spending. All agencies that have received emergency funding have forwarded data on obligations to date to their RMOs. This data has informed our consideration of subsequent emergency requests, and has resulted in several reprogramming requests rather than additional releases. For example, in the Department of Health and Human Services, we recently reprogrammed funds from HCFA to the Administration for Children

and Families. More reprogramming actions may be forthcoming as agencies further refine their estimates for fiscal year 1999 and 2000.

In addition, some RMOs monitor Y2K-related obligations and/or outlays on a more regular basis, and require detailed information on the expenditure of both base and emergency resources. Finally, because of their unique period of availability (fiscal year 1999-fiscal year 2001), emergency funds are very transparent in terms of budget execution. The RMOs have been given discretion in terms of treatment of both base and emergency funds in the apportionment process, as is OMB's general policy.

Your Committees have asked me to focus on the cost increases since the 1st OMB Y2K Quarterly Report, which was issued February 1997. In that report, the five year (fiscal years 1996–2000) Federal cost of Y2K was reported estimated at $2.3 billion. However, it is now clear that in the first quarterly report, we were not fully aware of the magnitude of the year 2000 problem. Initially, it was thought that fixing the problem would primarily involve mainframe computers and legacy applications.

However, as we and others learned in the course or remediation, the problem was far more complex, involving desktop personal computers, embedded chips, and telecommunications components. Cost increases from the 1st to 4th OMB Quarterly Report (through March 1998), totaling $2.4 billion, resulted from a better understanding of the scope of the problem and increasing agency attention on the cost estimates. It is important to note that until fiscal year 1999 agencies funded their year 2000 costs exclusively out of base appropriations. Prior to the availability of emergency funding, all costs increases were absorbed within agency operating budgets.

Since the broader universe of Y2K remediation was clearly established, costs have remained within a more predictable band. From the 4th OMB Quarterly Report (March 1998) to the 9th OMB Quarterly Report (June 1999), costs reported for fiscal years 1996–1998 changed by $164 million, or 4.7 percent of the three-year total. Of this, estimates for Defense have changed by $128 million, or 3.6 percent of the three-year total. Since last March, then, cost estimates for non-defense agencies for fiscal years 1996–1998 for have changed by a little more than one percent.

The increase in fiscal year 1999 funding, $2.8 billion between the 4th and 9th OMB Quarterly Reports, has supported activities that have been subjected to the rigorous policy review that I have discussed. Most of the cost increases can be attributed to specific activities: remediation for information technology systems, testing to ensure that systems are Y2K compliant, replacement of embedded computer chips, and creation and verification of BCCPs. I am confident that this funding has helped to ensure that important Federal programs will have a smooth transition into the year 2000. Fiscal year 2000 costs, which have increased by $509 million over the same period, are primarily for Y2K project offices to manage and monitor the transition into 2000, as well as for retesting and recertifying contingency plans. The details of agency spending plans continue to be made available for your review as this process moves forward.

I would now like to turn to another issue that I have been asked to address: the difference between agency estimates and actual costs. I believe that this question stems from the cost table in each OMB Quarterly Report. In that table, past years (fiscal years 1996–1998) are characterized as estimates even though, as you know, the budgetary data for those years reflects actual expenditures. With OMB's approval, agencies have refined the universe of Y2K-related costs since fiscal year 1996. As an activity is added to the Y2K universe, we want to make certain that we are capturing the five-year cost of that activity. For example, a Department may not have reported embedded chip replacement as part of their initial Y2K estimate. However, they later received guidance to do so. In such a case, OMB has worked with the Department to verify that the multi-year cost of embedded chip replacement was being reported. If this required changing an estimate in a past fiscal year, agencies did so with OMB approval. At the same time, future year estimates may have been adjusted to account for newly recognized activities. Thus, although the budget data for fiscal years 1996–1998 are actuals, since recognition of the scope of the Y2K problem has changed over time, OMB has not asked for or characterized costs for those years as actuals.

Another component of this issue is that Y2K-related expenses can be aggregated at a level below or above budget accounts. Y2K-related expenses are embedded in broader operating budgets. We have worked to ensure that we are capturing Y2K-related costs and that agencies are making defensible and standardized assumptions about these costs. Conversely, we are trying to filter out activities that were wholly planned for and would have been implemented regardless of Y2K.

NEXT STEPS

As I stated earlier, now that most of the work on fixing mission critical systems is completed, OMB will shift its focus from aggregate figures for system readiness to ensuring the readiness of individual systems. In addition, OMB and the agencies are beginning to focus on two new priorities.

—Ensuring the readiness of Federal programs, particularly 43 high impact programs that we have identified.

—Planning for business continuity and contingencies.

Ensuring the Readiness of Federal Programs

While we have made excellent progress in preparing our systems, we are not yet done. We must make sure that Federal programs, particularly those that have a direct and immediate affect on the health, safety, and well-being of the public, function smoothly. As I have just related to you, we are confident that critical systems will be ready. But because Federal programs partner with other entities, including other Federal agencies; State, Tribal, and local governments; banks; contractors; vendors; and other entities; it is critically important to ensure that all partners are working together to ensure that the program they support will be ready. The critical task is to make sure that not just systems, but the programs they support, will be ready.

Accordingly, on March 26, 1999, I asked agencies to take this next step. I also identified 42 "high impact" Federally supported programs and directed Federal agencies to take the lead on working with other Federal agencies, State, Tribal, and local governments, contractors, banks, and others to ensure that programs critical to public health, safety, and well-being will provide uninterrupted services. Examples include Medicare and Unemployment Insurance. The list was subsequently revised to include the National Crime Information Center at the Department of Justice, bringing the total to 43.

Agencies have also been asked to help partners develop year 2000 plans if they have not already done so to ensure that these programs will operate effectively. Such plans are to include end-to-end testing, developing complementary business continuity and contingency plans, and sharing key information on readiness with partner organizations and with the public. Agencies are reporting to us monthly and will demonstrate the readiness of each program by September 30, 1999. A table of the programs, including the partners agencies are working with is included last week's quarterly report.

Business Continuity and Contingency Planning

Although we expect all Federal mission critical systems to be ready by January 1, 2000, and although we are prepared to demonstrate the readiness of a number of critical programs, it is still important that every agency, no matter how well prepared, have a business continuity and contingency plan (BCCP) in place.

Agencies have identified their core business functions and are using these as a basis for developing business continuity and contingency plans, which will ensure that these core business functions will operate smoothly, no matter what glitch may occur in an agencies' systems or with an agencies' partners. While we are confident that the measures taken for Y2K compliance are sound, the chance remains that, despite testing, a bug may still slip through. Furthermore, elements beyond an agency's control are at risk from the Y2K problem as well. For example, bad data from a data exchange partner or the inability of a vendor to provide key supplies could disrupt work at an agency.

Let me make it clear that we do not anticipate any disastrous consequences as a result of year 2000 computer problems in Federal systems. It is possible, and even likely in some situations, that there will be glitches in systems that result in minor disruptions to the ways that agencies operate. Accordingly, for each core business function and its associated systems, agencies have identified risk factors, and assigned them a probability rating as well as an impact rating. The agencies use these ratings to prioritize functions and systems. Work-arounds and back-up plans are established as contingencies.

Although we do not expect any disasters, it is always wise to prepare for the worst. Since the 1970s, agencies have been required to have in place Continuity of Operations plans (COOP plans), to address such emergencies. In the event of a disaster, whether related to Y2K or to a national emergency, such as a terrorist attack or regional weather emergency such as a tornado or violent snowstorm, agencies are using their COOP plans to ensure that the agency will continue to function. I also asked agencies to ensure that the development of their BCCP was coordinated with pending revisions to each agency's COOP plan. Again, although we do not expect

any kind of Y2K disaster, agencies are developing plans, in coordination with their BCCPs, to address this contingency.

On May 13, 1999, I issued guidance on this subject, "Business Continuity and Contingency Planning for the Year 2000," (M99–16). This memorandum asked all agencies, including small and independent agencies, to submit to OMB by June 15 their business continuity and contingency plans (BCCPs). This memorandum also identified a number of infrastructure areas for which agencies should make common assumptions, such as electric power, financial services, and public voice and data communications. This common assumption is that there will be no nation-wide disruptions within these infrastructure services.

By setting these risk areas aside from agencies' business continuity and contingency planning, agencies are able to focus on ensuring that their core business functions and affiliated systems will work. In the extremely unlikely event that a catastrophic emergency occurs that damages local infrastructure, communications, or the agency building itself—whether caused by Y2K, or by a natural disaster, terrorism, or war—the agency's COOP plan will address these contingencies.

On the international side, the State Department is leading a working group of those agencies with employees overseas in order to develop risk assumptions and appropriate responses, to be used in the development and refinement of those programs' BCCPs.

BCCPs are an increasingly important component of agency progress. Like a good insurance policy, a sound plan is important, no matter how well you have taken care of your systems. To ensure quality and consistency, I have directed agencies to use the General Accounting Office's (GAO) guidance on this subject in preparing their plans. Additionally, many agencies are working closely with their Inspectors General and/or expert contractors in the development and testing of these plans. Finally, OMB is reviewing the high-level BCCPs of agencies, which were due June 15, and will provide feedback and guidance to the agencies on an individual basis.

Prepayment

As part of their contingency planning, some agencies have explored the possibility of making some payments in December that would otherwise be due in January to beneficiaries, contractors, and others. However, the Administration has determined that such actions are not necessary at this time, given the level of readiness of agency payment systems and agency business continuity and contingency plans. Moreover, the extensive downside risk to prepayment mitigates strongly against implementing this contingency plan in all but the most exceptional circumstances.

First, and most importantly, issuing such payments early would require reprogramming of payroll and other financial management systems. I have previously stated that any changes to systems should be minimized as they not only divert resources from fixing the Y2K problem, but also may undo Y2K fixes. It would be highly irresponsible to implement a contingency plan that could worsen the year 2000 problem.

Second, making early payments would have tax implications for individuals and businesses. Undoing any tax implications would require legislative changes for the Internal Revenue Service, which in turn would be required to make changes to the tax code and to their systems. All of these actions would be both costly and time-consuming.

Third, such actions could easily be interpreted by the public as an overall sign of lack of confidence in the ability of the Government to make its payments after January 1. Such a signal could prove disastrous for the national economy as panicked citizens turn to withdrawing their currency in anticipation of a currency shortage. This sort of panic is a self-fulfilling prophecy. Public panic and overreaction is a problem far larger than the technology problem and something we are very concerned about.

Finally, even allowing prepayment in extremely limited areas increases pressure to provide early payment for everyone.

Any uncertainty about the readiness of agencies to make benefits payments should be mitigated by continuing to focus on fixing and testing systems. Agencies should also consider alternative contingency plans that do not introduce such high levels of Y2K risk into systems or that could propagate public panic.

Despite these concerns, however, there may be a few rare instances in which early payment is the best option. In any such instances, agencies may request authority from OMB to pay certain benefits early if certain criteria are met. These include demonstration that there will be substantial harm to individuals from not getting a timely payment, a high likelihood that timely payments (either by normal program operation or through a contingency) will not be made, assurance that early payments made will be targeted only to those recipients who would be harmed, and

that early payment will substantially mitigate the harm. The agency must also be willing to make a public announcement of these decisions and to work with the Department of Treasury so that adequate cash management practices are maintained. Throughout the remainder of the year, we will continue to review this matter with agencies.

CONCLUSIONS

In conclusion, during the 192 days remaining before the year 2000, we plan to:
—Complete work on remaining mission critical systems and on other Federal systems.
—Conduct end-to-end testing with the States and other key partners, placing special emphasis on ensuring the readiness of programs that have a direct and immediate impact on public health, safety, and well-being.
—Complete and test business continuity and contingency plans as insurance against any disruptions related to Y2K failures.
—Promote Y2K awareness with State, local, and Tribal governments, with the private sector, and with other Nations.

Thank you for the opportunity to allow me to share information with you on the Administration's progress. The Administration continues to treat this challenge with the direct, high-level attention it deserves. The additional focus on the year 2000 problem by the President, Congress, and the public has resulted in agencies focusing management attention on the issue and taking a close look at their resource needs. The Year 2000 contingent emergency reserve has helped ensure that agencies have access to funds to facilitate their work. OMB remains committed to working with the Committees and Congress on this critical issue. I would be pleased to answer any questions you may have.

NUMBER OF FEDERAL MISSION-CRITICAL SYSTEMS THAT ARE Y2K COMPLIANT

Chairman BENNETT. Thank you very much. You use the phrase, 93 percent compliant as of June. That is the same number that John Koskinan reported in the end of March. Are you simply reporting that number, or are you telling us subliminally that there has been no progress from the end of March?

Mr. LEW. Well, the February report we submitted was at 79 percent, so from February until now we have gone to 93 percent. I think you have to look at the other areas where we have closed in on the 100 percent, and the fact that we have 14 agencies that are now 90 percent compliant or better.

Chairman BENNETT. I do not want to quibble numbers with you, but there are enough people who follow this on the Internet. We need to be careful here and give you an opportunity to focus on it.

The President set March 31 as the deadline by which every Federal agency was supposed to be 100-percent compliant. A number of agencies missed that deadline, and John Koskinan reported when that deadline came, a 93-percent overall number for the Federal Government. We are now 60 days beyond, 75 days beyond March 31, and you are using the 93 percent number. Are you using the 93 percent number because that is the last number we have and it comes as of March 31, or are you telling us that we are stuck, as of March 31, and we are still at the 93 percent number?

Mr. LEW. No, Senator, I am certainly not saying we are stuck. The numbers I am using are based on the ninth quarterly report we submitted to you last week. John Koskinan was basing his comments in March on estimates which were not yet in our quarterly report system and may have anticipated some of the progress that has been made.

Chairman BENNETT. So you are saying the 93 percent at the end of March was not fully accurate.

Mr. LEW. Well, I am saying it was an estimate. The numbers in the quarterly report are based on the rigorous review that we do of each agency's reporting, and the estimate in between reports is necessarily based on—I do not want to say less accurate data, but estimates are different than actual numbers, as we will probably discuss in other regards as well.

I think the important thing to focus on is that we are making continuous progress and very rapid progress in the areas where we had the most catching up to do. Look at the largest and most complicated departments, an agency like HHS with HCFA, where they have made tremendous progress such that HCFA is now compliant. Some of the resources that we thought would be needed for HCFA have actually been shifted over to other HHS activities because HCFA has completed most of its work.

You look at the Defense Department, where they have more systems than anywhere else. They are down to the point now where they are working on their systems that are not yet in service, the new technologies that have not yet been put in place. They are making great progress to ensure that they have continuity and that they do not have the kinds of delays that we had feared, if they could not get new systems to be compliant.

So I think we are continuing to make very good progress. I do not want to suggest for a minute we do not have a lot of work to do. We will be working very hard for the remainder of the time we have, and I think you will see in May and June and July and August considerable progress in each of the months.

As I looked over the report, I was struck at how many agencies expected to be reporting substantial progress in the very near-term timeframe. Now, I am not surprised by that. We would hope, given that we are 192 days away from the year 2000, that we would be seeing ourselves closing down problems at a rapid pace, and that is what our reports are showing, so I think we have continued to move forward. If there is some confusion between the numbers that were based on estimates and the quarterly reports, I would be happy to go through it outside of the hearing and look at what might lie behind that.

Chairman BENNETT. I think it is important to get it very clear, because one of our problems with respect to Y2K is the question of public confidence, and there are those who have attacked this committee for being too alarmist. Saying we are going to set off a panic that will be worse than the problem. Obviously, I do not accept that criticism. I think the committee has been responsible, but again, back to the public perception here.

The President said 1 year, 1½ years ago when he made his statement on Y2K, I believe it was at the National Science Foundation, that every Federal agency would be 100 percent compliant by March 31, 1999. We did not make that. I applauded that as the goal at the time he said it, and said that is the right goal, and that is what we should strive for, but privately I thought, we are not going to make it.

All right, we did not. Now, the number that was put out by the administration as of that date was 93 percent, and we were told the new target date for 100-percent compliance is June 30. Now, June 30 is 2 weeks away, and if there is an announcement as of

June 30 that we are 93 percent compliant, people who will not go into the details that you have shared with us here are going to start to panic and say, the Federal Government is not making it, has not had any progress.

So without asking for a specific response here—and I will be talking with John Koskinan tomorrow, we talk every week either face-to-face or on the phone—I will just signal that there is that public perception problem that has to be dealt with. Either the statement is made as of the end of June we are now up to 97, or whatever the number, or hey, we need to revise what was said in March that it was an estimate. We now know that the reality is that—I mean, we adjust statements around here all the time, when more data comes in. This is where we were in March, and we have made this much progress to June 30.

I am gathering from your testimony that we will not be able to announce on June 30 that we are 100-percent compliant.

Mr. LEW. No, I do not think we will be able to announce we are 100-percent compliant, but I am hopeful we will be able to show more continuing progress. Obviously, from our report last week to the end of June is a fairly short window, so I do not want to raise unreasonable expectations about how much we will be able to say, over what is really a matter of a few weeks, but we are not just doing quarterly reports.

We are keeping daily contact, as you mentioned. We are in regular contact with the committee as well. If there is a concern that we are not putting out frequent enough benchmarks of how much progress is made in a way that can be tracked clearly by the public, that is something we can look into.

I think the underlying facts are better than the impression that you are suggesting, which means we have a communication problem.

Chairman BENNETT. I think there are too, and I think it is a joint responsibility of the Congress and the administration to get the information out so that we do avoid panic.

Yes, Mr. Walker.

Mr. WALKER. Mr. Chairman, for the benefit of you and the committee, based upon self-reported data that we see from the agencies as of May 14, the number was 94 percent, and hopefully Jack will end up having more recent numbers in the near future.

Second, I have asked Joel Willemssen to join me, Mr. Chairman, in part because of his expertise and in part because of the recognition of the work that he and his team has done in the Y2K area working with your committee and others.

HAS THE Y2K PROBLEM UNDERMINED COMPUTER SECURITY?

Chairman BENNETT. Thank you, and the record will show, Mr. Willemssen, that you are at the table and available. If the time comes that you need to speak up, you will be identified for the record.

Let me get a dialogue going between the two witnesses for just a minute before I call on Senator Stevens. Mr. Walker, I was impressed by your statement in two areas, both of which I agree with absolutely. The first one had to do with pent-up demand. We are finding that in the private sector as well that, as we do our hear-

ings in the special committee, more and more industries are saying they are going to have no more IT activity the last half of 1999 because we are concentrating so heavily on testing and final installation of Y2K solutions, and since we do not want any new initiatives, there will be a significant pent-up demand.

Some high tech companies on the reverse side of that are reporting anticipation of lower sales in the third and fourth quarters of 1999, because they say that customers are so wrapped up in Y2K they do not have the time to look at anything now, and then it will explode in 2000.

Now, if we have serious Y2K problems, the preoccupation of Y2K will not carry over in the first and second quarters of 2000. The pent-up demand will not hit until they are taken care of, but is very much there. I would think, Mr. Lew, that it has got to be a real planning headache for OMB, and it is information that we in the Congress need as we face the appropriations process.

Because, as Chairman Stevens can tell you more eloquently than anybody, dealing with the caps and the challenges of the appropriations process is very, very difficult. To say, "Well, there is all this pent-up demand, where we are going to need more funds for Y2K capability," and that is caused by the slow-down, or the interruption, rather, of the normal flow of things as result of Y2K, that can be very serious business for the Appropriations Committee and its various subcommittees.

The second issue that I would like you to talk about, although perhaps not in the same breath, but just to alert you to the other thing I am concerned about, is this question of security. Now, Y2K has made a tremendous impact on me at least, as it has forced me to confront what will happen to our society if the computers fail.

Now, we are talking about close to $9 billion, and it may get to $10 billion by the time we are through, just to keep the Federal computers from failing. This amount in the general economy is—pick a number—somewhere between $50 and $100 billion that private entities and the State and local governments will spend just to keep the computers from failing. The potential for failure is a problem that is built into the software.

The potential for failure as a result of a deliberate act on the part of a terrorist group is just as great, and will cause just as much devastation as the Y2K. Right now, most of the attack, cyber attack if you want to call it that, is coming at the Defense Department. I have had conversations with Secretary Hamre about that and will continue to have those conversations. The Defense Department is hardening itself against those kinds of attacks and is building some expertise for dealing with them.

The rest of the economy is not, as nearly as I can tell, and some Government agencies are not. I do not want to give anybody any ideas, but I can see a scenario where a terrorist group says, "all right, if we want to take down the great Satan, we will not attack their military, we will destroy their ability to distribute welfare checks, and we can do that much more easily than we can hack into the military computers.

If we want to cause disruption in America, we will shut down the power grid, we will shut down the telephone system, we will interrupt the flow of commerce by taking down the Fed wire."

A whole series of security issues that have nothing to do with defense, but everything to do with our ability to continue to function as a Nation have come to my attention as a result of Y2K. I have spoken with the Majority Leader about it, and he has encouraged me to use the Y2K Committee to examine these issues in the time the committee has left. We go out of business on February 29.

But these are very serious issues, and I was glad to see you raise them, Mr. Walker, and at some point in this hearing between the two of you, you might want to talk about that.

So those are the two issues that I want to focus on, the pent-up demand, its immediate impact on the appropriations process, and then the overall security issue. We will get into those questions, Senator Stevens, unless you have a question now.

Chairman STEVENS. If they want to comment, that is fine.

Mr. WALKER. Mr. Chairman, I will comment on that.

First off, on pent-up demand, my experience both in the public and private sectors has shown over the years that there is always a pent-up demand for wants in the area of information technology, but what I think is different because of Y2K is that there is increasing pent-up demand for needs.

You pointed to the fact that many, both public and private, entities have frozen changes in their LANs, in their software, in various other areas dealing with information technology to focus full attention on the Y2K challenge. They need to stabilize their environment in order to deal with their most immediate time-sensitive need—that is Y2K.

The fact of the matter is that there is a pent-up demand for needs for enhancements as well as the second issue that you raise, which is computer security. Computer security is already on our high risk list, just as Y2K is. Computer security is going to follow up closely on the heels of Y2K. It has national security, economic security, and personal privacy considerations.

We are focusing a lot of our time and attention on that, and believe that the Congress will need to do the same, as well as the executive branch, and I am sure that they intend to do so. I think these are two very real issues that not only are important from a wants, needs and affords perspective. What can we afford? And there are tradeoffs. Money is fungible, and so the question is, What are the consequences of these choices?

Mr. LEW. Mr. Chairman, I think there is no doubt there will be some pent-up demand, and that we have separate but very important concerns about computer security that are unrelated to Y2K. I think I would actually take a slightly different tack, I think our experience with Y2K in some ways leaves us more ready to deal with both of these issues than we otherwise would be.

In the area of pent-up demand, there are many agencies that have much more modern computer systems now than they would have had if we had not been dealing with Y2K because, given the tightness of appropriated resources they would not have replaced their personal computers (PC's), they would not have done the work that they have done over the last couple of years.

That does not mean that it is all of what they need for the next stage of agency operations, but I think we are left with an architecture that is generally better, not just Y2K-compatible. We need, as

we calculate the pent-up demand, to really look at what the net pent-up demand is, not of the investments we have made.

The concerns I have looked at are more the programmatic than the hardware issues, where agencies have deferred activities. You look at HCFA. In order to comply with Y2K compliance requirements, they deferred some of their rulemaking activity.

There is going to be a pent-up demand which will mean that people have to work on those projects in the coming year that they should have done in the past year. I think that has potentially programmatic implications. I do not know yet whether it has funding implications. I think we have to get a little farther into it to determine that.

In the area of computer security, one of the things that the contingency planning process is serving to be very useful for is to take contingency planning generally more seriously. Many of the contingency plans for dealing with your potential year 2000 disruptions are no different, as you mentioned, than the kinds of disruptions that could occur from natural or hostile acts.

The Y2K problem is more complex, because the potential of things happening in a lot of places is greater, whereas when there is a natural disaster it is very local. Presumably the same would be true if there are hostile acts, though you raise the good question of what the risks are, and are the risks growing.

I think we are more prepared to deal with contingency planning now than we were before Y2K remediation was undertaken. We had underway, as you know, through the National Security Council (NSC) process planning for contingencies in this area. I think we need to continue to work together after January 1, 2000 on that problem.

I do not at the moment expect a spike in funding requirements for either pent-up demand or the security issues, but that does not mean there will not be ongoing funding requirements that we have to balance against other needs.

I think the core issue in both cases is, are the needs there greater than the needs in other areas, and do they warrant funding.

The thing about Y2K that was so unusual, and that did require the extraordinary funding mechanism that we had, was that all the expenses came at once, and we are marching against an inflexible deadline, where if we do not do it by January 1, 2000, it will not deal with the problem.

In these other areas, while there are serious problems, they are problems we can fit into the spectrum of all the other things that we do have to worry about, and I look forward to working with you on those issues.

Chairman BENNETT. Senator Stevens.

PROGRESS ON NONMISSION-CRITICAL SYSTEMS

Chairman STEVENS. Mr. Lew, because of where I am from, I worry about the nonmission-critical systems, and the definition of those, and I raised this last year. Do we have any idea of how many such systems there are that are nonmission-critical systems?

Mr. LEW. I do not have a number. I understand the question, and I will be happy to get back to you with a number. We are not ignoring nonmission-critical systems. The fact that we are setting a

more absolute deadline for dealing with mission-critical systems does not in any way mean that we are treating the noncritical remediation as something that could wait until later.

Chairman STEVENS. Did you ever get an estimate of what it would cost to deal with all Federal systems and Y2K implications?

Mr. LEW. I believe the cost that we have been referring to would be the $8.02 billion level.

Chairman STEVENS. That is mission-critical.

Mr. LEW. It is more than mission-critical. It is the total expenditure on Y2K. The total compliance is based on bringing all the mission-critical systems into compliance at a particular time.

If I could get back to you, Senator, what I would like to do is ask some questions about what do we expect in terms of lingering funding requirements after January 1 for the nonmission-critical systems. I think that may give me a better ability to answer your question, and I do not know off the top of my head the answer to that question.

Chairman STEVENS. The implication here is that, not counting the emergency funds, that agencies have used appropriated funds to pay for Y2K problems and deferred their normal programming. Is that your statement? You have indicated that.

Mr. LEW. I think it is a combination. I think some of the things that they have done with the money were exclusively Y2K-related. Other activities really have multiple purposes, and one of the reasons it has been difficult to give actual numbers is that the bookkeeping before 1997 was not very good in terms of how much money was Y2K-related and how much of it was just generally IT-related.

As Mr. Walker noted, even now we are dealing with agencies that are being much more clear in terms of their defining Y2K costs for the emergency funds than they are for their base funds. Some of the costs have to be disaggregated to see whether they are just Y2K. When you buy a new PC system, it obviously is Y2K-related, but it is also giving you infrastructure that the agency needed. They are all modernizing their computer systems as quickly as they can.

Chairman STEVENS. The indication here is that they deferred normal programming activities in order to make those adjustments. How extensive has that been?

Mr. LEW. I think what we have done is, we have built into our budget request in the last several years additional resources where we saw it as needed for Y2K, and we balanced it against the ongoing programmatic activities.

I think the areas where it would have created the clearest direct conflict were some of the funding that was directed to come out of the Y2K emergency reserve, and actually that went both directions. Some of that funding was really Y2K-related, and some of it was funding that we had in the base that we thought was only marginally Y2K-related, so a lot of these are gray areas.

I think that when we are dealing with caps, as you and I know painfully well, there are tough choices about how we can deal with all of the competing needs.

Chairman STEVENS. I am looking at it, as Senator Bennett mentioned, from two sides. One, it appears there are a lot of things

that have been deferred, normal program activities, because of the Y2K emergency, and on the other side of the coin is that there are increasing demands on the budgets of all agencies because of Y2K compliance activities.

Now, both of those add up to me to a need for more money, but it is sort of a feather pillow. I am not getting what I need.

Mr. LEW. I think there are really two different questions there. One is, did they get more money than they otherwise would have gotten to deal with Y2K within the base funding, and in our budget proposals we were allocating dollars to Y2K where we were not taking it necessarily from something else. We were making our decisions from the ground up. What did an agency need to do for its entire mission that had to do with Y2K? We came to the conclusion that we could not do it within totals, which is why we put the emergency fund proposal in our budget last year. It got beyond the point of our ability to work within the limits and still meet agency needs and Y2K needs.

ARE ADDITIONAL Y2K SUPPLEMENTAL FUNDS REQUIRED?

Chairman STEVENS. That is what we anticipated, and that is why we started the emergency presence. But what I am looking at is whether or not, one, are we going to get a supplemental request to make up for the moneys that agencies have spent, the Y2K activities, in order that they may have the funds to carry out their normal programming; and two, are we going to get a supplemental request for Y2K activities? This $8.7 billion is much higher than we anticipated 1 year ago, or 2 years ago. Are there two supplementals out there staring us in the face?

Mr. LEW. We have no immediate plans for any additional supplementals. Our calculation is $8.02 billion total, and does assume that we use the emergency funds, but it does not assume that we have any additional funding requirements in fiscal year 1999. The agencies have been using the emergency funds not just to deal with mission-critical systems. They have been using the emergency funds to deal with noncritical as well as critical.

I actually have never seen a breakout of how much of the money has gone to mission-critical versus nonmission-critical, and it is a good question. I actually will go back and ask to see it broken out that way.

I tried to use the example of HCFA as the kind of activity where we know that there was a deferral of some work. I do not think that that necessarily means we will need a supplemental appropriation for HCFA. It means there was a delay in putting some regulations into effect. As HCFA works through its 2000 and 2001 work plans, they will integrate completing the work that they deferred with the work that they have to do.

They may have increased needs overall. Agency needs change from year to year. But I do not foresee a spike of additional needs because of doing the deferred work that came about because of dealing with Y2K remediation.

It is a fair question. It is something we are keeping our eye on. I am not sure we can anticipate everything in advance, but I certainly at the moment do not see a huge number of deferred activities where we will need to come in for a supplemental request.

Chairman STEVENS. Do you have any comment on this, Mr. Walker?

Mr. WALKER. Mr. Chairman, first I would agree with Director Lew that what we ought to focus on is the net need. Second, as we say in our statement, we do believe that there is pent-up demand and pent-up need, as there is in the private sector. We believe it is important to try to survey that, and try to understand the nature and extent of that.

Chairman STEVENS. A need for non-Y2K funds, because of Y2K activities?

Mr. WALKER. A need for additional funds because there have been projects that have been delayed that may represent need rather than want. Director Lew mentioned one, where there are some types of activities to implement certain regulations. There also could be some computer security related system enhancement needs that could be essential and cost beneficial, however, they have been delayed.

I think there is a need to try to inventory that to understand the nature and extent, but then there is a management decision and a budget decision as to the merits of those various proposals, and how they will be handled; but we do think it is important to inventory it, because we do believe it exists.

Mr. LEW. The only thing I would add, Senator, is that these issues are not new issues, because we have been dealing with Y2K. We faced it at the Treasury Department in terms of putting a new computer system in place there, where completely apart from the year 2000 there was a need for a long-term capital program.

I am not sure, net of what we spent on Y2K, that it is as much a question of pent-up demand as it is fitting those IT requirements into the many demands that agencies have for resources. If there is a pent-up demand we certainly should, as the Comptroller General says, try to keep an eye on it and coordinate it in a managed way.

I just would not put up a red flag that there is a crisis looming. We may have additional requirements in these areas completely apart from Y2K. The question of cyber security is something we will have to keep dealing with. I do not think we should confuse the pent-up demand issue with what the absolute requirements are, and if so, it is just a timing question.

On the other hand, we should not panic. We are in better shape now in terms of contingency planning than we have ever been in the past, and I think as we continue to deal with these questions we will have a much better knowledge.

WHAT PROGRESS IS BEING MADE IN CONTINGENCY PLANNING?

Chairman STEVENS. I visited two major industries where they had been told that their systems were Y2K compliant and on a test found that they were not. Now, we are relying on this testing. It is sort of a self-testing process of each agency, but as I understand it, the cost of contingency planning is not permitted to be paid out of the emergency money, is that right?

Mr. LEW. Well, actually I would distinguish between contingency planning and funding of the contingency plans. We are helping agencies deal with funding requirements for the contingency plan-

ning. We are just beginning to see them, so I do not have a wealth of material to draw on yet.

As we see the plans, I think we can expect that the plans will identify two kinds of risks. One is risks that their own systems will fail and there may in fact be additional funding requirements there. As you know we continue to have $496 million in the non-defense and $165 million in the defense reserve, some of which may well be used for the agency contingency plans.

Chairman STEVENS. You use that for planning, or plans?

Mr. LEW. There may well be funding needed for plans. If they need to back up their own systems internally there is a whole separate kind of contingency planning where I do not know that we have the authority to fund it. We may need to talk further about this if they identify problems that are not their own, but problems that are connected to the environments they are in, such as telephone and electric grids.

Obviously, we do not have the resources to do contingency plans for every agency so, if there is a localized power failure for a brief period of time we will bring the whole grid back up. Utilities are dealing with that, and they are dealing with it quite well.

I think the question we have to answer is if there is a localized problem, does each agency have a credible plan so that it can continue its operations while the local utility is dealing with the outside problem.

We may decide that we want to take on as a Federal obligation, and I do not think I would recommend it, dealing well beyond the ambit of Federal responsibility. Clearly we do not have the resources for that, but that is also not a Federal responsibility. What we are trying to do is make sure that it is coordinated, that information is readily available, and to provide the leadership so that each of the different parts of the environment that Federal agencies find themselves in is also making the kind of progress they need to make.

We do not anticipate the kind of massive electric or telephone failures that people worried about years ago, but that does not mean there will not be isolated incidents. The purpose of contingency planning is to be able to respond, so we have continuity in all Federal operations.

Chairman STEVENS. Do we have any idea what the cost of those plans will be?

Mr. LEW. The June 15 deadline just passed. We have received some, not all. I would not even say most of them yet. Over the next several weeks we will review them and we will continue to work with the committees as we get a better understanding of what the contingency plans call for.

I think the agencies are struggling a little bit in terms of putting the price tag themselves on what are in some cases fairly imponderable costs. I think as they narrow down to the cost for their own backup plans, that is an area that is much more concrete. We will start to see what the numbers are fairly quickly on those. I do not anticipate that those will be enormous, but if they do turn out larger than we expect, we will come back as soon as we know more.

Chairman STEVENS. Mr. Walker.

Mr. WALKER. Mr. Chairman, we tried to note on page 13 of the full statement how much of the emergency supplemental to date has been spent for contingency planning. It is over $300 million, primarily the Defense Department, but also about $77 million for the civilian agencies.

As Director Lew noted, there is a need to try to get your arms around what type of plans are necessary on a contingent basis, and it is a separate and distinct matter as to what cost might be necessary if those plans have to be implemented, and that is something that is important to focus on.

Chairman STEVENS. Do the contingency plans themselves have to be tested, in your judgment?

Mr. WALKER. We do believe they need to be reviewed. We plan to review them. OMB needs to review them first. I believe they are due later this month. Joel, do you have a comment?

Mr. WILLEMSSEN. Yes. OMB has noted that they are following our guidance on contingency planning. One of the key phases in doing that is validation and testing of those plans. We have recommended that the validation and testing be completed no later than September 30 of this year.

Chairman STEVENS. Do you have the sense that we have enough funds available now to deal with this total Y2K problem on the Federal level without any additional money, Mr. Walker?

Mr. WALKER. Mr. Chairman, the real key is that, for fiscal year 2000, there are certain unknowns. As Director Lew said, we have still got 10 Federal agencies that have not completed their own remediation testing efforts.

Second, 10 of the 43 critical Federal programs have significant State involvement. Many of those States are not going to be completed with the Y2K efforts until the fourth quarter of this calendar year.

In addition, there are other factors that frankly, until we get more clarity on those, it is difficult, if not impossible, to predict the funds that will be necessary. The real key is, what are the tradeoffs?

If additional funds are needed for Y2K, there are several ways to handle that. Obviously, one way is through a supplemental. Another way is through changing priorities within the existing baseline, and the key is to try to understand what the possibilities are, what the magnitude might be, and to be able to make informed choices about what those tradeoffs should be.

WHAT IS THE DIFFERENCE BETWEEN MISSION-CRITICAL AND NONMISSION-CRITICAL?

Chairman STEVENS. Both of you were talking about internal reprogramming. There could be a massive amount if there are any contingencies that develop between now and the end of the year, and we are dealing with two different fiscal years as far as the restraints on spending. I do hope that we are monitoring the marshaling of this money towards achieving objectives within the laws available. Maybe we need some additional flexibility on this, and if you do, we might have to give it to you in one of these bills. I would hope that you would both look at that.

But one of the critical problems here to me is the definition of what is critical. I am afraid the people sitting here in Washington have an idea of what is critical, and people out in the rural areas, and the western States in particular, have an entirely different attitude about what is critical. Has anyone reviewed the definition of what is critical in your agency?

Mr. WALKER. Mr. Chairman, let me comment on a couple of things, and I would ask Joel to add. First, the dollars that have been spent so far have been spent on Y2K, both mission-critical and nonmission-critical systems. Second, at this point in time we believe the important thing to focus on is the programs.

Candidly, the taxpayers, our citizens care about the results, they do not care about the process, and so the key is to assure, either through the remediation efforts or through the contingency planning that the programs will operate as intended at the taxpayer and the citizen level.

And Joel, I would ask you to add.

Mr. WILLEMSSEN. Mr. Walker hit it right on the nail. We have applauded what OMB has done in terms of moving its focus away from systems and into programs. I think there is still room for debate as to whether they have targeted the right programs. As Mr. Walker mentioned in his statement, there are some outliers that are not within the definition of the 43 programs that I think would raise some issues, but I believe now OMB has the correct focus, especially on testing end-to-end multiple systems. I think that is the appropriate emphasis that now needs to be placed.

Mr. LEW. That is actually the point I was going to make. The value of testing is that we will have a much better understanding if there is going to be a problem in rural areas, or in isolated areas. That is one of the reasons the funding has been going out in the pattern it has. As we have discovered problems, we have been using funds to deal with the problems.

We have been very careful, and frankly I think you deserve a lot of credit for designing a flexible-enough authority so that we have had the authority to fund basically everything we have needed to fund while still reserving resources for the final period.

The imponderable about the contingency planning is different from whether we are taking the kinds of effective steps to deal with the programmatic needs that agencies have, and I think it would be a mistake to think that there is a looming, huge problem in terms of basic agency operations that are unfunded.

If we discover that the contingency plans have funding requirements that are greater than what we think they will be, I assure you it is not something we would just keep to ourselves. Just as we shared with you the need for the $3¼ billion emergency fund, we would come back. I just at this moment do not anticipate it, and frankly it gets into an area fairly quickly that is not the Federal Government's primary responsibility. We have been using the money that was appropriated to deal with the testing to make sure that we discover, within the Federal systems, what else we need to do.

WHO WILL AGENCIES TURN TO IF THEY HAVE Y2K PROBLEMS?

Chairman STEVENS. Do we have any reserve capacity for the Government as a whole? Is there an agency that has been designated to come forward and assist any Federal program that runs into a glitch in the last part of the year?

As the next fiscal year started sometime after October 1, you run into problems. Who do these agencies turn to for assistance if some real difficult problem emerges that has not been contemplated?

Mr. LEW. As you know, John Koskinan has been coordinating overall the administration's planning and implementation of the Y2K effort. That has been, I think, a very effective process where we have had agency heads take on the responsibility personally to make sure that they were doing what needed to be done, and coming in with the kind of technical support.

We do not have a formal process where there is one agency that is doing things for the other agencies, but there has been a lot of sharing of information and cooperation amongst agencies in the way that you would want to see in a situation like this. As one agency learns something we do not wait for each of the others to discover it on their own, there is a sharing of information.

Chairman STEVENS. I am looking for something different. We have the Federal Emergency Management Agency (FEMA) if there is a natural disaster. What agency has the role of FEMA in dealing with Y2K, if something really goes bad in December?

Mr. LEW. Let me distinguish the work up until January 1 and deal a little bit separately with what happens in the immediate period at the new year.

The President made it very clear that it was the obligation of each agency head to assure that his or her agency was taking the action needed. Frankly, if there was a more centralized responsibility we would not be able to sit here today and report the kind of progress that we have made.

Chairman STEVENS. I am not interested in that. I am interested in emergency assistance at a time when it may be needed.

Mr. LEW. In terms of emergency assistance, we have planned for what we call an Information Coordination Center which we have worked with the committees on to bring together information at the end of the year. At the beginning of the new year, as we learn of disruptions, as we learn of problems, so that there will be a clear flow of information and an ability to muster appropriate responses.

I think that is more of an information exercise than it is a command and control exercise. It is not that we have a special weapons and tactics (SWAT) team that will go in, but it is a way to marshall the resources of the Federal Government to deal with situations as they occur. It is not the case, as in a natural disaster, where we designate FEMA or one agency to be the lead agency, because frankly, the problems are not necessarily going to be within the expertise of one agency.

If you have a transportation issue, the Department of Transportation is going to deal with it. If you have a communication issue, it is largely going to be private, and more information at the Federal level rather than action at the Federal level.

But there is going to be information coming in. Frankly, January 1 will come in many hours earlier in other parts of the world. We will gather information from what happens in other parts of the world and be able to perhaps take some preventative steps as we learn what happens in other places and be able to have the preparedness in real time.

I do not think that it would be as effective, frankly, if we had a single designated agency that would deal with all problems that might arise, because it would be more than any one agency could handle within its expertise.

Mr. WALKER. Mr. Chairman, four points that might be helpful. Obviously, John Koskinan has been handling overall interagency coordination and strategic planning. Second, it is my understanding that for each of the high-impact programs OMB has designated, in working with John Koskinan, a lead agency has responsibility for that program, even though there may be numerous agencies that have to be involved.

Third, based upon our experience so far, if there is one agency that probably has shined in this, it has been the Social Security Administration, but obviously no one agency, as Director Lew noted, could really handle contingency planning for everything.

IS THE POSTAL SERVICE Y2K COMPLIANT?

And last, but certainly not least, the Postal Service is critical. They are making progress, but they represent the contingency plan, or have an integral part in the contingency plans of not only the Federal Government but, quite frankly, the private sector, and that is one I think we have to keep our eye on the ball.

Chairman STEVENS. Who is monitoring that?

Mr. WALKER. I am sure that OMB and we at GAO are monitoring their progress.

Chairman BENNETT. Can you tell us where they are?

Mr. WILLEMSSEN. The Postal Service after a fairly slow start has made very rapid progress, and we have recently testified that the kind of management controls that they have put in place should give them greater assurance of being ready in time. There are still some risks, such as a number of systems that they have to get ready in a relatively short period of time, but the attention is now being placed on that, and frankly that was not the case some time ago.

I think one of the things that spurred the Postal Service on was when OMB last year put their additional reporting requirement on other entities beyond the 24 major Federal departments and agencies. That led to the Postal Service coming in with their first report, and that first report raised a lot more questions than it did answers. That led to enhanced oversight which contributed to the Postal Service being on the road they need to be on.

NEED FOR PROGRESS FOR FEDERAL SYSTEMS THAT INTERACT WITH STATE AND LOCAL SYSTEMS

Chairman STEVENS. What about the Federal systems programs that interface with the State and local activities such as food stamps, Medicare, and others that are dependent on State actions and State implementation?

Mr. WILLEMSSEN. I think there remains much room for concern there, and OMB is very aware of those concerns. States are working quite diligently with the Federal agencies, but many of those States do not plan to be compliant until the end of the year.

What we have seen as a model agency in terms of oversight of State systems has been the Health Care Financing Administration and Medicaid. When we came out with a report last fall that indicated that only about 16 percent of those systems were compliant, the Administrator of HCFA took the lead and obtained needed contractor help.

They've gone out and done risk assessments and visits of all States. They completed that first round in April and made detailed risk assessments. They are now in the midst of doing a second round of visits and, concurrent with that, they have outside help focusing on contingency planning for those States.

It is really a very good model, one that could be emulated by some of the other Federal agencies in working with their State partners. Although it is getting fairly late in the game, we think with the time remaining, activities like that could be very beneficial.

PROGRESS WITH OUR INTERNATIONAL PARTNERS

Chairman STEVENS. I have taken a lot of time. One last question, and this is a North American economy now, not a United States economy. What about Canada and Mexico, and the tremendous interface of our private economy with our neighbors to the north and south?

Mr. LEW. Senator, we have participated actively in international forums to help other countries learn from our experience as we discovered what needed to be done. In fact, the largest conference ever in terms of U.N. focusing on a single topic is being held either this week or next week in New York. I do not know for a fact, but I assume Mexico, Canada, and most of the countries of the Western Hemisphere are participating.

The challenge we have is, we clearly cannot take on as a U.S. obligation direct responsibility for the systems in other countries, but we have been trying very hard to share information and help others learn to take responsibility and take the actions necessary.

I do not have country-by-country reports. We would be happy to get back to you if you have specific questions about Mexico and Canada. I suspect the bigger concerns we have are in other parts of the world, though.

Chairman STEVENS. Well, that is a prime time for illegal immigrants to cross the border from California all the way over to Louisiana.

Mr. LEW. That is obviously a question of our critical systems working, and that is our responsibility.

If I could just respond on the question of the States, because I think it is one of the significant issues we have to continue to focus on from now until the end of the year. It is more difficult in the sense that it is not something we can just go out and fix. We have to work with others to fix their systems.

But we can encourage and require that there be backup arrangements, and that there be testing. We have been providing that

leadership. Putting into the quarterly report the State-by-State data we inputed was a very useful step in terms of getting each of the agencies to work with the States on their systems and, frankly, to put the public attention on which States are scheduled to be completed and which States are falling behind. I know that up here there is a lot of concern not just for the aggregate number, but on each individual State, and I would commend to your attention the State-by-State data in the ninth quarterly report.

We are going to be doing that on a regular basis from now through the end of the year. We have directed the agencies to work closely with the States to try and be helpful to them as they plan their own activities, but this is one of the remaining challenges that is going to require a lot of our attention.

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

NEED FOR ADDITIONAL Y2K FUNDING

Chairman BENNETT. Thank you. This is just a little bit of institutional jealousy, and I probably should not say it, but I will anyway. Mr. Lew, you made the comment, in your words, ''we shared with you the need for the $3¼ billion emergency.'' Just for the record, the initiative for the $3¼ billion emergency came from Senator Stevens. I was in the room when he came up with that number and announced it.

I remember the phone call I received from John Koskinan where he said, ''Senator, we had no idea you were going to do that. We had no tip-off at OMB in advance that this Congress was going to do that.'' I thought he was going to complain that the Congress was doing things, and then he said, and we think it's a really, really, really good idea. So I think just for the record Senator Stevens should receive the credit for having come up with that.

Let me talk about that supplemental. After the allocations against the funds, there is $165 million in reserve, as you said, for defense, and $400 million for nondefense. Mr. Walker, you say in your testimony that the cost of end-to-end testing and contingency plans will be high.

Do you share my concern that these reserve funds may not be enough? That too much of the money that was allocated in the emergency, $3.25 billion in emergency money, has already been spent, given the size of what we are still looking at, or do you think the expenditures and allocations up until now have been about right, and that these reserves are adequate? Either one of you.

Mr. WALKER. Mr. Chairman, I think there are two issues. One issue is whether or not the remaining funds that exist in the reserve will adequately cover all the additional Y2K costs versus whether or not there is a need for an additional supplemental, for example. I think there is a much higher risk that there will be more money necessary in order to address all the Y2K issues, given the contingencies that we have articulated today.

I think it is a separate and important, yet somewhat distinct, question as to how best to do that. Will it be through tradeoffs in other funding that already exists in fiscal year 2000 for these programs, or will there be a need for supplemental funding, and I would ask Director Lew to comment.

Chairman BENNETT. Do you share that view? I have the feeling you have a slightly different view.

Mr. LEW. The reason I am hesitant is that we are just beginning to review the contingency plans for the agencies. The real answer to the question will come after we have reviewed their plans.

Frankly, the early plans we are getting do not have cost estimates in them in many cases, so we have to go back and work with the agencies. To the extent that contingency planning costs are much larger than we have anticipated I would have a very different response. If the contingency plans fit within what we have expected, and I will not know that for several weeks, to the extent that they identify expenses that are not within the authority of the emergency fund, we would clearly need to come back and seek additional flexibilities.

I did not mean to detract at all from the contributions of Senator Stevens in particular. We very much appreciate it. We put a place marker in our budget, as you know, and it became real when Senator Stevens offered the amendment that he did and the flexibility the fund provides is very helpful.

Chairman BENNETT. Just a little executive branch-legislative branch——

Mr. LEW. I appreciate that. The answer to your question ultimately I think would be something I would want to get back to you after we have reviewed the continuity and contingency plans, because I think that is where the wild card would be.

At the moment, I cannot sit here today saying we anticipate tremendous additional needs, though I think Mr. Walker is right that to the extent that there are ongoing requirements. Either at the very end of this year or at the beginning of next year, there may be some tension within the existing budgets. That is not always a bad thing. I mean, agencies do deal with some costs that are outside of their normal business without it causing tremendous disruption.

What happened in Y2K was the amounts required so far exceeded the ability to manage the totals, so it was necessary to have the emergency fund.

Chairman BENNETT. Senator Stevens has an additional question, but before he gets to that, let me just pick up on what you are saying about the contingency plans. Your deadline was June 15. By your testimony most of the agencies missed that deadline, and that concerns us.

We do not have, as everybody knows, any fudge factor on the ultimate date that is hitting us here, and just quickly, do you have any sense when you will have all of the contingency plans with estimates in front of you? Can you give us a new date that we can hold people accountable for?

Mr. LEW. I cannot give you a firm date and, frankly, I think what is going to be happening is, we are going to be working with the agencies to refine what we get on an ongoing basis. There will not be a date when they are finished. They are going to keep proceeding with their planning and their work right until the end. I think in the next several weeks we will have a lot more than we have now. We have been working with the committees' staff and

with you directly on each of the allocations, and we will continue to do so as we review the contingency plans.

We have tried to be responsive to any of the issues raised in the course of those consultations and would continue to do so. If we discover a problem, or you discover a problem, we would like to keep the conversation going.

I wish I could say that I will have all the plans on June 30. When we set deadlines we try to be realistic about agency compliance patterns, and I think we are still in decent shape. If the President had not set March 31 as a deadline, we would not be sitting here today with the results that we have, and I dare say the same is true about the June 15 deadline.

I would wish that at all times agencies would respond with great punctuality, but we did build in a little bit of room.

Chairman BENNETT. If my friend Senator Dodd were here, I know he would have a few words to you to say about the importance of meeting deadlines and how carefully he will monitor those deadlines. Since he got married over the weekend he may have other things on his mind, but I assure you that he and the committee will be watching these dates very carefully.

Senator Stevens.

POTENTIAL NEED FOR ANOTHER FLEXIBLE FUND TO RESPOND TO Y2K PROBLEMS

Chairman STEVENS. Well, I want to make sure about this authority problem that you have indicated a couple of times, Mr. Lew. I have the same feeling. There is no basic authority like the President, as Commander in Chief, possesses for taking care of troops. You know, the food and forage concept.

I would like to contemplate, or like to have resolved how to establish an emergency authority in one single area. I take it would be the President's decision that would get that, but I also assume it would be OMB. I think we have to have that. I think we have to have someone with the authority to make the decision to use funds from wherever they have to be taken if there is an emergency that develops. We will be out of session. It is the holiday period where these crises could take place.

We also have critical non-Federal actions that may need correction, or might need assistance because they impact our mission-critical systems at a time in an unexpected way. I do not think you have the authority today to use funding for that purpose, but I do think you should have it. I also think that whatever we do along that line we should require a report from you to Congress, so that when we come back into session we can review what has happened and see whether adjustments are necessary to other accounts because of that.

But I would urge you to think about that, and Mr. Walker, you might review that also. I think in one of these bills that is coming along we ought to start a basic designation of who has that authority, how it is to be exercised, and what the scope of it is. If it goes outside the mission-critical Federal systems to the area where non-Federal actions might have an impact on the plans or contingency plans that we may have to put into effect.

Clearly, I think that the public is going to expect that we have placed, somewhere in the administration, the authority to take action, and I still believe it is sort of like any other time of weakness.

Are you a fisherman? I remember when I was fishing down off of Pulaski Light, and I learned how to fish for the giant barracuda. You really fish for the mackerel, but just as the mackerel hits the bait, that is when the barracuda likes to hit the mackerel. I am thinking there are a lot of barracudas out there that would like to have an impact on our Federal systems at a time of apparent weakness. We ought to guard against that, and we ought to have authority.

Again, I urge you to think about someone having a FEMA responsibility. There has to be a fireman there somewhere, and it is going to take some further analysis of this, as I am sure that Senator Bennett's committee will do.

We are here today primarily because of the implications of future funding that may be required. Even beyond that is the basic authority to use whatever funds are available should a substantial crisis develop.

Mr. LEW. Senator Stevens, I think it is an important distinction, because the truth is, if there is an emergency in an area where funds have been appropriated and authority exists, you could spend down money and could replenish the funds with a supplemental later on. I think the real critical issue in terms of being able to respond in a timely manner is whether the scope of authority is broad enough.

We have very substantial authorities to respond to most of the contingencies that are directly Federal. I think the issue here is whether it would be desirable to have a broader Federal responsibility for non-Federal response.

Chairman STEVENS. I am not talking about responsibility. I am talking about ability to act where there is a definite connection between the systems we rely on for our people through the Federal Government and those that are non-Federal, where the contingency planning or the planning may be defective, and we will not know that until it is too late.

Mr. LEW. Just to use an example, if there is a Federal agency where communications are critical, then the Federal responsibility is to have backup communication capacity so the Federal agency can communicate. It is not a Federal obligation to bring up the telephone system for the entire area. We have the authorities to our knowledge to do what we need for the Federal backups to be provided for.

The area where there is a question about authority is also, I think, where there is a question about whether it is a desirable Federal role. As we go through these contingency plans, if we discover additional needs for authority, I would welcome the invitation to pursue it with you. We clearly want to have whatever authorities we need to deal quickly and with agility to things that almost by definition are as unpredictable as the barracuda eating the mackerel.

Chairman STEVENS. The National Guard is in every State, and it is an entity in every State. I think somewhere along the line there has to be some entity like that where the standby capacity

to assist in areas that are life threatening, that relate to Federal activities, or are threatening to the economy in general—well, we will work with you on it.

Mr. Walker.

Mr. WALKER. Mr. Chairman, while obviously our first and foremost priority needs to be Federal programs and U.S. citizens, you touched on the international aspect. The fact of the matter is, we are in a global economy, and as I looked today at GAO's daily news clips, there is an article that comes to mind, the source of which is published through the Gartner Group, which is one of the leading information consulting firms. It has attempted—we have not attempted to verify this—to rank various countries into different levels, level 1 being the best prepared, of which I am pleased to say the United States and Canada are on that level; level 2 is where Mexico falls; but if I look at level 4, which is the lowest level, you have countries such as Russia and Pakistan, and clearly there are security issues associated with that which I think we have to keep in mind. While that is not our primary responsibility, it is not inconceivable that there could be some issues there.

Thank you, Mr. Chairman.

Chairman STEVENS. Thank you very much.

Chairman BENNETT. Thank you. We appreciate your being here and appreciate your patience with the questioning. If we have further questions we will submit them to you in writing, and as Senator Stevens said, Senator Byrd, who was not able to be with us, will have some questions for you in writing.

CONCLUSION OF HEARING

Chairman BENNETT. Thank you very much. The committee is recessed.

[Whereupon, at 11:10 a.m., Tuesday, June 22, the hearing was concluded, and the joint committees were recessed, to reconvene subject to the call of the Chair.]

○