For Release on Delivery
Expected at
9:30 a.m.
Tuesday,
June 22, 1999

YEAR 2000 COMPUTING CHALLENGE

Estimated Costs, Planned Uses of Emergency Funding, and Future Implications

Statement of David M. Walker
Comptroller General of the United States

GAO
Accountability ★ Integrity ★ Reliability

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 one billion dollars. 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.

---

[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).

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.

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

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

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

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

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 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

---

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

[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).

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.

[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 1: Emergency Supplemental Funds Allocated to Agencies (Dollars in Millions)
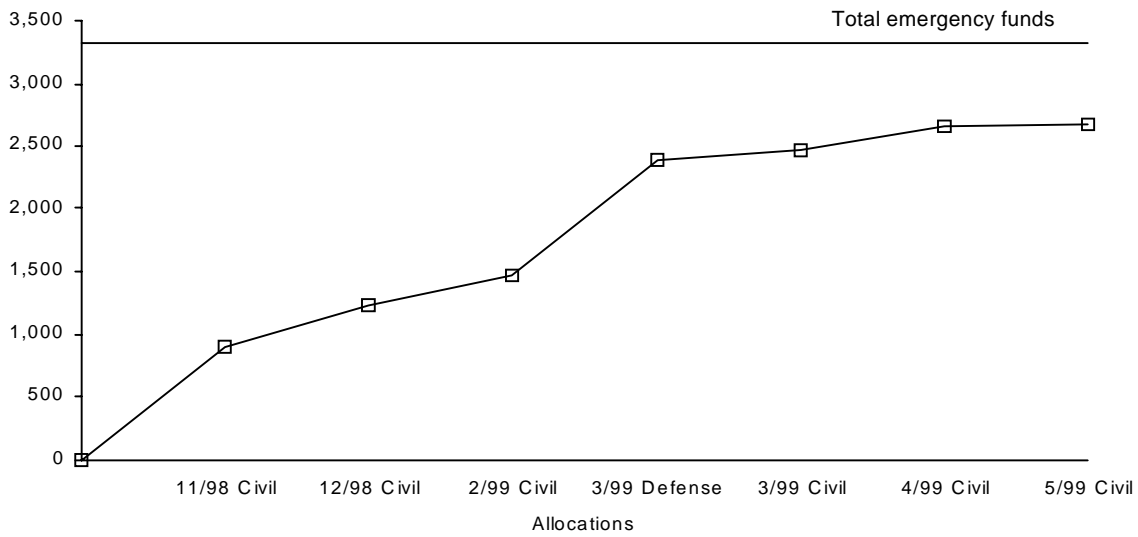
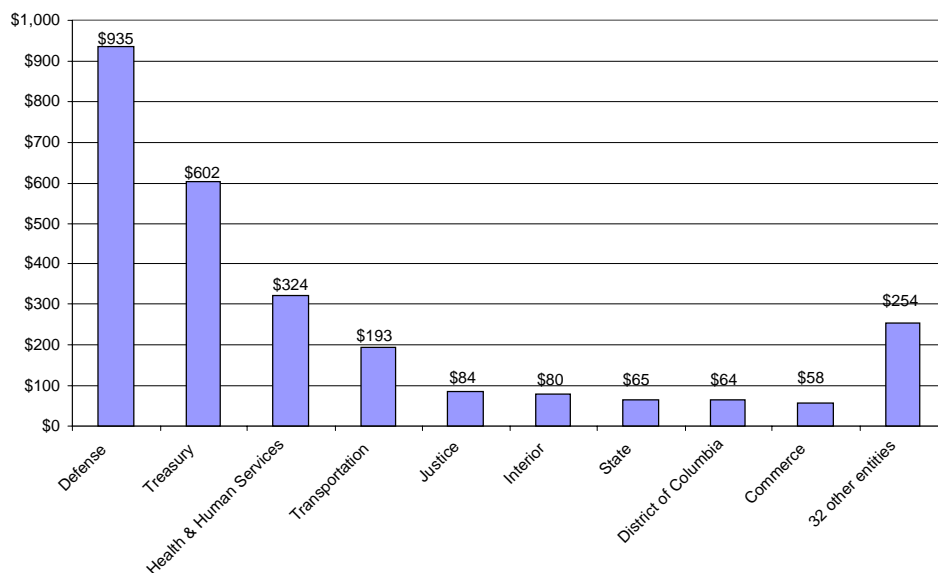Note: This chart does not include the amount set aside for the legislative and judicial branches ($29.9 million).

Source: OMB.

Figure 2 illustrates the entities that received the largest allocations.

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]

---

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

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.

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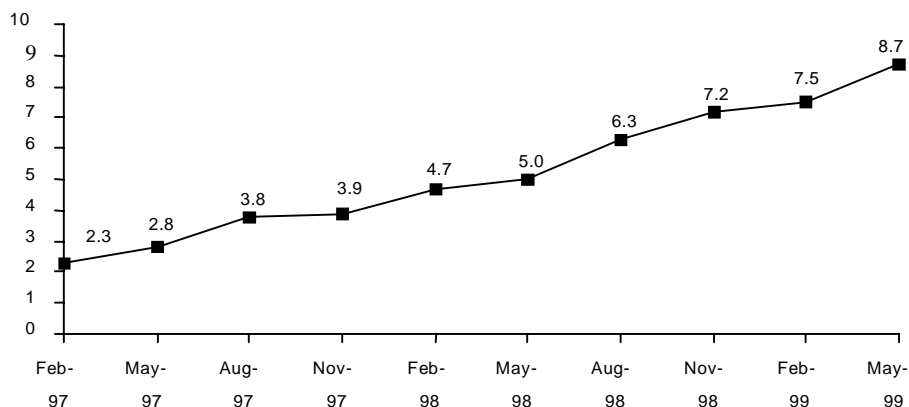
(Figure notes on next page)

---

[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.

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 (1125 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),

---

[12]One agency also reported Year 2000 costs that were prior to fiscal year 1996.

[13]GAO/AIMD-99-154, April 28, 1999.

- 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 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.

---

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

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

Category	Amount
Embedded systems	$36
Contingency planning	$77
Independent verification & validation	$98
Outreach	$137
Renovation, validation, implementation	$720
Other	$655
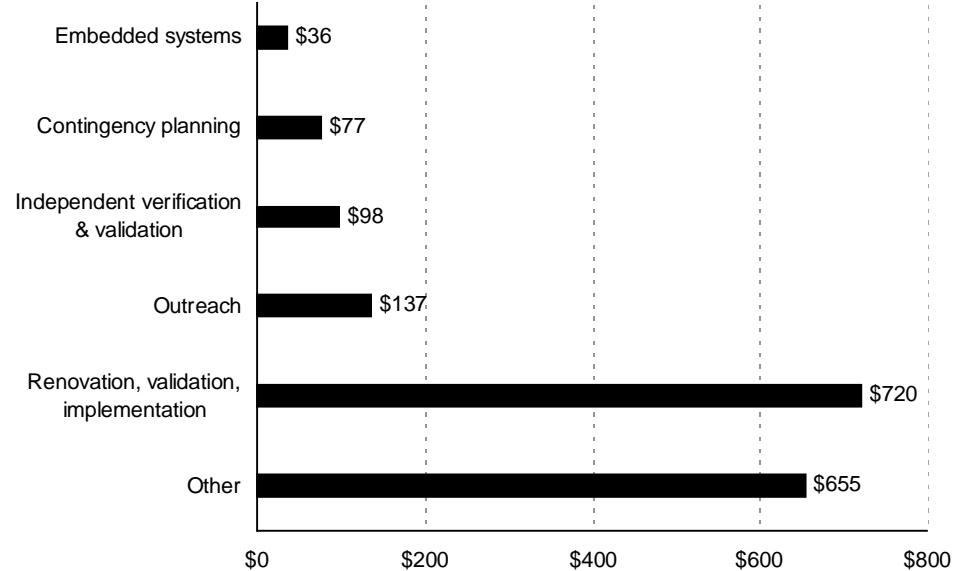
Note: The *other* category primarily includes funds for replacement of personal computers and network hardware and software. In their justifications, some organizations said the personal computers and network hardware and software could not be upgraded to be Y2K compliant, and in other cases they determined 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.

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,

---

[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.

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 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

---

[16]GAO/AIMD-10.1.19, August 1998.

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.
- 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

---

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

[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).

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

---

[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).

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 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

---

[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).

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

---

[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).

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 result, 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.

Organizations Receiving Emergency Allocations (as of May 1999)

Organization	Amount allocated (in thousands)
Department of theTreasury	$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[a]	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
Commodity Futures Trading Commission	356
Selective Service System	250
Federal Labor Relations Authority	243
African Development Foundation	137

Organization	Amount allocated (in thousands)
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**

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

Source: OMB.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov