

GAO

---

January 1999

# High-Risk Series

## An Update



---

---



**United States  
General Accounting Office  
Washington, D.C. 20548**

---

**Comptroller General  
of the United States**

January 1999

The President of the Senate  
The Speaker of the House of Representatives

Since 1990, GAO has periodically reported on government operations that we have identified as “high risk” because of their greater vulnerabilities to waste, fraud, abuse, and mismanagement. This effort, which was supported by the Senate Committee on Governmental Affairs and the House Committee on Government Reform, brought a much-needed focus on problems that are costing the government billions of dollars. To help, GAO has made hundreds of recommendations to improve these high-risk operations.

Overall, agencies are taking these problems seriously and making progress in trying to correct them. The Congress has acted to address individual high-risk areas through hearings and legislation. Moreover, these high-risk problems contributed to the Congress enacting a series of governmentwide reforms to strengthen financial management, improve information technology practices, and instill a more results-oriented government.

GAO’s high-risk status reports are now provided at the start of each new Congress. This update should help the 106th Congress in crafting its oversight and legislative agenda. While progress has been made in correcting high-risk problems, sustained attention by the Congress

---

in overseeing agency efforts is needed to make further headway in producing lasting solutions.

Over time, as high-risk operations have been corrected and other risks have emerged, we have removed areas from the list and added new ones to keep the Congress current on areas needing attention. The appendixes to this report show this chronology, provide our current high-risk list, and identify GAO staff who can provide additional information.

The determinations of which government operations are considered “high risk” in our 1999 update report were made using the same methodologies and criteria as prior reports. This was done in order to assure consistency in approach between update reports and minimize related “expectation gaps” on the part of the departments and agencies being reviewed. An increasing amount of information is becoming available as a result of implementation of various federal management reform initiatives, such as the Results Act and the Chief Financial Officers Act. This information makes it possible and appropriate to periodically reassess the methodologies and criteria used to determine which operations, functions, and entities are considered “high risk.”

GAO plans to undertake a comprehensive review and reassessment of this area, employing matrix management and other concepts, for use in our next update report scheduled for 2001. In conducting this review and reassessment, and consistent with our normal practices,

---

we will consult with key stakeholders, including congressional and agency representatives, before finalizing our approach. This effort will likely result in new ways of determining and presenting risk, especially in connection with selected functions (e.g., strategic planning, organizational alignment, human capital strategies, contract management) as well as at the overall department and agency level. At the same time, the ultimate determination of what is considered “high risk” will continue to involve the independent, professional, and objective judgment of GAO professionals.

Copies of this report are being sent to the President, the congressional leadership, all other Members of the Congress, and the heads of major departments and agencies.

A handwritten signature in black ink, appearing to read "D.M. Walker", with a long horizontal flourish extending to the right.

David M. Walker  
Comptroller General  
of the United States

---

# Contents

---

Executive Summary	6
Addressing Urgent Year 2000 Computing Challenge	33
Resolving Serious Information Security Weaknesses	55
Ensuring Major Technology Investments Improve Services	66
Providing Basic Financial Accountability	82
Reducing Inordinate Program Management Risks	115

---

**Contents**

---

<b>Managing Large Procurement Operations More Efficiently</b>	<b>146</b>
<b>Appendix I Chronology of High-Risk Designations</b>	<b>170</b>
<b>Appendix II Key Contacts for High-Risk Areas</b>	<b>173</b>

---

# Executive Summary

---

In our 1997 update for the 105th Congress, we reported that progress had been made in addressing the 20 high-risk areas being tracked at that time. We cautioned, however, that much more effort was needed to fully implement real solutions to these serious and long-standing problems. Also in 1997, we added five areas—the Year 2000 computing challenge and information security as governmentwide risks, the Supplemental Security Income program, defense infrastructure, and the 2000 Decennial Census.

Since 1997, agencies have focused on developing action plans and are trying to resolve weaknesses; the Congress has heightened its attention by reviewing agencies' progress and taking legislative action. Because of sustained, tangible improvement in one area—the U.S. Customs Service's financial management—we are removing its high-risk designation, making this the sixth area to come off the high-risk list since GAO began this effort in 1990.<sup>1</sup>

---

<sup>1</sup>Prior areas removed include (1) the Bank Insurance Fund, (2) the Pension Benefit Guaranty Corporation, (3) the Resolution Trust Corporation, (4) State Department Management of Overseas Real Property, and (5) Federal Transit Administration Grant Management (GAO/HR-95-1, February 1995).

In the remaining areas, more needs to be done to achieve real and sustained improvements. In many cases, agencies have agreed with GAO recommendations but have not yet fully implemented them. Also, many good plans have been conceived but the more difficult implementation task of successfully translating those plans into day-to-day management reality lies ahead. It will take time to fully resolve most high-risk areas because they are deep-rooted, difficult problems in very large programs and organizations.

Continued perseverance in addressing the 26 areas that are the current focus of our high-risk initiative will ultimately yield significant benefits. Collectively, these areas affect almost all of the government's annual \$1.7 trillion in revenue and span critical government programs and operations from certain benefit programs to large lending operations, major military and civilian agency contracting, and defense infrastructure. Lasting solutions to high-risk problems offer the potential to save billions of dollars, dramatically improve services to the American public, and strengthen confidence in the accountability and performance of our national government.

---

Addressing  
Urgent Year 2000  
Computing  
Challenge

Resolving the Year 2000 computing problem is the most pervasive, time-critical risk facing the federal government today due to its widespread dependence on large-scale, complex computer systems to deliver vital public services and carry out its massive operations. Unless adequate actions are taken, key federal operations—national defense, benefit payments, air traffic management, and more—could be seriously disrupted. Our purpose in designating this area high-risk in 1997 was to stimulate greater attention to assessing the government's exposure to Year 2000 risks and to strengthening planning for achieving Year 2000 compliance for mission-critical systems.

Over the past 2 years, the government has revamped and intensified its approach to this problem. Due to growing recognition of the challenges involved and encouragement from the Congress, in February 1998, the President established a Year 2000 Council and agencies have been much more aggressive in tackling the problem. Also, both the House and Senate have been relentless in assessing the state of readiness in government and the private sector through many hearings as well as passing emergency funding and legislation to

promote sharing of information on Year 2000 issues.

Preparedness has improved markedly, but significant challenges remain and time is running out. Critical testing activities need to be thoroughly completed and effective business continuity and contingency plans must be crafted and in place throughout government. To help agencies mitigate their Year 2000 risks, we produced a series of Year 2000 guides and issued over 70 reports detailing specific recommendations related to Year 2000 readiness of the government as a whole and of a wide range of individual agencies.

Moreover, the nation faces significant Year 2000 challenges which span all spectrums of our national economy as well as globally. Accordingly, the President's Year 2000 Council has been reaching out to the private sector, state and local governments, and other countries to increase awareness. Consistent with our recommendations, the Council has recently begun to assess the readiness of various sectors, including power, water, telecommunications, health care, and emergency services.

However, at this juncture, a comprehensive picture of the nation's readiness remains incomplete. A great deal more needs to be done—both domestically and internationally—to effectively determine readiness and prepare necessary contingency plans. Such actions are imperative to ensure that technology-dependent services and operations operate reliably after the turn of the century and that disruptions are minimized. (See page 33.)

---

**Resolving Serious  
Information  
Security  
Weaknesses**

Information security has become a concern in virtually every aspect of our lives as we move toward a society that is increasingly supported by computer technology and interconnected on a global scale. We designated information security as a governmentwide risk in 1997 because growing evidence indicated that controls over computerized operations were not effective and there was compelling information that risks were increasing. Since then, greatly increased recognition of the importance of information security has led to significant actions, including a Presidential directive requiring each major department and agency to develop a plan for protecting critical infrastructures. A series of

Senate hearings has also highlighted these risks and the need for greater action.

Continuing computer security weaknesses put critical federal operations and assets at great risk. Such problems are disturbing because they make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. In today's environment, these threats include a range of military enemies, criminals, and terrorists who have the capability to severely disrupt or damage the systems and infrastructures upon which our government depends. Accordingly, much more needs to be done to ensure that systems and data supporting essential federal operations are adequately protected.

To help further strengthen computer security practices, we issued a framework—based on best practices of leading organizations known for excellent security practices—for managing risks through an ongoing cycle of activities coordinated by a central focal point. While agencies have responded to numerous recommendations included in our reports and those of the Inspectors General,

agencies need to put in place comprehensive security programs based on best practices. Strong governmentwide leadership also is important to ensure that executives understand their risks, monitor agency performance, and resolve issues affecting multiple agencies. (See page 55.)

---

**Ensuring Major  
Technology  
Investments  
Improve Services**

Successfully applying modern technology is central to improving government operations and generating better service to the American people. Many efforts to achieve such goals have been plagued by huge cost overruns; schedule slippages measured in years; and marginal benefits in improving mission performance, cutting costs, and enhancing responsiveness. In 1995, we designated four troubled multibillion dollar modernizations as high risk; their ultimate success is key to the government's future ability to deliver critical services—safe and efficient air travel, modern tax processing and customer service operations, and improved weather forecasting—and the improvement of systems that support national defense operations.

- Over the past 17 years, the Federal Aviation Administration's (FAA) \$42 billion air traffic control modernization program has

experienced cost overruns, schedule delays, and performance shortfalls. Our work has pinpointed solutions to some of the root causes of these problems, and FAA has initiated efforts to resolve them. However, FAA's reforms are not yet complete and several major projects continue to face challenges that could affect their cost, schedule, and performance.

- The Internal Revenue Service (IRS) has spent over \$3 billion during the last decade attempting to modernize its outdated, paper-intensive approach to tax return processing. Our reviews over the past few years identified serious management and technical weaknesses with IRS' modernization, and we made recommendations to help IRS, among other things, build the capability necessary to successfully modernize its systems. IRS has agreed to implement our recommendations and is working to build its capability before it begins modernizing tax processing systems.
- In the 1980s, the National Weather Service (NWS) began a nationwide modernization program to upgrade weather observing systems to achieve more uniform weather services across the nation, improve forecasts, provide better prediction of severe weather and flooding, and achieve higher

productivity. Although NWS is nearing completion of its modernization, we are concerned about its ability to deliver on the final and most critical piece of the modernization—the Advanced Weather Interactive Processing System—which is to provide the workstations that integrate observing systems data and support forecaster decision-making. The Advanced Weather Interactive Processing System has been delayed and become more expensive because of design problems and management shortcomings. NWS reports that it is making considerable progress in developing and testing these workstations, but concerns about cost, schedule, and technical risks remain.

- The Department of Defense (DOD) has an \$18 billion investment to replace almost 2,000 inefficient, duplicative systems with more cost-effective systems. This effort—while necessary—is plagued with poor management controls and too little assurance that the investment will achieve the department’s technology objectives.

In summary, we have made comprehensive recommendations for each of these efforts that, if implemented, would fundamentally improve project management, introduce needed engineering rigor, and promote

disciplined decisions on project funding. These four agencies are making needed improvements, but most of our recommendations have not yet been fully implemented. Consequently, serious risks remain. (See page 66.)

---

**Providing Basic  
Financial  
Accountability**

The requirements of the Chief Financial Officers Act, as expanded by the Government Management Reform Act, are prompting steady improvements in financial accountability across government. However, progress is very uneven; several major departments are not yet able to produce auditable financial statements consistently. Also, our first ever audit of the U.S. government's financial statements framed the most serious challenges facing the government in accurately reporting a large portion of its assets, liabilities, and costs. Such deficiencies precluded us from being able to form an opinion on the reliability of the government's consolidated financial statements.

The President reacted strongly, requiring agency heads to submit plans to the Office of Management and Budget (OMB) to correct deficiencies. Financial management reform was designated a top management priority of

the executive branch, behind the Year 2000 computing problem. The House of Representatives also passed a resolution urging quick resolution of these problems. We are working with OMB, the Department of the Treasury, and agencies across government to provide recommendations for fixing the major deficiencies cited in our audit. A high-risk designation is intended to highlight individual departments and agencies that are material to the government's financial statements and have been unable to meet the most basic mandate to produce auditable financial statements for their own operations.<sup>2</sup>

The most significant in this regard is DOD, which represents a large percentage of the government's assets, liabilities, and net costs. None of the military services or the department as a whole has yet been able to produce auditable financial statements. We designated DOD financial management to be a high-risk area in 1995, and it remains so today, although we have noticed increased attention to rectify this situation. (See page 89.)

---

<sup>2</sup>Other departments and agencies also still need to improve their financial management operations. Challenges facing them in this area are discussed in our series of reports on major performance and accountability issues facing each agency. Major Management Challenges and Program Risks: A Governmentwide Perspective (GAO/OCG-99-1, January 1999).

Two other large organizations also have been unable to produce auditable statements for their entire operations—the Department of Agriculture (USDA) and the Department of Transportation (DOT). Unlike DOD, however, significant parts of these organizations have been able to produce auditable statements while other major components have not. Consequently, we are adding the most problematic parts of these departments to the high-risk list—financial management of the Forest Service at USDA and financial management of the Federal Aviation Administration at DOT. (See pages 94 and 98.)

Another major focus of the government's financial management entails its revenue collection operations. As a result, we have looked closely at IRS and the Customs Service. IRS has made progress recently and was able for the first time to obtain an unqualified opinion on its financial statements for fiscal year 1997—after five previous attempts did not yield auditable statements. This outcome was achieved, however, through material audit adjustments, and serious internal control weaknesses over refunds, receipts, and unpaid tax assessments remain. Until IRS can demonstrate a consistent ability to produce auditable statements, meet key new

accounting and reporting requirements, and make greater and sustained progress in addressing significant material weaknesses, we consider its revenue accounting to still be high risk, especially since it collected over \$1.7 trillion in revenue in fiscal year 1998—virtually all of the government’s revenue. (See pages 102 and 107.)

The Customs Service has made major strides since we began to focus on its financial management as a high-risk area. Customs has made several important improvements in its ability to assess and collect duties and excise taxes and has received unqualified opinions on its financial statements for the past 2 fiscal years. Therefore, we no longer consider Customs financial management high risk, although we will continue to monitor its progress. (See page 112.)

---

**Reducing  
Inordinate  
Program  
Management  
Risks**

We have identified several government programs that are not managed effectively or that experience chronic waste and inefficiency. These problems result in inordinate risks—the loss of billions of dollars annually due to improper payments in certain benefit programs, difficulty in controlling tax filing fraud, inefficient and weak lending programs, and challenges in

reducing defense infrastructure costs. Consequently, fixing the underlying weaknesses in high-risk program management areas can significantly reduce government costs and improve services.

For example, the Department of Health and Human Services' (HHS) Health Care Financing Administration (HCFA) had not developed its own process for estimating the national error rate for fee-for-service payments. For fiscal year 1997, the HHS Inspector General estimated that about 11 percent of all Medicare fee-for-service payments for claims, or about \$20 billion, did not comply with Medicare laws and regulations. In 1996, the Congress gave HHS new authority and began increasing resources to help prevent fraud, abuse, and mispayments. However, HCFA's deployment of these tools has lagged. In addition, HCFA has had to give priority to preparing its systems for the year 2000, which has halted the implementation of streamlined claims processing systems and new payment methodologies designed to curb excess spending. (See page 116.)

Also, the Supplemental Security Income (SSI) program continues to be hampered by long-standing problems such as program

abuses and mismanagement, increasing overpayments, and the Social Security Administration's (SSA) inability to recover outstanding SSI debt. During fiscal year 1998, current and former recipients owed SSA more than \$3.3 billion, including \$1.2 billion in newly detected overpayments for the year. SSA has initiatives planned to improve SSI's overall payment accuracy, increase continuing disability reviews, combat program fraud, and improve debt collection. SSA now needs to implement its plans in these areas and continually improve its payment controls and debt collection activities. (See page 119.)

Another high-risk area involves the filing of fraudulent refund claims by taxpayers and/or tax return preparers. Since 1995, IRS has taken several steps to reduce its exposure to filing fraud such as (1) better screening electronic tax submissions, (2) strengthening processes for checking the applications from tax preparers who apply to participate in the electronic filing program, (3) revising computer formulas to score tax returns for fraud potential, and (4) enhancing procedures to deal with paper returns involving missing or incorrect Social Security numbers. Also, the Congress passed legislation giving IRS new enforcement tools

and additional funding specifically designated for activities related to Earned Income Credit, which involves most of the fraudulent refund claims.

In April 1997, IRS released the results of its study of Earned Income Credit noncompliance on tax returns filed in 1995 (i.e., tax year 1994 returns), which showed that of the \$17.2 billion in such claims, about \$4.4 billion (25.8 percent) was estimated to be overclaims. How much of this \$4.4 billion involved fraud, as opposed to less serious noncompliance, is unknown. The returns included in IRS' study were filed before IRS was given increased authority to deal with missing or invalid Social Security numbers. Even after adjusting for the potential effect of that increased authority, however, IRS determined that the rate of Earned Income Credit noncompliance would still be over 20 percent. While IRS has begun implementing a 5-year Earned Income Credit compliance initiative, its effect on reducing the incidences of Earned Income Credit noncompliance is not yet known. (See page 121.)

DOD is seeking ways to address inefficiencies in its mission support operations through a variety of approaches, including

consolidations, competing support services sourcing, and public-private partnership arrangements. Faced with a limited budget, these inefficiencies, if not addressed, will consume money that could be made available to meet other defense priorities, such as force modernization and readiness needs. For example, significant cost savings can be achieved through infrastructure reductions, but doing so is difficult because it requires up-front investments, the closure of installations, and the elimination of military and civilian jobs. While DOD's infrastructure reduction initiatives are steps in the right direction, they do not provide a comprehensive plan that focuses on long-range strategies for facilities revitalization, replacement, and maintenance. Further, we have identified significant efficiencies that could be achieved by eliminating, streamlining, or reengineering infrastructure activities involving acquisition infrastructure, central logistics, installation support, central training, force management, and medical facilities and services. (See page 125.)

At the Department of Housing and Urban Development (HUD), four serious, long-standing departmentwide management deficiencies, taken together, place the

integrity and accountability of the department's programs at high risk. With close oversight by the Congress, HUD is making significant changes and has made credible progress since 1997 in laying the framework for improving its management. Given the severity of the management deficiencies that we and others (e.g., HUD's Inspector General, external auditors) have observed, it would not be realistic to expect that HUD would have substantially implemented its reform efforts and demonstrated success in resolving its management deficiencies in the 2 years since we issued our last report. To resolve its management deficiencies, HUD needs to ensure that the actions being taken eliminate the remaining major internal control weaknesses, improve information and financial systems, and strengthen staff resources and skills. (See page 128.)

Two other lending operations are at risk—student financial aid programs and farm loan programs. The Department of Education's student financial aid programs are inherently vulnerable to waste, fraud, abuse, and mismanagement, putting a premium on effective management. We have found, however, that the department's administration of these programs had

contributed to exposure to mismanagement and abuses. For example, audits have found instances in which students fraudulently obtained grants and loans, schools were inappropriately recertified to continue participating in federal student aid programs, and state-designated guaranty agencies misused federal funds in their custody. Also, in fiscal year 1997, the federal government paid over \$3.3 billion to make good its guarantee on defaulted student loans. The Congress and the department have acted to address a number of program management and oversight issues, but problems continue—especially with regard to the reliability of financial and other management information for overseeing student financial aid programs. (See page 133.)

The financial condition of USDA's farm loan portfolio has improved since we designated farm loan programs high-risk. The value of farm loans held by delinquent borrowers has been reduced from a reported \$4.6 billion, or 40.7 percent of USDA's total outstanding direct farm loan principal, in 1995 to a reported \$2.7 billion, or 28.2 percent, in 1997. However, USDA continues to carry a high level of delinquent debt and to write off large amounts of unpaid loans held by problem borrowers. Moreover, these delinquencies

may increase because of the droughts and low prices for major crops and livestock in 1998. USDA and the Congress need to continue to monitor the effects of recent lending and servicing reforms intended to improve the financial integrity of farm loan programs. (See page 136.)

In another program area—asset forfeiture programs—the federal government faces difficult problems managing a reported \$1.8 billion in property seized by the Departments of Justice and the Treasury. Many improvements have been made in this area since 1990, but Justice has reported that its asset forfeiture systems continue to be inadequate to keep track of these assets and the Treasury has reported weaknesses in the accountability and reporting over seized and forfeited property. In September 1998, the Justice Inspector General reported that at most of the Immigration and Naturalization Service Border Patrol stations his staff visited, they found problems with the management of seized drugs. Further, Justice and the Treasury continue to operate two similar but separate seized asset management and disposal programs, even though program consolidation could offer options for cost reductions and efficiency gains. (See page 139.)

Lastly, major challenges and uncertainties have led us to conclude that there is a high risk that the 2000 census will be less accurate and more costly than previous ones. The Congress and the administration have yet to agree on the final design of the census because of congressional concerns over the legal and methodological issues surrounding the planned use of sampling and statistical estimation. Also, federal courts have recently ruled that sampling is illegal for purposes of apportionment; the administration has appealed the rulings to the Supreme Court. Irrespective of how the controversy over the use of sampling and statistical estimation is resolved later this year, the Department of Commerce's Bureau of the Census will have little time remaining to make final census design changes and implement those changes in time for the census in 2000. In that regard, our work has shown that the bureau faces a number of formidable challenges to a cost-effective, accurate, and complete census no matter which design is chosen. The bureau can take actions to mitigate the risk of an unsuccessful census, such as ensuring that its evaluation of the dress rehearsal for the 2000 census is rigorously analyzed and used to refine operations, help set priorities, and allocate resources. (See page 142.)

---

**Managing Large  
Procurement  
Operations More  
Efficiently**

Our work has shown that some of the government's largest procurement operations are not always run efficiently. We have recommended ways to operate them better and thus, help to ensure that the government gets what it pays for under its contracts and that contractors' work is done at a reasonable cost. At DOD, our high-risk procurement management work focuses on three areas—inventory management, weapons systems acquisition, and contract management. At civilian agencies, our focus has been on the contract management practices at three agencies—the Department of Energy (DOE), the Environmental Protection Agency (EPA) for Superfund, and the National Aeronautics and Space Administration (NASA).

In 1990, we identified DOD's management of secondary inventories (spare and repair parts, clothing, medical supplies, and other items) as high risk because levels of inventory were too high and management systems and procedures were ineffective. While some improvements have been made, these general conditions still exist. Since 1991, we have identified significant opportunities for DOD to test and adopt, where feasible, best inventory management practices used in the private sector to

improve logistics operations and lower costs. Recent legislation calls for the implementation of best commercial practices in DOD's acquisition and distribution of inventory items, and in November 1997, DOD announced an initiative to reengineer support activities and business practices by incorporating many business practices that private sector companies have used. Unless DOD acts more aggressively to correct systemic problems, its inventory management problems will continue well into the next century. (See page 147.)

Further, DOD spends about \$85 billion annually to research, develop, and acquire weapon systems. Although DOD has many acquisition reform initiatives in process, pervasive problems persist regarding (1) questionable requirements and solutions that are not the most cost-effective available, (2) unrealistic cost, schedule, and performance estimates, (3) questionable program affordability, and (4) the use of high-risk acquisition strategies. Overall, acquisition reforms and commercial practices can produce better outcomes on DOD acquisitions when they help a program succeed in its environment. Thus, the way to get lasting reform is to realign the incentives of the weapon acquisition process with

desired program outcomes. Changing these incentives—that is, redefining program success—will take the efforts of the Congress as well as DOD and the military services. (See page 150.)

Also, DOD spends over \$100 billion a year contracting for goods and services. Over the last few years, several broad-based changes have been made to DOD contracting processes to improve the way DOD relates to its contractors and the rules governing their relationships. And the changes are by no means complete. DOD faces a number of areas where risks appear particularly acute, including the need for DOD to (1) achieve effective control over its payment process—or risk erroneously paying contractors millions of dollars and (2) strengthen the quality of its analyses for commercial purchases—or, for example, continue to pay higher prices for commercial spare parts than necessary. Acquisition reform, with its emphasis on widespread reengineering of fundamental processes, continues to receive attention at the highest levels in DOD. (See page 155.)

Turning to the government's largest civilian contracting agency, in fiscal year 1997, DOE obligated about \$16.2 billion, or about

91 percent of its obligations, to contracts. We have reported on weaknesses in DOE's contracting practices, including noncompetitive awards and lax oversight of costs and activities. Since we designated DOE's contracting as a high-risk area in 1990, DOE has put in place a framework for contract reform. For example, DOE has increased its use of competition in awarding contracts for managing and operating its facilities and has begun incorporating performance-based incentives in its management and operating contracts to better link a contractor's fees to the satisfactory accomplishment of specific tasks. While reforms such as these are generally steps in the right direction, DOE has had some problems in implementing them, and in some instances, their effectiveness will not be known for several years. (See page 158.)

Another civilian agency, EPA, has had long-standing challenges with controlling the costs of the contractors it uses to clean up sites or to monitor private party cleanups for EPA. Since 1990, when we designated Superfund contract management as high risk, EPA has increased its use of independent government cost estimates to set better contract prices for the government, but

some estimates are still of questionable quality. In addition, according to EPA officials, the agency has improved the timeliness of contractor audits and has almost eliminated the backlog of these audits. However, EPA continues to experience high program support costs related to contractors. These continuing concerns suggest that EPA may need to evaluate whether it needs to overhaul some of its contracting practices. (See page 163.)

Further, NASA, which now spends over \$12 billion annually for goods and services—mostly on contracts with businesses and other organizations—has progressed in correcting contract management weaknesses. For example, NASA is implementing a new system for measuring procurement performance and conducting evaluations of its field centers' procurement activities based on international quality standards. NASA continues to develop a new integrated financial management system—which offers the promise of providing reliable and timely information, such as the status of procurement requests and contracts—but agencywide implementation of the system has been delayed from July 1, 1999, to June 1, 2000. Until the financial management system is

---

**Executive Summary**

---

developed and operational, performance assessments relying on cost data may be incomplete. (See page 166.)

---

To ensure that progress continues in addressing high-risk problems, sustained management attention and congressional oversight are necessary. We will continue to closely monitor agencies' progress in resolving high-risk areas and advance additional recommendations for improvements.

---

# Addressing Urgent Year 2000 Computing Challenge

---

A critical and sweeping management task facing public and private organizations is successfully addressing the tremendous challenges imposed by the Year 2000 (Y2K) computing problem.<sup>1</sup> It represents an enormous undertaking for the federal government due to its widespread dependence on large scale, complex computer systems to deliver vital public services and carry out its massive operations. Unless adequately confronted, the Year 2000 computing problem could lead to serious disruptions in key federal operations ranging from national defense to benefit payments to air traffic management.

Consequently, in February 1997, we designated the Year 2000 computing problem as a high-risk area. Our purpose was to stimulate greater attention to assessing the government's exposure to Year 2000 risks and to strengthening planning for achieving Year 2000 compliance for mission-critical systems. Fortunately, the past 2 years have witnessed marked improvement in preparedness as the government has

---

<sup>1</sup>For the past several decades, computer systems have typically used two digits to represent the year, such as "98" for 1998, 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.

revamped and intensified its approach to this problem.

Significant challenges remain, however, and time is running out. In particular, complete and thorough Year 2000 testing is essential to provide reasonable assurance that new or modified systems process dates correctly and will not jeopardize an organization's ability to perform core business operations. Moreover, adequate business continuity and contingency plans throughout government must be successfully completed.

The scope of the Year 2000 problem extends well beyond federal operations—it spans all spectrums of our national economy as well as globally. Accordingly, the President's Year 2000 Council has been reaching out to the private sector, state and local governments, and other countries to increase awareness. Working with these entities, the Council has recently begun to assess the readiness of various sectors, including power, water, telecommunications, health care, and emergency services.

However, at this juncture, a comprehensive picture of the nation's readiness remains incomplete. A great deal more needs to be done—both domestically and

internationally—to effectively determine readiness and prepare necessary contingency plans. Such actions are imperative to ensure that technology-dependent services and operations continue to operate reliably after the turn of the century and that disruptions are minimized.

---

**Federal  
Government Has  
Enhanced Its  
Approach**

Since February 1997, action to address the Year 2000 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, and expanded its outlook beyond federal agencies. In February 1998, the President took a major step in establishing the President's Council on Year 2000 Conversion. He established a goal that no system critical to the federal government's mission experience disruption because of the Year 2000 problem and charged agency heads with ensuring that the Year 2000 problem receives the highest priority attention.

The President tasked the Chair of the Council with being chief spokesperson on Year 2000 issues in national and

international forums; overseeing Year 2000 activities of federal agencies; providing Year 2000 policy coordination of executive branch activities with state, local, and tribal governments; and promoting appropriate federal roles with respect to private-sector activities. Among the initiatives the Chair has implemented in carrying out these responsibilities are attending monthly meetings with senior managers of agencies that are not making sufficient progress; establishing numerous workgroups 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.

OMB, for its part, has tightened requirements on agency reporting of Year 2000 progress. It now requires that, beyond the original 24 major departments and agencies that are 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. OMB has clarified instructions on agencies preparing business continuity and contingency plans. Quarterly, OMB also places each of the 24 agencies into one of three tiers, determined by its

judgment of whether the agency has reported sufficient evidence of progress.

Several agencies have reported substantial progress in repairing or replacing systems to be Year 2000 compliant. In December 1998, for example, the President announced that all of SSA's mission-critical systems were compliant. In October 1997, we reported that SSA had made significant progress in assessing and renovating mission-critical mainframe software, although certain areas of risk remained.<sup>2</sup> Accordingly, we made several recommendations to address these risks, including the development of business continuity and contingency plans. SSA agreed and, in July 1998, we reported that actions to implement these recommendations had either been taken or were underway.<sup>3</sup>

Many congressional committees have played a central role in addressing the Year 2000 challenge by holding agencies accountable for demonstrating progress and by heightening public appreciation of the problem. The Senate formed a Special

---

<sup>2</sup>Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).

<sup>3</sup>Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner (GAO/AIMD-98-235R, July 10, 1998).

Committee on the Year 2000 Technology Problem, which held hearings on the readiness of key economic sectors, including power, health care, telecommunications, transportation, financial services, emergency services, and general business. The House called on the Subcommittee on Government Management, Information and Technology of the Committee on Government Reform; and the Subcommittee on Technology of the Committee on Science to co-chair the House's Year 2000 oversight. These committees and others have held many hearings to obtain information on the readiness of federal agencies, states, localities, and other important nonfederal entities, such as the securities industry.

The Congress also passed Year 2000 legislation. In October 1998 it passed—and the President signed—the Year 2000 Information and Readiness Disclosure Act. Its purposes include (1) promoting the free disclosure and exchange of information related to Year 2000 readiness and (2) lessening the burdens on interstate commerce by establishing certain uniform legal principles in connection with the disclosure and exchange of information related to Year 2000 readiness. In addition, the Congress passed (and the President

signed) the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, which included \$3.35 billion in contingent emergency funding for Year 2000 conversion activities.

---

**GAO's Efforts to  
Help Meet the  
Challenge**

To help agencies mitigate their Year 2000 risks, we produced a series of Year 2000 guides. The first of these, on enterprise readiness, provides a systematic, step-by-step approach for agency planning and management of its Year 2000 program.<sup>4</sup> The second guide, on business continuity and contingency planning, provides a structured approach to helping agencies ensure minimum levels of services through proper planning.<sup>5</sup> Our third guide, on testing, sets forth a disciplined approach to Year 2000 testing.<sup>6</sup> Federal agencies and other organizations have used these guides to help organize and manage their Year 2000 programs.

---

<sup>4</sup>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).

<sup>5</sup>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).

<sup>6</sup>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).

We also have issued over 70 reports detailing specific findings and made over 100 recommendations related to the Year 2000 readiness of the government as a whole and of a wide range of individual agencies.<sup>7</sup> These recommendations have been almost universally embraced.

Our recommendations have centered on the following:

- Project planning. We have recommended better organizational planning and management oversight—including systems inventorying and analysis—in a number of programs and entities.
- Priority-setting. With over 2,600 mission-critical systems still needing to be made Year 2000 compliant, it is important to establish priorities. Resources need to be focused on those business processes and supporting systems that could threaten national security, the economy, the health and safety of Americans, or their financial well-being.
- Data exchanges. To remediate their data exchanges, agencies must (1) identify data exchanges that are not Year 2000 compliant, (2) reach agreement with exchange partners

---

<sup>7</sup>See GAO's World Wide Web page at [www.gao.gov/y2kr.htm](http://www.gao.gov/y2kr.htm) for a list of reports and testimony on the Year 2000 problem.

(such as states) on the date format to be used, (3) determine if data bridges and filters are needed and, if so, reach agreement on their development,<sup>8</sup> (4) develop and test such bridges and filters, and (5) test and implement new exchange formats.

- Testing. Agencies should perform thorough testing of their systems, including end-to-end testing of multiple systems supporting a major business function.
- Business continuity and contingency planning. Given the interdependencies among agencies, their business partners, and the public infrastructure, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency.

---

**Serious Risks  
Remain**

While considerable effort has been put forth, the change to the new century will still present great challenges. Our reviews of federal Year 2000 programs have found uneven progress; some major agencies are significantly behind schedule and are at high risk that they will not correct all of their mission-critical systems in time. As

---

<sup>8</sup>A bridge is used to convert two-digit years to four-digit years or to convert four-digit years to two-digit years. A filter is used to screen and identify incoming noncompliant data to prevent it from corrupting data in the receiving system.

remaining time diminishes, it becomes increasingly difficult to ensure that all mission-critical systems will be compliant in time.

Figure 1 shows OMB's assessment of agencies' Y2K progress based on their November 1998 quarterly reports.

Figure 1: OMB's Assessment of Agencies' Y2K Progress (November 1998)

**Tier 1: Agencies Demonstrating Insufficient Evidence of Progress**

- *Defense*
- *Energy*
- *HHS*
- *State*
- *Transportation*
- *AID*

**Tier 2: Agencies Showing Evidence of Progress But About Which OMB Had Concerns**

- *Agriculture*
- *Commerce*
- *Education*
- *Justice*
- *Labor*
- *Treasury*
- *OPM*

**Tier 3: Agencies Making Satisfactory Progress**

- *HUD*
- *Interior*
- *VA*
- *EPA*
- *FEMA*
- *GSA*
- *NASA*
- *NSF*
- *NRC*
- *SBA*
- *SSA*

We have made detailed recommendations to agencies responsible for some of the government's most essential services. For example:

- DOD and the military services face the threat of significant problems.<sup>9</sup> In April 1998, we reported that the department lacked complete and reliable information on systems, interfaces, other equipment needing repair, and the cost of its correction efforts.<sup>10</sup> We found that these and other problems seriously threatened the department's chances of successfully meeting the Year 2000 deadline for its mission-critical systems. Further, taken together, the problems in Defense's Year 2000 program made failure of at least some mission-critical systems and the operation they support almost certain unless corrective actions were taken. We have recommended numerous improvements for critical matters such as data exchanges, testing, and contingency planning; DOD concurred with

---

<sup>9</sup>Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998), Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998), Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998), and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

<sup>10</sup>GAO/AIMD-98-72, April 30, 1998.

these recommendations and agreed to implement them.

- We previously reported<sup>11</sup> that the Health Care Financing Administration (HCFA) had made improvements in its Year 2000 management but HCFA and its contractors were severely behind schedule in repairing, testing, and implementing the mission-critical systems supporting Medicare. Given the magnitude of the tasks, and the risks and limited time remaining, we concluded in September 1998 that it was highly unlikely that all of the Medicare systems would be compliant in time to ensure the delivery of uninterrupted benefits and services. To improve prospects for minimizing disruptions, we recommended that HCFA (1) rank its remaining Year 2000 work on the basis of an integrated project schedule, (2) ensure that all critical tasks are prioritized and completed in time to prevent unnecessary delays, (3) define the scope of an end-to-end test of the claims process and develop plans and a schedule for conducting such a test, (4) develop a risk management process, and (5) accelerate the development of business continuity and contingency plans. HCFA has agreed to implement these recommendations.

---

<sup>11</sup>Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

- As we reported in August 1998,<sup>12</sup> FAA had made progress in managing its Year 2000 problem and had completed critical steps in defining which systems needed to be corrected and how to accomplish this. The agency had acted upon several of our recommendations from earlier in the year, including finalizing a Year 2000 strategy and setting priorities.<sup>13</sup> However, with less than 17 months to go, FAA still had to correct, test, and implement many of its mission-critical systems. Accordingly, FAA must determine how to ensure continuity of critical operations in the event that some systems fail.

Such examples underscore the difficulties confronting agencies to make up for time lost; Year 2000 testing alone is consuming between 50 and 70 percent of a project's time and resources. Thorough testing is essential to provide reasonable assurance that new or modified systems process dates correctly and will not jeopardize an organization's ability to perform core

---

<sup>12</sup>FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

<sup>13</sup>FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998) and Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998).

business functions after the change of century.

Even for agencies that are making progress, other critical issues must be successfully resolved; these include data exchanges, telecommunications, and embedded systems.<sup>14</sup> First, should the government's hundreds of thousands of data exchanges not be Year 2000 compliant, data either will not be successfully exchanged or invalid data could cause the receiving computer systems to malfunction or produce inaccurate computations. Second, the government depends heavily on the telecommunications infrastructure; reliable services are made possible by a complex web of highly interconnected networks supported by national and local carriers and service providers, equipment manufacturers and suppliers, and customers. Third, the year 2000 could cause problems for the many embedded computer systems used to control, monitor, or assist in operations.

---

<sup>14</sup>Embedded systems are special-purpose computers built into other devices. Examples include systems in elevators, heating and air conditioning units, and biomedical devices, such as cardiac defibrillators and cardiac monitoring systems, which can record, process, analyze, display, and/or transmit medical data. (See Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).)

If issues such as these are not adequately addressed, the impact of Year 2000 failures could disrupt vital government operations. Moreover, federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure (power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause a cascading effect of major shutdowns of business operations. Consequently, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Without such plans, when unpredicted failures occur, agencies will lack well-defined responses, and may not have enough time to develop and test alternatives.

---

**The Nation As a  
Whole Faces  
Significant Year  
2000 Challenges**

Our nation's reliance on the complex array of public and private enterprises having scores of system interdependencies at all levels, accentuates the potential repercussions a single failure could cause. It is essential that the Year 2000 issues be adequately addressed in arenas beyond the federal government: state and local

governments, the public infrastructure, and other key economic sectors.

State and local governments are responsible for the implementation of many national programs—such as food stamps and Medicaid—while also providing vital local and regional services. Accordingly, Year 2000-induced failures could result in payment delays felt at the local level, or in the interruption of key public services such as law enforcement, traffic management, and emergency and health services. For example, our survey of the state systems used in federal welfare programs revealed that the majority of them were not yet Year 2000 compliant.<sup>15</sup> Failure to complete Year 2000 conversion could result in billions of dollars in benefits payments not being delivered. In an attempt to prevent this for Medicaid systems, HCFA has recently hired a contractor to independently verify and validate state systems.

---

<sup>15</sup>Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998). The survey was conducted in July and August 1998 and included the following welfare programs: Medicaid; Temporary Assistance for Needy Families; Women, Infants, and Children; food stamps; child support enforcement; child care; and child welfare. Forty-nine states, the District of Columbia, and three territories responded to our survey.

The public infrastructure, including critical areas such as power, water, and telecommunications, is particularly important because most, if not all, major enterprises rely on these essential elements for daily functioning. Other key economic sectors include health, safety, and emergency services; banking and finance; transportation; and manufacturing and small business.

These sectors are critical, yet the nation has not had a complete picture of their readiness. Accordingly, in our April 1998 report,<sup>16</sup> we recommended that the President's Council on Year 2000 Conversion develop such a comprehensive picture, to include identifying and assessing risks to the nation's key economic sectors—including risks posed by international links. We also recommended that the Council use a sector-based approach to establishing the effective public-private partnerships necessary to address this issue.

The Council adopted a sector-based focus and has been initiating outreach activities since it became operational last spring. More recently, in October 1998, the Chair directed

---

<sup>16</sup>Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

the Council's sector working groups to begin assessing their sectors. The Chair, in turn, plans to issue periodic public reports summarizing these assessments.<sup>17</sup> These assessments will be used to help prepare contingency plans and aid in crisis management, in which the Council will respond to disruptions that may arise in critical services. Completing these activities is absolutely vital to adequately understanding the full range of national and international risks.

International concerns are underscored by a September 1998 report by the Organization for Economic Co-operation and Development.<sup>18</sup> This report stated that (1) while awareness is increasing, the amount of remediation still required is daunting, (2) significant negative economic impact is likely in the short term, although much uncertainty exists about the extent of

---

<sup>17</sup>The first such report issued on January 7, 1999, summarizes information collected to date and notes that many organizations are still working to gather vital survey data on Year 2000 readiness.

<sup>18</sup>The Organization for Economic Co-operation and Development surveyed its member countries and reviewed existing studies and media reports on the Year 2000 problem and issued a report on its findings, *The Year 2000 Problem: Impacts and Actions* (September 1998). The organization's 29 member countries are Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

Year 2000-induced disruptions, (3) governments face a major public management challenge requiring acceleration of their own preparations and stronger leadership, and (4) stronger international cooperation is essential, especially in conjunction with cross-border testing.

In addition to addressing domestic Y2K issues, the United States has attempted to promote international dialog on the Y2K problem. In June 1998, the United Nations General Assembly adopted a resolution on the global implications of the Year 2000 issue. The resolution recognized that effective operation of governments, companies, and other organizations was threatened by the Year 2000 issue and coordinated efforts were required to address it. The resolution went on to request that all member countries attach a high priority to raising the level of awareness and to consider appointing a nationwide coordinator to tackle the problem.

The Chair of the President's Council also has met with the United Nations and other international bodies, and helped organize a significant December 1998 National Y2K Coordinators' meeting attended by over 120

countries, hosted by the United Nations' Working Group on Informatics. This meeting should help encourage the establishment of regional coordinating mechanisms and foster greater international dialog on the Year 2000 issue.

Further, we have discussed the Year 2000 issue with the leadership of audit organizations from around the world at a recent international conference. Subsequently, we wrote to these leaders to draw greater attention to, and to share with them our recent publications on, this issue.

In summary, considerable progress has been made on the Year 2000 problem, yet a great deal remains to be accomplished. It is critical that priorities continue to be set, rigorous testing be completed, and thorough business continuity and contingency plans be prepared. Further, aggressive and sustained efforts to assess and mitigate national and international Y2K risks in the public infrastructure and key economic sectors are needed. Federal leadership, effective public-private partnerships, and international cooperation are all essential to successfully meeting the Year 2000 challenge. We plan to continue evaluating the effectiveness of these efforts and offer

---

**Addressing Urgent Year 2000  
Computing Challenge**

---

suggestions for mitigating the risk of serious  
disruptions.

---

# Resolving Serious Information Security Weaknesses

---

We designated information security as a governmentwide high-risk area in February 1997 for two basic reasons. First, growing evidence indicated that controls over computerized operations were not effective. In September 1996, we reported that serious security weaknesses were identified at 10 of the largest 15 federal agencies and summarized many recommendations made for needed improvements. Due to the problem's pervasive nature, we also recommended that OMB be more active in overseeing agency practices, in part through its role as chair of the then newly established Chief Information Officers (CIO) Council.<sup>1</sup>

Second, there was compelling information that risks were increasing. Tests at DOD indicated that the number of attacks on its computer systems was increasing and that many attacks were not being detected.<sup>2</sup> In addition, federal agencies, like many private sector organizations, were becoming increasingly dependent on vulnerable interconnected computer systems and on the

---

<sup>1</sup>Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996).

<sup>2</sup>Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

Internet, a trend that continues to accelerate today.

---

**Important Actions Taken**

Since February 1997, greatly increased recognition of the importance of addressing information security problems has led to significant actions.

- In October 1997, our concerns regarding federal information security were corroborated by the President's Commission on Critical Infrastructure Protection.<sup>3</sup> Its report described the potentially devastating implications of poor information security from a national perspective, recognized that the federal government must "lead by example," and included recommendations for improving systems security.
- In late 1997, the CIO Council designated information security a priority area and established a Security Committee. During 1998, the committee sponsored a security awareness seminar and developed plans for improving incident response services.
- In May 1998, Presidential Decision Directive 63 was issued, which established entities within the National Security Council, the Department of Commerce, and the Federal

---

<sup>3</sup>Critical Foundations: Protecting America's Infrastructures, October 1997.

Bureau of Investigation to address critical infrastructure issues. It required each major department and agency to develop a plan for protecting its own critical infrastructure. Other provisions include (1) enhanced analysis of information on threats, (2) assessments of government systems' susceptibility to exploitation, and (3) incorporation of infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

- During 1997 and 1998, the Congress held important hearings on information security that served to clarify issues and set expectations for implementation of needed reforms.

---

**Continuing Weaknesses Underscore Need for Further Actions**

Much more needs to be done to ensure that systems and data supporting critical federal operations are adequately protected. Our views were outlined in a recent report entitled Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998). That report described information security problems across government. Such weaknesses are disturbing because they make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems

and use such access to obtain sensitive information, commit fraud, or disrupt operations.

Examples follow:

- In November 1997, the SSA Inspector General reported that security weaknesses subjected sensitive information to potential unauthorized access, modification, or disclosure.<sup>4</sup> He reported that 29 convictions involving agency employees were obtained during fiscal year 1997, most of which involved creating fictitious identities, fraudulently selling social security cards, misappropriating funds, or abusing access to confidential information. During fiscal year 1998, improvements were noted, but auditors recommended that SSA (1) further strengthen controls to protect its information, (2) accelerate efforts to improve and fully test plans for maintaining continuity of operations, and (3) improve controls over separation of duties.<sup>5</sup>
- In May 1998, we reported that (1) the Department of State's information systems and the sensitive data they maintain were

---

<sup>4</sup>Social Security Accountability Report for Fiscal Year 1997, SSA Pub. No. 31-231, November 1997.

<sup>5</sup>Social Security Accountability Report for Fiscal Year 1998, SSA Pub. No. 31-231, November 1998.

vulnerable to access, change, disclosure, and disruption by unauthorized individuals<sup>6</sup> and (2) weak computer security practices at FAA jeopardize flight safety.<sup>7</sup> In addition to recommendations to correct individual deficiencies, we recommended that each of these agencies strengthen its management structures for planning and implementing information security program.

- In September 1998, we reported that weaknesses at the Department of Veterans Affairs placed critical operations, such as healthcare delivery, benefit payments, and life insurance services, at risk of misuse and disruption. We recommended that the department's CIO correct all identified weaknesses and implement a comprehensive computer security planning and management program.<sup>8</sup>
- In September 1998, we reported that, during our review of two cases of Air Force vendor payment fraud, computer security weaknesses continued to make the Air Force vulnerable to such incidents. We recommended strengthening operating system controls and assessing the need for

---

<sup>6</sup>Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998).

<sup>7</sup>Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

<sup>8</sup>VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

stronger controls over user identifications and passwords.<sup>9</sup>

- In October 1998, we reported that weaknesses at Treasury's Financial Management Service placed billions of dollars of payments and collections at risk of fraud. We recommended that the service assign responsibility and accountability for correcting each identified weakness to designated individuals and implement an effective entitywide security program.<sup>10</sup>
- For the last 7 years, the USDA Inspector General reported serious computer control weaknesses at the National Finance Center, which annually makes over \$21 billion in payroll disbursements to about 434,000 employees and about \$15 billion in other payments. The Inspector General reported that the center had not ensured that (1) systems security adequately prevented misuse or unauthorized modifications, (2) access to data was needed or appropriate, and (3) modifications made to software programs were properly authorized and tested. USDA has actions planned to correct these serious weaknesses.

---

<sup>9</sup>Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

<sup>10</sup>Financial Management Service: Areas for Improvement in Computer Controls (GAO/AIMD-99-10, October 20, 1998).

Although the nature of agency operations and the related risks vary, there are striking similarities in control weaknesses reported. The most widely reported has been poor control over access to sensitive data and systems, such as providing overly broad access privileges to very large user groups, allowing shared passwords and user accounts, and inadequate monitoring of users' activities. Other types of weaknesses pertain to (1) mitigating and recovering from unplanned interruptions in computer service, (2) adequately segregating duties to help ensure that people do not conduct unauthorized actions without detection, and (3) preventing unauthorized software from being implemented.

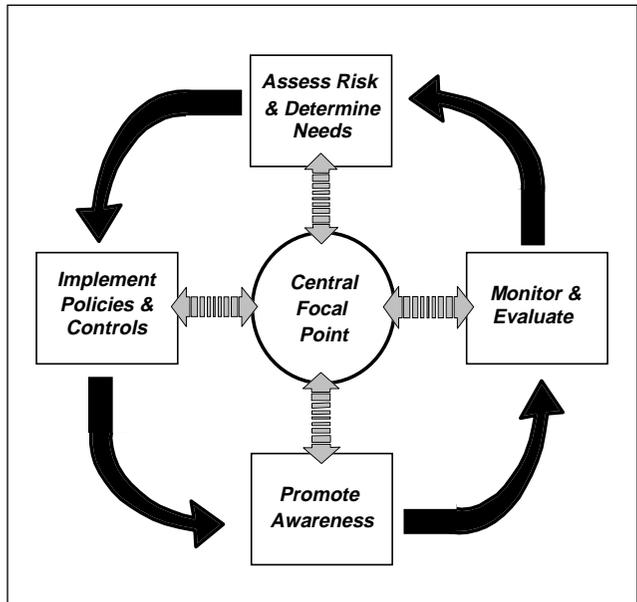
---

**Best Practices Help Shape a Blueprint for Action**

To help further strengthen computer security practices, we issued an executive guide in May 1998 entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). It describes a framework for managing risks through an ongoing cycle of activities coordinated by a central focal point, as shown in figure 2. The guide, which is based on the best practices of organizations noted for superior security programs, has been

endorsed by the Chief Information Officers Council, and distributed to all major agency heads, Chief Information Officers, and Inspectors General.

**Figure 2: The Risk Management Cycle**



**Further Actions Needed**

Security risks to government computer systems are significant, and they are growing. Although efforts have been initiated, improving information security will require a more concerted effort at individual agencies and at the governmentwide level.

First, agencies need to more proactively manage risks. Over the last 2 years, agencies have responded to scores of our recommendations and those of the Inspectors General. However, agencies have reacted to individual audit findings, with not enough attention to the systemic problems. Agencies need to implement comprehensive security programs based on best practices. Second, governmentwide leadership is important to ensure that executives understand their risks, monitor agency performance, and resolve issues affecting multiple agencies.

As these efforts progress, it is important that a comprehensive strategy emerge. As we recently recommended to the Director of OMB and the Assistant to the President for National Security Affairs, such a strategy should<sup>11</sup>

- clearly delineate the roles of federal organizations with responsibilities for information security;
- rank the greatest risks;
- promote proven security tools and best practices;
- ensure the adequacy of workforce skills;

---

<sup>11</sup>Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998).

- provide for evaluating systems on a regular basis; and
- identify long-term goals, as well as time frames, priorities, and annual performance goals.

OMB, the CIO Council, and the National Security Council are working collaboratively on a plan to (1) assess agencies' security postures, (2) implement best practices, and (3) establish a process of continued maintenance. Further, those involved in implementing Presidential Decision Directive 63 and Year 2000 conversion efforts are coordinating their efforts.

The Year 2000 computing challenge is a vivid example of the need to protect critical systems; it illustrates the government's widespread dependence on systems and their vulnerability to disruption. During the Year 2000 conversion period, it is important that agencies be especially attuned to security issues. Most are under severe time constraints to make an unprecedented number of software changes. Consequently, there is a danger that already weak controls will be further compromised if agencies bypass or truncate security in an effort to speed the software modification process. This increases the risk that erroneous or

malicious code will be implemented and that inadequately tested systems will be rushed into use.

The threat of disruption, however, will not end with the advent of the new millennium. There is a long-term danger of attack from malicious individuals or groups; it is imperative that the government's long-term solutions be designed to address this security risk. We will closely monitor this critical area and continue to advance constructive suggestions for improvements.

---

# Ensuring Major Technology Investments Improve Services

---

Successfully applying modern technology is central to improving government operations and generating better service to the American people. Many efforts to achieve such goals have been plagued by huge cost overruns; schedule slippages measured in years; and/or marginal benefits in improving mission performance, cutting costs, and enhancing responsiveness. In 1995, we designated four troubled multibillion dollar modernizations as high risk; their ultimate success is key to the government's future ability to deliver critical services—safe and efficient air travel, modern tax processing and customer service operations, and improved weather forecasting—and in improving systems that support national defense operations.

Since 1995, we have made comprehensive recommendations for each of these efforts that, if implemented, would fundamentally improve project management, introduce needed engineering rigor, and promote disciplined decisions on project funding. Agencies are acting to make needed improvements, but most of our recommendations have not yet been fully implemented. Consequently, serious risks remain.

**High-Risk Information  
Technology Areas**

- *Air Traffic Control Modernization*
- *Tax Systems Modernization*
- *National Weather Service  
Modernization*
- *DOD Systems Development and  
Modernization Efforts*

---

**Air Traffic  
Control  
Modernization**

Faced with rapidly growing traffic volume and aging equipment, the FAA initiated an ambitious air traffic control modernization program in 1981. This effort involves acquiring new air traffic control facilities, as well as a vast network of radar, automated data processing, navigation, and communications equipment, with an expected total cost of \$42 billion through fiscal year 2004. The Congress had appropriated over \$25 billion by fiscal year 1998, and FAA estimates that it will need \$17 billion more for fiscal years 1999 through 2004.

Over the past 17 years, the modernization program has experienced cost overruns, schedule delays, and performance shortfalls of large proportions. Our work has pinpointed solutions to address root causes of such problems.

- In March 1997, we recommended that FAA improve its software acquisition capabilities by institutionalizing mature processes.<sup>1</sup> FAA's processes for acquiring software, the most costly and complex component of air traffic control systems, are ad hoc, sometimes chaotic, and not repeatable across projects. As a result, FAA is at great risk of not delivering promised software capabilities on time and within budget.
- In February 1997, we recommended that FAA develop and enforce a systems architecture.<sup>2</sup> Many systems have been developed without the benefit of a complete systems architecture, or overall blueprint, to guide the program. This has resulted in unnecessarily higher spending to buy, integrate, and maintain hardware and software.

---

<sup>1</sup>Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, March 21, 1997).

<sup>2</sup>Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, February 3, 1997).

- In January 1997, we recommended that FAA institutionalize defined processes for estimating the projects' costs and implement a cost accounting capability.<sup>3</sup> FAA lacks the reliable estimating and cost-accounting practices needed to effectively manage information technology investments. This leaves FAA at risk of making ill-informed decisions on critical multimillion, even billion, dollar air traffic control systems.
- Given the importance and the magnitude of information technology at FAA, we have recommended on multiple occasions that FAA establish an effective Chief Information Officer (CIO) management structure. Such a structure, similar to the department-level CIOs prescribed by the Clinger-Cohen Act, would have a CIO who is solely responsible for the management of information technology and reports directly to the head of the agency.
- In August 1996, we recommended that FAA develop a comprehensive strategy for addressing an organizational culture that has impaired the acquisition process.<sup>4</sup> Employees have acted in ways that did not reflect a strong enough commitment to

---

<sup>3</sup>Air Traffic Control: Improved Cost Information Needed to Make Billion Dollar Modernization Investment Decisions (GAO/AIMD-97-20, January 22, 1997).

<sup>4</sup>Aviation Acquisition: A Comprehensive Strategy Is Needed for Cultural Change at FAA (GAO/RCED-96-159, August 22, 1996).

mission focus, accountability, coordination, and adaptability.

In responding to our recommendations, FAA has started developing a complete air traffic control systems architecture, establishing defined cost-estimating processes, acquiring a cost-accounting system, and improving its software acquisition capability. Most recently, FAA has committed to hiring a CIO who would report directly to FAA's Administrator.

Moreover, in restructuring the modernization program, FAA—in consultation with the aviation community—is developing a phased approach, including a new way of managing air traffic known as “free flight.”<sup>5</sup> Free flight would allow pilots more flexibility in choosing routes and is expected to help improve aviation safety and efficiency. The agency, however, faces many challenges in implementing free flight cost effectively. These include developing detailed plans in collaboration with the aviation community and addressing outstanding issues related to the development and deployment of technology.

---

<sup>5</sup>National Airspace System: FAA Has Implemented Some Free Flight Initiatives, But Challenges Remain (GAO/RCED-98-246, September 28, 1998).

While improvements have been initiated, FAA's reform efforts are not yet completed, and several major projects continue to face challenges that could affect their cost, schedule, and performance. See Major Management Challenges and Program Risks: Department of Transportation (GAO/OCG-99-13, January 1999) for additional information on FAA's air traffic control modernization.

---

## **Tax Systems Modernization**

IRS has spent over \$3 billion during the last decade attempting to modernize its outdated, paper-intensive approach to tax return processing. Our reviews over the past few years identified serious management and technical weaknesses with IRS' modernization, and we made recommendations to help IRS, among other things, build the capability necessary to successfully modernize its systems. IRS has agreed to implement our recommendations and is working to build its capability before it begins modernizing tax processing systems.

In 1995, we identified serious management and technical weaknesses in IRS' modernization that jeopardized its successful completion; more than a dozen

recommendations were made.<sup>6</sup> In 1996, the Congress limited IRS information technology spending to certain cost-effective categories until it had successfully implemented our recommendations.<sup>7</sup> IRS has continued to act in this regard. For example:

- IRS hired a CIO and created an investment review board to select, control, and evaluate information technology investments. Together, they reviewed and terminated marginal systems development projects.
- In May 1997, IRS provided the first two levels of a four-level modernization blueprint to the Congress.
- In December 1998, IRS engaged a prime systems modernization integration contractor to overhaul its systems over the next 10 to 15 years.

IRS' 1997 blueprint was a good first step and provides a solid foundation from which to define the level of detail and precision needed to build a modernized system.<sup>8</sup>

---

<sup>6</sup>Tax Systems Modernization: Management and Technical Weaknesses Must Be Corrected If Modernization Is to Succeed (GAO/AIMD-95-156, July 26, 1995).

<sup>7</sup>Tax Systems Modernization: Actions Underway But Management and Technical Weaknesses Not Yet Corrected (GAO/T-AIMD-96-165, September 10, 1996).

<sup>8</sup>Tax Systems Modernization: Blueprint Is a Good Start But Not Yet Sufficiently Complete to Build or Acquire Systems (GAO/AIMD/GGD-98-54, February 24, 1998).

However, until these levels are complete, IRS will not have fully addressed our recommendations calling for disciplined processes and a complete information system architecture.

The IRS Commissioner agreed with our findings and the Congress limited IRS' ability to obligate information technology investment funds until certain conditions were met. These include that IRS submit to the Congress for approval an expenditure plan that (1) implements the blueprint, (2) meets the requirements of OMB's system investment guidelines, (3) is reviewed and approved by OMB and Treasury's IRS Management Board, and (4) is reviewed by us.

Additional information on IRS' readiness and capability to effectively modernize its systems is presented in Major Management Challenges and Program Risks: Department of the Treasury (GAO/OCG-99-14, January 1999).

---

**National Weather  
Service  
Modernization**

The National Weather Service (NWS) began a nationwide program in the 1980s to upgrade observing systems, such as satellites and radars, to achieve more uniform weather services across the nation, improve

forecasts, provide better prediction of severe weather and flooding, and achieve higher productivity. NWS' modernization includes four major programs: the Next Generation Weather Radar, the Next Generation Geostationary Operational Environmental Satellite, the Automated Surface Observing System, and the Advanced Weather Interactive Processing System (AWIPS).

In 1997, we reported that although the deployment of the observing systems were nearing completion, unresolved issues concerning the systems' operational effectiveness and efficient maintenance remained. To illustrate, we reported that the new radars were not always up and running when severe weather was threatening, and the ground-based sensors fell short of performance and user expectations. We recommended that NWS correct shortfalls in radar performance and define and prioritize all ground-based sensor corrections needed to meet user needs.<sup>9</sup> NWS addressed some of these performance concerns, but others remain. We recently reported that a radar located in Southern California was not consistently meeting availability

---

<sup>9</sup>Weather Forecasting: Radar Availability Requirements Not Being Met (GAO/AIMD-95-132, May 31, 1995) and Weather Forecasting: Unmet Needs and Unknown Costs Warrant Reassessment of Observing System Plans (GAO/AIMD-95-81, April 21, 1995).

requirements and recommended that NWS correct the problems. NWS concurred and mentioned several planned activities to improve radar availability.<sup>10</sup>

Although NWS is nearing completion of its modernization, we remain concerned about its lack of an overall architecture and ability to deliver the final piece of the modernization—AWIPS. NWS has acknowledged that a technical blueprint is needed to guide the effort; however, it has made little progress in developing the architecture. In the meantime, NWS will continue to incur higher costs and experience reduced performance.<sup>11</sup>

The centerpiece of the modernization, AWIPS—the forecaster workstations that are to integrate observing systems' data and support forecaster decisionmaking—is far from providing all the promised capabilities. It has been delayed and become more expensive because of design problems and management shortcomings. AWIPS is now scheduled to be deployed in June 1999, but with less than full functionality. Until this

---

<sup>10</sup>National Weather Service: Sulphur Mountain Radar Performance (GAO/AIMD-99-7, October 16, 1998).

<sup>11</sup>Weather Forecasting: Systems Architecture Needed for National Weather Service Modernization (GAO/AIMD-94-28, March 11, 1994).

system is deployed and functioning properly, NWS will not be able to take full advantage of the total \$4.5 billion investment it has made in the modernization.

For the past several years, we have reported that serious risks continue to be associated with AWIPS' costs, schedule, development, and maintenance.<sup>12</sup> In 1996, we made several recommendations to (1) improve NWS' process to test software and establish a software quality assurance program, (2) obtain an independent cost estimate since NWS does not have reliable project cost information, and (3) validate all workstation requirements on the basis of mission impact.<sup>13</sup>

NWS officials have acted on all these recommendations. They said they are continuing to strengthen their software development and testing processes, and an independent cost estimate and requirements validation review were completed in February and August 1998, respectively.

---

<sup>12</sup>National Weather Service: Budget Events and Continuing Risks of Systems Modernization (GAO/T-AIMD-98-97, March 4, 1998) and Weather Service Modernization: Risks Remain That Full Systems Potential Will Not Be Achieved (GAO/T-AIMD-97-85, April 24, 1997).

<sup>13</sup>Weather Forecasting: Recommendations to Address New Weather Processing Systems Development Risks (GAO/AIMD-96-74, May 13, 1996).

These reviews concluded that AWIPS costs will increase at least \$20 million and that some requirements should not be pursued.

NWS reports that it is making considerable progress on the development and testing of the forecaster workstations. However, we continue to be concerned about cost, schedule, and technical risks associated with the workstations. The NWS modernization is further discussed in Major Management Challenges and Program Risks: Department of Commerce (GAO/OCG-99-3, January 1999).

---

## **DOD Systems Development and Modernization Efforts**

DOD has taken steps to implement legislative requirements to institute modern information technology management practices. However, it faces a major challenge in changing its current organizational structure and culture. This impedes oversight and coordination of information resources from a departmentwide perspective. In previous reports, we have designated DOD's information technology project management as high risk. In those reports, these efforts were referred to as the "Corporate Information Management Initiative," a term that is no longer widely used in DOD.

A prime example of DOD's poor management of information technology is its \$18 billion system migration effort to replace almost 2,000 duplicative and inefficient systems. One functional area of the migration effort, which we reported on in 1996, spent over \$700 million pursuing a substantially flawed effort—which was later abandoned—without rigorous department-level oversight.<sup>14</sup> In October 1997, we reported that the department had little assurance that the migration systems being developed would help achieve DOD's technology goals.

Effective information technology project planning and oversight are especially important as DOD moves to coordinate its thousands of decentralized command, control, communications, intelligence, surveillance, and reconnaissance systems in order to ensure information superiority over our nation's enemies. To this end, we made a number of recommendations that would establish and enforce processes to thoroughly examine alternatives and develop business cases before investing in new systems. Further, we recommended that system investments be consistent with

---

<sup>14</sup>Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy At Risk (GAO/AIMD-98-5, October 20, 1997).

department technical standards and that controls and performance measures be established to allow management “visibility” over system development efforts. The department generally agreed with these recommendations and is now finalizing a plan that will show how it intends to comply with new federal information technology management requirements.

DOD’s systems development and modernization efforts are discussed in Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999).

---

**Other  
Modernization  
Efforts Bear  
Watching**

Unfortunately, these four high-risk modernizations are not the only indications of the difficulties facing agencies across government in successfully harnessing modern information technology. Our initial designation of these major modernizations as high risk in early 1995, along with our research on best practices of leading organizations in managing information

technology,<sup>15</sup> helped create a consensus between the Congress and the executive branch to pass major management reforms. These included the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996, which set forth requirements for improving government operations through more effective use of information technology. Requirements include establishing Chief Information Officers and using proven modern investment and management practices.

The status of these reforms is outlined in our report Major Management Challenges and Program Risks: A Governmentwide Perspective (GAO/OCG-99-1, January 1999). It is important to note that such reforms are in their early stages of implementation and have been complicated by the urgent need to address Year 2000 issues. Consequently, we are not designating any new modernizations

---

<sup>15</sup>Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology—Learning From Leading Organizations (GAO/AIMD-94-115, May 1994), Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making (GAO/AIMD-10.1.13, February 1997), Business Process Reengineering Assessment Guide (GAO/AIMD-10.1.15, April 1997), Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments (GAO/AIMD-98-89, March 1998), Executive Guide: Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998), and Executive Guide: Leading Practices in Capital Decision-making (GAO/AIMD-99-32, December 1998).

as high risk at this time. However, going forward, there are planned modernizations that bear watching in such departments as Agriculture, State, Interior, and Treasury and in the Agency for International Development. These issues are highlighted in the series of management booklets on individual agencies that is being issued concurrently with this high-risk update.

---

# Providing Basic Financial Accountability

---

Our early high-risk reports describing the serious consequences of financial management deficiencies helped highlight the need for major reforms, which the Congress passed in the 1990 Chief Financial Officers (CFO) Act, as expanded by the 1994 Government Management Reform Act. These laws called for strengthening financial accountability and producing more reliable cost and performance information on federal operations. Two of the most basic mandates are that (1) major departments and agencies now produce annual financial statements subject to independent audit beginning with those for fiscal year 1996 and (2) the Secretary of the Treasury, in cooperation with the Director of OMB, prepare financial statements for the U.S. government, starting with those for fiscal year 1997, that are audited by GAO.

These requirements are prompting steady improvements in financial accountability, as discussed more fully in our overview document on the status of management reforms in government.<sup>1</sup> However, progress is very uneven. As figure 3 shows, 11 of the 24 CFO Act departments and agencies received unqualified opinions on their fiscal

---

<sup>1</sup>Major Management Challenges and Program Risks: A Governmentwide Perspective (GAO/OCG-99-1, January 1999).

year 1997 financial statements. However, several major departments are not yet able to produce auditable financial statements consistently.

Audited financial statements are essential to identifying any serious financial management problems that might exist, to helping ensure accountability, and to providing an annual public scorecard on accountability. An unqualified audit opinion on those statements, however, while certainly important, is not an end in itself. The CFO Act is focused on providing accurate, timely, relevant financial information needed for management decisionmaking and accountability, on a systematic basis, throughout the year. Efforts to obtain reliable year-end data that are not backed up by fundamental improvements in underlying financial management systems and operations that enable the routine production of accurate, relevant, timely data to support ongoing program management and accountability will not achieve the intended results of the CFO Act over the long-term.

Figure 3: The 24 CFO Agencies' Fiscal Year 1997 Financial Statement Audit Opinions

**Unqualified audit opinions were received by:**

- *Education*
- *Labor*
- *GSA*
- *SBA*
- *Energy*
- *State*
- *NASA*
- *SSA*
- *Interior*
- *EPA*
- *NRC*

**Qualified audit opinions were received by:**

- *HHS*
- *VA*
- *HUD*
- *NSF*

**Disclaimers were received by:**

- *Agriculture*
- *Defense*
- *Transportation*
- *Commerce*
- *Justice*
- *AID*

**Other CFO agencies:**

- *Treasury received an unqualified opinion on its administrative financial statements and a qualified opinion on its custodial schedules.*
- *FEMA received an unqualified opinion on a financial statement for a part of the agency. Financial statements were not prepared for the whole agency.*
- *OPM's Retirement Fund and Life Insurance Fund received unqualified opinions; revolving funds, health benefits, and salaries and expenses received disclaimers.*

Our first ever audit of the U.S. government's financial statements framed the most serious challenges across government. In summary, significant financial systems weaknesses, problems with fundamental recordkeeping, incomplete documentation, and weak internal controls, including computer controls, prevented the government, as a whole, from accurately reporting a large portion of its assets, liabilities, and costs. Such deficiencies also precluded us from being able to form an opinion on the reliability of the government's financial statements.

The President reacted strongly, requiring agency heads to submit plans to OMB to correct deficiencies. Financial management reform was designated a top management priority of the executive branch, behind the Year 2000 computing problem. The House of Representatives also passed a resolution urging quick resolution of these problems.

We are working with OMB, the Treasury, and agencies across government to provide recommendations for fixing the major deficiencies cited in our audit. The most serious situations are candidates for high-risk designations. A high-risk designation is intended to highlight

individual departments and agencies that are material to the government's financial statements and have been unable to produce auditable financial statements for their own operations.<sup>2</sup>

The most significant in this regard is DOD, which represents a large percentage of the government's assets, liabilities, and net costs. None of the military services or the department as a whole have yet been able to produce auditable financial statements. We designated DOD financial management to be a high-risk area in 1995 and it remains so today, although we have seen increased attention to rectify this situation.

Two other large organizations also have been unable to produce auditable statements for their entire operations—USDA and DOT. Unlike DOD, however, significant parts of these organizations have been able to produce auditable statements while other major components have not. Consequently, we are adding the most problematic parts of these departments to the high-risk list—financial management at the Forest

---

<sup>2</sup>Other departments and agencies also still need to improve their financial management operations. Challenges facing them in this area are discussed in our series of reports on agencies' performance and accountability. (See GAO/OCG-99-1 through GAO/OCG-99-21, January 1999.)

Service at USDA and financial management at the Federal Aviation Administration at DOT.

Another major focus of the government's financial management entails its revenue collection operations. As a result, we have looked closely at IRS and the Customs Service, which together account for virtually all the government's revenue. We have designated both areas high risk in the past.

IRS has made progress recently and was able for the first time to obtain an unqualified opinion on its financial statements for fiscal year 1997, after five previous attempts did not yield auditable statements. However, achieving this outcome took extraordinary effort, including material audit adjustments, and several serious weaknesses remain regarding refunds, receipts, and unpaid tax assessments. Also, important new accounting and reporting requirements became effective for fiscal year 1998 and these will present new challenges for IRS. Until IRS can demonstrate a consistent ability to produce auditable statements, meet the new requirements, and make greater progress in addressing significant material weaknesses, we still consider its revenue accounting to be high risk, especially given the fact that it collected over \$1.7 trillion in

revenue in fiscal year 1998—virtually all of the government’s revenue.

The Customs Service has made major financial management strides, including several important improvements in its ability to assess and collect duties and excise taxes and receiving unqualified opinions on its financial statements for the past 2 fiscal years. Therefore, we no longer consider Customs financial management high risk; thus, we are removing the high-risk designation, although we will continue to monitor Customs’ progress.

---

**High-Risk  
Financial Management Areas**

- *DOD Financial Management*
- *Forest Service Financial Management<sup>1</sup>*
- *FAA Financial Management<sup>1</sup>*
- *IRS Financial Management and Receivables*

<sup>1</sup>*Added in 1999*

---

**DOD Financial  
Management**

DOD is responsible for hundreds of billions of dollars of assets worldwide and, with a budget of an estimated \$250 billion annually, it is accountable for about half of the government's discretionary spending. However, long-standing weaknesses in DOD's financial management operations undermine DOD's ability to efficiently manage its vast operations, limit the reliability of financial information provided to the Congress, and continue to result in wasted resources. Since 1995, we have monitored DOD's efforts as it has struggled to resolve the many problems brought about by decades of inattention to sound financial management practices.

Examples follow:

- DOD has not properly accounted for and reported billions of dollars of property, equipment, inventory, and supplies.<sup>3</sup> For example, recorded information on the number and location of several military equipment items—such as F-4 engines and service craft—was not reliable and on-hand quantities of inventories differed by

---

<sup>3</sup>Department of Defense: Financial Audits Highlight Continuing Challenges to Correct Serious Financial Management Problems (GAO/T-AIMD/NSIAD-98-158, April 16, 1998).

23 percent from inventory records at selected major storage locations.<sup>4</sup>

- DOD has not properly accounted for billions of dollars of basic transactions. For example, DOD was unable to reconcile at least \$4 billion in differences between checks issued by DOD and reported to the Treasury Department. In addition, DOD reported an estimated \$22 billion in disbursements that it has been unable to match with corresponding obligations.<sup>5</sup>
- DOD has not accurately reported the net costs of its operations and has acknowledged its fundamental problems in accumulating reliable cost information. DOD's 1998 Annual Report to the President and the Congress cited the lack of a widespread, robust cost accounting system as the single largest impediment to controlling and managing weapon system life-cycle costs.
- DOD has not ensured that all disbursements were properly recorded and reconciled. For example, we recently reported that weak controls led to two fraud cases involving nearly \$1 million in embezzled Air Force vendor payments and that similar control weaknesses continue to leave Air Force

---

<sup>4</sup>Financial Audit: DOD Mission Asset Existence Verification (GAO/AIMD-98-196R, May 29, 1998).

<sup>5</sup>GAO/T-AIMD/NSIAD-98-158, April 16, 1998.

funds vulnerable to additional fraudulent and improper vendor payments.<sup>6</sup>

- DOD has not adequately determined its liability associated with the future cost of post-retirement health benefits for military employees, reported in the neighborhood of \$220 billion.<sup>7</sup>
- DOD has not estimated and reported on material environmental and disposal liabilities. While DOD reported nearly \$40 billion in estimated environmental cleanup and disposal liabilities for fiscal year 1997, it excluded costs associated with military weapon systems or training ranges—which are likely to be an additional tens of billions of dollars.<sup>8</sup>

To achieve the wide-ranging reforms necessary to address its long-standing financial management deficiencies, we have made numerous recommendations to DOD regarding its need to upgrade the skills of its financial personnel and successfully overcome serious design flaws in its financial systems.

---

<sup>6</sup>Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

<sup>7</sup>GAO/T-AIMD/NSIAD-98-158, April 16, 1998.

<sup>8</sup>GAO/T-AIMD/NSIAD-98-158, April 16, 1998.

DOD's financial operations involve about 32,000 financial management personnel. Our survey of over 1,400 key DOD financial managers—individuals often serving in comptroller, deputy comptroller, or budget officer positions—showed that over half (53 percent) had received no financial or accounting-related training during 1995 and 1996. These personnel will be challenged to lead DOD's reform efforts to produce reliable financial data based on more comprehensive accounting standards and systems requirements throughout a large and complex organization with acknowledged difficult financial deficiencies. We made recommendations directed at developing and implementing a formalized, structured training program for financial personnel throughout the department. The department's response to our report expressed agreement with our overall conclusion regarding providing a strong emphasis on training as a means of upgrading workforce accounting knowledge.<sup>9</sup>

Until DOD has developed integrated financial management systems, its operations will continue to be burdened by costly,

---

<sup>9</sup>Financial Management: Training of DOD Financial Managers Could Be Enhanced (GAO/AIMD-98-126, June 24, 1998).

error-prone systems that do not provide financial controls to ensure that DOD's assets are safeguarded, its resources are appropriately accounted for, or the cost of its activities are accurately measured. Concern continues over whether DOD has (1) comprehensively identified all the systems it relies on to carry out its financial management operations, (2) corrected weaknesses that would allow both hackers and hundreds of thousands of legitimate users with valid access privileges to modify, steal, or inappropriately disclose, and destroy sensitive DOD data, and (3) effectively documented how it conducts its financial management operations now and plans to in the future.<sup>10</sup>

DOD has many well-intentioned planned and ongoing improvement efforts. DOD is developing a detailed action plan, in collaboration with OMB and the audit community, to identify short-term initiatives to address financial reporting deficiencies. Further, the National Defense Authorization Act of 1998 requires DOD to develop a broad-based plan for improving its financial operations. In response, in late October 1998, DOD issued its first Biennial Financial Management Improvement Plan.

---

<sup>10</sup>GAO/T-AIMD/NSIAD-98-158, April 16, 1998.

DOD's plan represents an important step in improving the department's financial management operations. The plan, however, needs to be supplemented with additional elements in order to address all of the needed aspects of long-term financial management performance improvement.

See Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999) for additional information on DOD's financial management weaknesses.

---

**Forest Service  
Financial  
Management**

Since its first audit of the Forest Service's financial statements, which covered fiscal year 1991, the USDA Inspector General (IG) has found serious accounting and financial reporting weaknesses. These include pervasive errors in the field-level data supporting land, buildings, equipment, accounts receivable, and accounts payable accounts. Thus, when the IG issued an adverse audit opinion in July 1996, concluding that the Forest Service's financial statements for fiscal year 1995 were unreliable, the findings represented a continuing pattern of unfavorable conclusions about the Forest Service's financial statements.

Due to the severity of the accounting and reporting deficiencies, the Forest Service did not prepare financial statements for fiscal year 1996, but chose instead to focus on trying to resolve these problems. The Forest Service's goal was to correct some of the deficiencies during fiscal year 1997 and to achieve financial accountability—which the agency defines as an unqualified audit opinion—by the end of fiscal year 1999.

The IG's audit of Forest Service fiscal year 1997 financial statements disclosed continuing major weaknesses in accounting and reporting, particularly for real property (land, buildings, and roads), accounts receivable, and accounts payable. Errors were also detected in the Forest Service's records when it attempted to reconcile its fund balance with the Department of the Treasury's records. As a result, the IG was unable to determine the reliability of the Forest Service's fiscal year 1997 financial statements and, therefore, issued a disclaimer of opinion.

For example, the IG could not verify the balance for the Forest Service's reported \$8.2 billion in real property because inventories and valuations of these assets had not been completed at the time of the

audit.<sup>11</sup> The IG also could not verify the accuracy of the reported \$119 million in accounts receivable because the Forest Service did not maintain centralized records of individual accounts. Also, the IG reported that adjustments to accounts receivable totaling about \$166 million could not be verified because the automated data files documenting the adjustments had been recorded over and, therefore, were no longer available. Similarly, the Forest Service continued to lack a system that provided detailed accounts payable balances, and relied instead on its obligations system to estimate accounts payable at year-end. This precluded the agency from knowing costs it had incurred and amounts owed to others at any given point throughout the year. These weaknesses mean that Forest Service managers' ability to effectively manage operations, monitor revenue and spending levels, and make informed decisions about future funding needs will continue to be hampered until corrective measures are completed.

The aforementioned problems were exacerbated by problems with the Forest Service's partial implementation of its new

---

<sup>11</sup>Forest Service: Barriers to Financial Accountability Remain (GAO/AIMD-99-1, October 2, 1998).

financial accounting system. This system was unable to produce certain critical budgetary and accounting reports that track obligations, assets, liabilities, revenues, and costs for the units that converted to the new system.<sup>12</sup> Since January of 1998, we, the IG, and an outside consultant hired by Forest Service have identified serious problems with the implementation process for the new system. These problems were caused by, among other things, not simplifying the Forest Service's business processes before the system was implemented, adding feeder systems, implementing the system before it was fully tested, and inadequate oversight and management control over the project.

Although major barriers to financial accountability still remain, the Forest Service has begun and/or completed several actions, that, if successfully carried through, represent important steps towards achieving financial accountability. For example, the Forest Service has substantially completed equipment inventories and is in the process of correcting the erroneous data recorded in its old accounting system. In addition, the Forest Service has issued an accounting desk guide for all staff that provides uniform

---

<sup>12</sup>Forest Service: Status of Progress Toward Financial Accountability (GAO/AIMD-98-84, February 27, 1998).

accounting instructions. This guide, if consistently used, should help improve the accuracy of data entered into the new system. Further, Forest Service management continues to emphasize the importance of financial accountability to its line managers, has established a team to improve selected financial processes, and has obtained advice from outside consultants on how to improve its financial operations.

While the Forest Service has committed considerable resources and progressed in addressing some of its long-standing financial management deficiencies, much work remains. Also, the problems encountered in implementing the new accounting system have been a major setback. Because of the serious nature of these long-standing problems, we are designating Forest Service financial management a high-risk area. Also see Major Management Challenges and Program Risks: Department of Agriculture (GAO/OCG-99-2, January 1999).

financial information provided to the Congress. Since 1994, the Department of Transportation's Office of the Inspector General has undertaken audits of FAA's financial statements and has consistently reported that it has been unable to determine whether the financial information presented is reliable.

In the fiscal year 1997 audit report, the Inspector General was unable to express an opinion on the reliability of FAA's financial statements because property, plant, and equipment—reported at about \$12 billion—and inventory and related property—reported at \$764 million—could not be verified. Deficiencies included (1) FAA's lack of comprehensive inventory counts, (2) inaccurate general ledger balances and subsidiary records, (3) inadequate supporting documentation, and (4) unreconciled discrepancies between general ledger balances maintained in FAA's accounting system and its subsidiary records.

We have reported that problems in accounting for property, plant, and equipment affect FAA's ability to properly manage these assets and may result in

operating inefficiencies.<sup>13</sup> For example, mission-critical equipment, such as radars and other air traffic control equipment, may be difficult to locate when needed, which could exacerbate an emergency situation. Also, theft could go undetected, and funds could be spent unnecessarily to acquire equipment that is already on hand. The lack of accurate inventory information may result in program officials' inability to make prudent business decisions and safeguard assets adequately and may also impair operational effectiveness. For example, inaccurate inventory information may result in a shortage of, or the inability to locate, essential parts necessary to repair mission-critical systems. Further, funding requests may not be based on actual needs, unnecessary purchases may be made, and inventory may be overstocked or hoarded due to availability concerns.

Many problems in the property, plant, and equipment and inventory accounts result from the lack of a reliable system for accumulating project cost accounting information. The lack of cost accounting information also limits FAA's ability to (1) make effective decisions about resource

---

<sup>13</sup>Financial Management: Federal Aviation Administration Lacked Accountability for Major Assets (GAO/AIMD-98-62, February 18, 1998).

needs and adequately control major projects, such as the \$42 billion air traffic control modernization program, (2) estimate future costs for purposes of preparing and reviewing budgets, (3) control and reduce costs in order to increase efficiency and avoid waste, (4) develop a system of user fees based on the cost of services provided, and (5) meaningfully evaluate performance measures in terms of efficiency and cost-effectiveness.

On September 30, 1998, DOT submitted a plan to OMB to resolve its financial reporting deficiencies including FAA's property, plant, and equipment and inventory deficiencies. In addition, FAA has efforts underway to implement its cost accounting system, but plans for full implementation have slipped from October 1, 1998, to March 31, 1999. This new date has been described by the Inspector General as very ambitious. Until FAA implements effective policies and procedures to provide accountability over inventory and property, plant, and equipment, including implementing a reliable cost accounting system, it remains vulnerable to significant mismanagement of appropriated funds used to acquire these assets. Therefore, we are adding FAA's financial management to our high-risk list.

These problems also are among those discussed in Major Management Challenges and Program Risks: Department of Transportation (GAO/OCG-99-13, January 1999).

---

---

**IRS Financial  
Management**

In fiscal year 1997, IRS received an unqualified opinion on its custodial financial statements for the first time since we began auditing them in fiscal year 1992.<sup>14</sup> This achievement was largely attributable to IRS' efforts to reconcile tax receipt and refund activity between its systems and those of Treasury's Financial Management Service. However, IRS had to use extensive ad hoc procedures to enable it to prepare auditable financial statements because of its inability to rely on the general ledger system to support its financial statements. To compensate, IRS uses specialized computer programs to extract information from its master files—its only detailed database of taxpayer information—to derive amounts to be reported in the financial statements. However, the amounts produced by this approach needed material audit adjustments to produce reliable financial statements.

---

<sup>14</sup>The custodial financial statements did not report on activities related to IRS' administrative costs funded by appropriations and reimbursements from other agencies, state and local governments, and the public. These activities were reported separately in IRS' administrative financial statements, which were audited by the Treasury Office of Inspector General.

In our audit report on IRS' fiscal year 1997 financial statements, we cited long-standing material weaknesses that prevented IRS from routinely generating timely and reliable information as a tool for managing its operations or as a basis for preparing financial statements.<sup>15</sup> These weaknesses also expose the federal government and taxpayers to financial loss and create an undue burden for taxpayers. IRS' primary internal control weaknesses relate to tax receipts, taxpayer data, tax refunds, and unpaid tax assessments. We have issued reports providing IRS with numerous recommendations for both short- and long-term corrective actions to address these weaknesses.

IRS generally agreed with our recommendations and has initiated corrective actions. However, many initiatives, which include IRS' systems modernization effort and plans to improve its financial reporting capabilities are long term and, according to IRS, may take 10 years or more of sustained effort to fully implement. Some other issues can be resolved in the next few years by improving policies, procedures, and internal controls,

---

<sup>15</sup>Financial Audit: Examination of IRS' Fiscal Year 1997 Custodial Financial Statements (GAO/AIMD-98-77, February 26, 1998).

as discussed below. These weaknesses underscore the extent to which IRS still has extensive work ahead to resolve its financial management and internal control deficiencies. IRS' financial management, therefore, continues to be a high-risk area.

---

**Internal Control  
Weaknesses With  
Regard to Tax  
Receipts and  
Taxpayer Data**

IRS' controls over tax receipts and taxpayer data do not adequately reduce the vulnerability to theft and inappropriate disclosure. For example, receipts were left in unrestricted areas accessible to individuals not authorized to handle receipts. In addition, employees were hired and worked in positions requiring the handling of cash, checks, or sensitive taxpayer information before IRS received the results of their background or fingerprint checks. Of the 80 thefts IRS investigated at service centers from January 1995 through July 1997, 12 (15 percent) were committed by individuals who had previous arrest records or convictions that were not identified before their employment. In addition, we found that single, unarmed couriers were used to transport IRS deposits totaling hundreds of millions of dollars to the depository institutions during the peak filing season. One courier left a deposit totaling more than \$200 million unattended in an open vehicle

while he returned to the service center. At one district office, IRS relied upon a bicycle messenger to deliver daily deposits ranging from more than \$1 million during the nonpeak season to more than \$100 million during the peak season.

Although receipts and taxpayer information will always be vulnerable to theft, IRS has a responsibility to protect the government and taxpayers from such losses. In November 1998, we made recommendations to (1) prohibit new employees from being assigned to process receipts until fingerprint checks are received and reviewed by management, (2) enhance physical security over receipts and taxpayer data on hand, and (3) improve the level of security over receipts and taxpayer data in transit to depository institutions.<sup>16</sup> IRS generally agreed and has indicated plans to address our recommendations.

---

**Internal Control  
Weaknesses With  
Regard to Tax  
Refunds**

IRS' internal controls for the issuance of tax refunds need strengthening. Because of weaknesses in its internal controls over issuing tax refunds, IRS sometimes issued refunds that were based on erroneous or

---

<sup>16</sup>Internal Revenue Service: Physical Security Over Taxpayer Receipts and Data Needs Improvement (GAO/AIMD-99-15, November 30, 1998).

fraudulent refund claims filed by taxpayers, tax preparers, or IRS employees, or were disbursed in incorrect amounts due to discrepancies between tax returns and corresponding other third-party documentation that IRS did not catch due to significant delays in its procedure for comparing these documents. IRS also lacked adequate internal controls to prevent duplicate refunds from being issued. In addition, the Earned Income Credit program is subject to high rates of invalid or overstated claims, as discussed further later in the IRS tax filing fraud section of this report.

---

**Internal Control  
Weaknesses Over  
Unpaid Tax  
Assessments**

IRS does not have a detailed listing that tracks and accumulates unpaid tax assessments on an ongoing basis.<sup>17</sup> The lack of a subsidiary ledger impairs IRS' ability to effectively manage its unpaid assessments. This weakness has resulted in IRS inappropriately directing collection efforts against taxpayers after amounts owed had been paid. In one case, three taxpayers had multimillion dollar tax liabilities and liens placed against their property, although the taxes had actually been paid and two of the

---

<sup>17</sup>Internal Revenue Service: Immediate and Long-Term Actions Needed to Improve Financial Management (GAO/AIMD-99-16, October 30, 1998).

individuals were owed refunds. In addition, IRS must rely on computer programs to extract data from its master files to prepare its financial statements, a process that necessitated tens of billions of dollars in adjustments to correct misclassifications and eliminate duplicate transactions in fiscal year 1997. IRS also lacks adequate documentation to support its unpaid assessments. For example, the estate case files we reviewed generally did not include audited financial statements or an independent appraisal of the estate's assets—information that would greatly assist in determining collectibility and underreporting. Such weaknesses inhibit focusing on those accounts with the greatest degree of collection potential.

IRS financial management issues are discussed in more detail in Major Management Challenges and Program Risks: Department of the Treasury (GAO/OCG-99-14, January 1999).

---

## IRS Receivables

While IRS collected over \$1.7 trillion in tax revenue in fiscal year 1998, it has not been able to collect a significant portion of the

amount of taxes due the government.<sup>18</sup> This problem has been compounded by serious system deficiencies and the lack of sound, reliable information, which impede IRS' efforts to collect unpaid tax assessments.

As of September 30, 1997, IRS had identified \$214 billion in unpaid tax assessments. These assessments, which have historically been referred to as IRS' accounts receivable, consist of (1) \$90 billion in taxes due from taxpayers for which IRS can support the existence of a federal tax receivable through taxpayer agreement or a favorable court ruling,<sup>19</sup> (2) \$48 billion in compliance assessments for which neither a taxpayer nor a court has affirmed that the amounts are owed, and (3) \$76 billion in write-offs, which represent unpaid assessments for which IRS does not expect further collection because of factors such as the taxpayer's death, bankruptcy, or insolvency.

Under federal accounting standards, only the \$90 billion in unpaid assessments that IRS can support by taxpayer agreement or

---

<sup>18</sup>Internal Revenue Service: Composition and Collectibility of Unpaid Assessments (GAO/AIMD-99-12, October 29, 1998).

<sup>19</sup>When Statement of Federal Financial Accounting Standards No. 7 became effective for fiscal year 1998, these transactions were redefined and are now appropriately referred to as federal taxes receivable.

favorable court ruling represent federal taxes receivable. For the first time since we began auditing IRS, the agency has reported a reasonable estimate of the amount of federal taxes receivable it expects to ultimately collect. This amount, \$28 billion as of September 30, 1997, represents just 31 percent of the total of federal taxes receivable, and just 13 percent of the total balance of unpaid assessments.

Our work has shown that this low level of expected collectibility is a reasonable estimate given the composition of IRS' unpaid assessments. The \$76 billion in write-offs are amounts primarily due from bankrupt and insolvent taxpayers, including billions in delinquent taxes that are owed by failed financial institutions and thus have virtually no hope of collection. The \$48 billion in compliance assessments are primarily amounts that are owed by individuals and businesses for income and payroll taxes. However, IRS' future prospects of collecting these amounts are low because (1) these taxpayers have not acknowledged the debt and (2) in many instances, these amounts are derived through IRS' various compliance and enforcement programs and may not ultimately represent the amounts actually owed by the taxpayer.

Of the \$90 billion in taxes receivable, our work has shown that \$62 billion (68 percent) is also not likely to be collectible. This amount is owed primarily by taxpayers (1) experiencing financial hardships, (2) undergoing bankruptcy, or (3) unwilling to pay some or all of the amounts they owe. Only \$28 billion of the \$90 billion of taxes receivable represents amounts where collection is likely based on the financial status and willingness by the taxpayers to pay some or all of the amounts they owe.

Striving to close the gap between the amount of tax revenue owed the government and the amount likely to be collected is a major challenge for IRS. However, IRS' long-standing systems deficiencies make this challenge even more difficult. IRS has continually tried to manage its federal taxes receivable and other unpaid assessments with systems that are unable to provide timely, useful, and reliable information on the status of taxpayers' accounts. Consequently, IRS does not have the complete and reliable information it needs to effectively focus collection efforts on accounts with the greatest collection potential. This is critical given the fact that 87 percent of IRS' estimated unpaid assessments, including the

\$62 billion in federal taxes receivable, have little or no potential for collection.

Additionally, because IRS' systems are not integrated, they create high rates of error in taxpayers' accounts and, in some cases, create unnecessary taxpayer burden. This burden results in cost to both the taxpayer and IRS in resolving the errors caused by these system deficiencies. System weaknesses and the lack of adequate data also affect IRS' ability to identify delinquencies so it can target its compliance and enforcement initiatives. These deficiencies impede IRS' efforts to detect noncompliant taxpayers earlier, increasing the likelihood that such amounts, if and when detected, will yield little collection.

We have provided IRS a series of long- and short-term recommendations to assist it in addressing the serious financial management issues associated with federal taxes receivable and other unpaid assessments.<sup>20</sup> However, these issues and their implications continue to expose the federal government to significant loss of tax revenue, as discussed in Major Management Challenges and Program Risks: Department of the Treasury (GAO/OCG-99-14, January 1999).

---

<sup>20</sup>GAO/AIMD-99-16, October 30, 1998.

---

**Customs Service  
Financial  
Management  
High-Risk  
Designation  
Removed**

The U.S. Customs Service has demonstrated a consistent ability to develop and implement actions to address the problems that originally contributed to its designation as a high-risk area. In 1995, we began focusing on Customs' efforts to implement our recommendations to help promote better financial management, especially strengthening controls over assessing and collecting revenues. The Customs Service has made considerable progress in addressing its financial management weaknesses and has demonstrated its ability to receive unqualified audit opinions on its financial statements for the past 2 fiscal years—1996 and 1997. The Results Caucus commissioned by the House leadership has provided added attention to resolving problems in this and other high-risk areas.

Over the past several years, Customs has continually shown a commitment to improving its financial management and has implemented significant corrective actions. Such actions include

- statistically sampling compliance of commercial importations through ports of entry, which helps Customs to better focus its enforcement efforts and project the level of the trade community's noncompliance

with trade laws and the associated loss of revenue;

- programming the Automated Commercial System in fiscal year 1995 to identify any drawback claims<sup>21</sup> that exceeded the total amount of duty and tax paid on related import entries, which improved Customs' ability to detect and prevent any duplicate or excessive drawbacks; and
- aggressively pursuing collection of delinquent receivables, which has resulted in collections of over \$37 million.

In addition, Customs has several initiatives currently underway to further improve its controls over assessing and collecting revenues. For example, in September 1998, Customs began implementing a nationwide in-bond shipments Compliance Measurement Program which is intended to provide some assurance of compliance over in-bond shipments through random examinations of such items.<sup>22</sup> The program involved system changes for in-bond shipments, as well as adding compliance measurement inspections for randomly selected in-bond shipments. Additionally,

---

<sup>21</sup>Drawbacks are refunds of duties and taxes paid on imported goods that are subsequently exported or destroyed.

<sup>22</sup>In-bond shipment refers to goods authorized, by law, to move within the United States prior to release or export without appraisalment or classification.

according to Customs officials, Customs plans to implement a Compliance Measurement Program for foreign trade zones,<sup>23</sup> and is reviewing drawbacks and drawback claims for quality assurance.

Given the significant improvement efforts, including those related to assessing and collecting revenues, we are removing our high-risk designation for Customs financial management. However, Customs needs to continue to improve controls primarily related to accessing sensitive data maintained in its automated systems, maintaining complete and reliable information in its core financial systems, and addressing system architecture issues that hinder development of Customs' Automated Commercial Environment system. We will continue to monitor Customs' efforts to address these matters, which are further discussed in Major Management Challenges and Program Risks: Department of the Treasury (GAO/OCG-99-14, January 1999).

---

<sup>23</sup>Foreign trade zones are geographic areas, designated in accordance with the Foreign Trade Zone Act of 1934, as amended, where merchants may bring domestic or foreign merchandise for storage, exhibition, manipulation, manufacturing, assembly, or other processing, without subjecting it to formal Customs entry procedures and payment of duties. Foreign goods held in foreign trade zones are not assessed duties, taxes, and fees until the goods are released into the commerce of the United States.

---

# Reducing Inordinate Program Management Risks

---

Our work has identified several programs that need to be managed more effectively or that suffer from chronic waste and inefficiency. The high-risk areas we have identified span a range of government operations, including certain benefit programs that lose billions of dollars annually in improper payments, IRS' difficulty in controlling tax filing fraud, inefficient and weak lending programs, and the challenges DOD faces in reducing infrastructure costs. They also include HUD because of four serious, long-standing management deficiencies in internal controls, information and financial management systems, organizational structure, and staffing, which taken together, place the integrity and accountability of HUD's programs at risk. Effectively addressing the underlying causes of program management weaknesses offers tremendous opportunities to reduce government cost and improve services.

**High-Risk  
Program Management Areas**

- *Medicare*
- *Supplemental Security Income*
- *IRS Tax Filing Fraud*
- *DOD Infrastructure Management*
- *HUD Programs*
- *Student Financial Aid Programs*
- *Farm Loan Programs*
- *Asset Forfeiture Programs*
- *The 2000 Census*

---

**Medicare**

With annual payments totaling about \$200 billion and responsibility for financing health services delivered by hundreds of thousands of providers on behalf of tens of millions of beneficiaries, Medicare is inherently vulnerable to fraud, waste, and abuse. For example, the Department of Health and Human Services' (HHS) Health Care Financing Administration (HCFA) had not developed its own process for estimating the national error rate for fee-for-service payments. For fiscal year 1997, the HHS Inspector General estimated that about 11

percent of all Medicare fee-for-service payments for claims, or about \$20 billion, did not comply with Medicare laws and regulations.

While the Congress has given HHS new resources and authorities to improve oversight of Medicare, HCFA's deployment of these tools has lagged. Specifically:

- HCFA has been slow to distribute funding and implement new authority to help prevent fraud, abuse, and mispayments in the Medicare program. HCFA has not yet implemented a specialty contract for claims review or other program safeguard activities due to design issues. Furthermore, when implemented, the contract will likely have a more limited scope and provide fewer benefits than originally envisioned.<sup>1</sup>
- The implementation of new methods to determine provider payment—intended to curb rapid spending increases for certain services in the Medicare program—has stalled. HCFA needs to give first priority to year 2000 data systems changes. Other computer systems changes—such as those needed to implement new payment methods for home health services and outpatient

---

<sup>1</sup>Medicare: HCFA's Use of Anti-Fraud-and-Abuse Funding and Authorities (GAO/HEHS-98-160, June 1, 1998).

care—are on hold. In addition, the new methods being implemented to pay skilled nursing facilities have design flaws. These flaws, coupled with the use of unaudited cost data, may have led HCFA to set payment rates too high.<sup>2</sup>

- Implementation problems threaten the success of HCFA's Medicare+Choice program, which is designed to widen beneficiary and health plan participation in Medicare managed care. Medicare's payment rates may be overcompensating some plans and HCFA is having difficulty collecting the information needed to adjust those rates. HCFA's current financial oversight of managed care plans is inadequate. The Balanced Budget Act of 1997 required plan audits every 3 years to ensure that plans are not collecting excessive profits, but HCFA will not begin these audits until 2000. Moreover, HCFA is facing faltering plan participation and difficulties implementing its beneficiary information campaign.<sup>3</sup>
- Efforts to streamline the Medicare claims processing system have halted so that resources can be focused on critical Year

---

<sup>2</sup>Balanced Budget Act: Implementation of Key Medicare Mandates Must Evolve to Fulfill Congressional Objectives (GAO/T-HEHS-98-214, July 16, 1998).

<sup>3</sup>Medicare Managed Care: Payment Rates, Local Fee-for-Service Spending, and Other Factors Affect Plans' Benefit Packages (GAO/HEHS-99-9R, October 9, 1998).

2000 work. This has dealt a major setback to HCFA's attempt to increase the efficiency of its claims processing, better manage contractors, improve customer service, and help reduce fraud and abuse.<sup>4</sup>

Additional information on the challenges in maintaining Medicare program integrity are discussed in Major Management Challenges and Program Risks: Department of Health and Human Services (GAO/OCG-99-7, January 1999).

---

**Supplemental  
Security Income**

Since the Social Security Administration (SSA) assumed responsibility in 1974 for the Supplemental Security Income (SSI) program, SSA officials have been challenged to serve the diverse needs of program recipients while still protecting the program's overall financial health and integrity. Long-standing problems, such as program abuses and mismanagement, increasing SSI overpayments, and SSA's inability to recover outstanding SSI debt, have continued and have contributed to recent congressional criticism of SSA's ability to effectively manage this program and ensure program integrity.

---

<sup>4</sup>Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

---

## **Reducing Inordinate Program Management Risks**

---

During fiscal year 1998, for example, current and former recipients owed SSA more than \$3.3 billion, including \$1.2 billion in newly detected overpayments for the year. Based on prior experience, SSA is likely to collect less than 15 percent of the outstanding debt in a given year.

In September 1998, we reported that SSI's problems are attributable to two underlying causes: an organizational culture that places a greater priority on processing and paying claims than on controlling program expenditures and a management approach characterized by SSA's reluctance to fulfill its policy development and planning role in advance of major program crises.<sup>5</sup>

A recently issued SSI management report, in which SSA discussed the need to take aggressive action to improve overall payment accuracy, increase continuing disability reviews, combat program fraud, and improve debt collection, established goals to measure the anticipated yearly impact of its planned initiatives in each of these areas. The agency now intends to begin planning how it will implement these goals in day-to-day operations.

---

<sup>5</sup>Supplemental Security Income: Action Needed on Long-Standing Problems Affecting Program Integrity (GAO/HEHS-98-158, September 14, 1998).

To remove the SSI program from our high-risk list, however, SSA must produce and use research information on the program, be more responsive in suggesting legislative changes, and improve program policies. The agency should also continually search for ways to improve its payment controls and debt collection activities.

The SSI program's vulnerabilities and their root causes and solutions are discussed at greater length in Major Management Challenges and Program Risks: Social Security Administration (GAO/OCG-99-20, January 1999).

---

**IRS Tax Filing  
Fraud**

Filing fraud refers to the filing of fraudulent refund claims by taxpayers and/or tax return preparers. Since we first identified filing fraud as a high-risk area in February 1995, IRS has taken several steps in an attempt to reduce its exposure to filing fraud. For example, IRS has

- expanded the number of upfront filters in the electronic filing system designed to screen electronic submissions for problems, such as missing or incorrect Social Security numbers (SSN), to prevent returns with those problems from being filed electronically;

- strengthened the process for checking the suitability of persons applying to participate in the electronic filing program as return preparers or transmitters by requiring fingerprint and credit checks; and
- revised the computerized formulas used to score all tax returns as to their fraud potential, upgraded the Electronic Fraud Detection System to give staff in the Questionable Refund Program better research capabilities, and placed an increased emphasis on validating SSNs on filed paper returns.

A significant change in IRS' return processing procedures in 1997 significantly enhanced its ability to deal with paper returns involving missing or incorrect SSNs.<sup>6</sup> That year, as legislatively authorized, IRS began treating missing or incorrect SSNs as math errors, similar to the way it had historically handled computational errors. That meant that IRS could adjust refunds claimed by persons filing paper returns if required SSNs were missing or incorrect. Before 1997, IRS could not make adjustments to a refund involving a missing or incorrect SSN until it had gone through more time-consuming and labor-intensive examination procedures. As

---

<sup>6</sup>Tax Administration: IRS' 1997 Tax Filing Season (GAO/GGD-98-33, December 29, 1997).

we reported in 1996, those procedures limited the number of cases IRS could work and resulted in millions of questionable refunds being issued.

Most of the fraudulent refund claims identified by IRS involved the Earned Income Credit (EIC)—a refundable tax credit available to low-income, working taxpayers. In April 1997, IRS released the results of its study of EIC noncompliance on tax returns filed in 1995 (i.e., tax year 1994 returns). That study showed that of the \$17.2 billion in EIC claims on tax year 1994 returns, about \$4.4 billion (25.8 percent) was estimated to be overclaims. How much of this \$4.4 billion involved fraud, as opposed to less serious noncompliance, is unknown. The returns included in IRS' study were filed before IRS was given increased authority to deal with missing or invalid SSNS. Even after adjusting for the potential effect of that increased authority, however, IRS determined that the rate of EIC noncompliance would still be over 20 percent.

In response to IRS' findings, the Congress passed legislation that gave IRS (1) new enforcement tools and (2) additional funding specifically designated for EIC-related activities. With those new tools and funds,

IRS, in 1998, began implementing a 5-year EIC compliance initiative that involved several components directed at issues that were identified by IRS' study as major sources of EIC noncompliance. For example, IRS initiated enforcement efforts that focused on (1) cases where an EIC-qualifying child's SSN was used on more than one tax return for the same tax year and (2) returns filed by certain EIC claimants who claimed the head-of-household filing status. IRS also began a study of noncompliance among EIC claimants who report income from self-employment, increased staffing in the Questionable Refund Program, and issued procedures requiring tax return preparers to exercise due diligence in preparing returns involving EIC claims.

As we reported in July 1998, most of IRS' efforts under the EIC compliance initiative had not progressed far enough at the time we completed our audit work for us to judge their effectiveness.<sup>7</sup> To help assess the overall effectiveness of its efforts, IRS plans to do annual studies of EIC compliance starting with a baseline study of returns filed in 1998 (i.e., tax year 1997 returns), which is currently under way. Using the results of

---

<sup>7</sup>Earned Income Credit: IRS' Tax Year 1994 Compliance Study and Recent Efforts to Reduce Noncompliance (GAO/GGD-98-150, July 28, 1998).

that baseline study and subsequent years' studies, IRS plans to measure the rate of compliance and improvement in that rate over time. Those studies should eventually provide the necessary data to assess the impact of IRS' efforts on reducing the incidence of noncompliance associated with the EIC.

IRS tax filing fraud is among the management problems discussed in Major Management Challenges and Program Risks: Department of the Treasury (GAO/OCG-99-14, January 1999).

---

**DOD  
Infrastructure**

DOD has found that infrastructure reductions are difficult and painful because achieving significant cost savings requires up-front investments, the closure of installations, and the elimination of military and civilian jobs. DOD's ability to reduce infrastructure has been affected by service parochialism, a cultural resistance to change, and congressional and public concern about the effects and impartiality of decisions. For fiscal year 1998, DOD estimated that about \$147 billion, or 58 percent of its budget, would still be needed for infrastructure requirements, which included installation support, training, medical care, logistics,

force management, acquisition infrastructure, and personnel.

The Secretary of Defense's November 1997 Defense Reform Initiative (DRI) Report emphasizes the need to reduce excess Cold War infrastructure to free up resources for force modernization. Specific initiatives cited in the report included privatizing military housing and utility systems, emphasizing demolition of excess buildings, consolidating and regionalizing many defense support agencies, and requesting legislative authority to conduct two additional base realignment and closure rounds. Other initiatives include partnering with the private sector at depot maintenance activities and potentially other facilities to more efficiently use resources.

In responding to Section 2824 of the Fiscal Year 1998 Defense Authorization Act, DOD emphasized the problem of continuing excess infrastructure in its April 1998 report to the Congress concerning base realignment and closure issues. More recently, in our November 1998 report on Army industrial facilities, we noted the continuing existence of significant excess capacity in the Army's

maintenance depots and manufacturing arsenals.<sup>8</sup>

While the Defense reform initiatives are steps in the right direction and have brought high-level attention to the need for infrastructure reductions, collectively they do not provide a comprehensive long-range plan for facilities infrastructure. We have cited the need for such a plan but have noted that DOD's past plans were not focused on long-term comprehensive strategies for facilities revitalization, replacement, and maintenance and were not tied to measurable goals to be accomplished over specified time frames or linked to funding.

We have not completed an in-depth analysis of all the categories of infrastructure, but we have identified numerous areas in which infrastructure activities can be eliminated, streamlined, or reengineered to be made more efficient. Significant efficiencies could be achieved in the areas of acquisition infrastructure, central logistics, installation support, central training, force management, and medical facilities and services.

---

<sup>8</sup>Army Industrial Facilities: Workforce Requirements and Related Issues Affecting Depots and Arsenals (GAO/NSIAD-99-31, November 30, 1998).

Reducing DOD's infrastructure is among the management problems DOD faces and that are discussed in Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999).

---

## HUD Programs

The Department of Housing and Urban Development (HUD) (1) makes housing affordable by insuring loans for multifamily rental housing properties, (2) provides rental assistance for about 4.5 million lower-income residents, (3) helps revitalize over 4,000 localities through community development programs, and (4) encourages homeownership by providing mortgage insurance to about 7 million homeowners who might not have been able to qualify for nonfederally supported loans. HUD is one of the nation's largest financial institutions, with significant commitments, obligations, and exposure. As of September 30, 1997, HUD was responsible for managing about \$454 billion in insured mortgages and \$531 billion in guarantees of mortgage-backed securities, and, for fiscal year 1999, it has \$24.3 billion in budget authority.

We designated HUD as a high-risk area in 1994 because of four serious, long-standing

departmentwide management deficiencies and reported on these deficiencies and HUD's progress in resolving them in our 1995 and 1997 updates.<sup>9</sup> Taken together, these deficiencies placed the integrity and accountability of HUD's programs at high risk. Specifically, internal control weaknesses, such as a lack of necessary data and management processes, were a major factor leading to the HUD scandals of the late 1980s. Second, poorly integrated, ineffective, and generally unreliable information and financial management systems did not meet the needs of program managers and weakened their ability to provide management control over housing and community development programs. Third, HUD had organizational deficiencies, such as overlapping and ill-defined responsibilities and authorities between its headquarters and field organizations and a fundamental lack of management accountability and responsibility. Finally, an insufficient mix of staff with the proper skills hampered the effective monitoring and oversight of HUD's programs and the timely updating of procedures.

---

<sup>9</sup>High-Risk Series: Department of Housing and Urban Development (GAO/HR-95-11, February 1995 and GAO/HR-97-12, February 1997).

Resolving these management deficiencies is particularly critical for HUD because its housing and community development programs rely extensively on the integrity of thousands of diverse individuals and entities, such as cities, public housing authorities, mortgage lenders, contractors, and property owners, over whom it does not have direct control.

HUD continues to make credible progress in overhauling its operations to correct its management deficiencies. Among other things, HUD has

- improved its financial reporting and received qualified opinions from its Office of Inspector General on its fiscal years 1996 and 1997 financial statements following a report by the Office of Inspector General that it was unable to express an opinion on the reliability of its fiscal year 1995 financial statements;
- deployed components for improving its information and financial management systems;
- reorganized its resources by function and established various consolidated or centralized entities for single-family insurance operations, payment of rental assistance, assessments of HUD owned or

- supported rental properties, and enforcement activities; and
- refocused and begun retraining its workforce.

A major contributor to this progress is the June 1997 “HUD 2020 Management Reform Plan,” a set of proposals intended to, among other things, correct the management deficiencies that we and others (e.g., HUD’s Inspector General, external auditors) identified. The plan calls for reducing the number of programs, reducing staffing levels, retraining the majority of the staff and separating service from compliance functions, reorganizing the 81 field offices, consolidating processes and functions within and across program areas into specialized centers, and modernizing and integrating the financial and management information systems. In addition, HUD has linked its management reform efforts to the strategic and annual plans developed under the Government Performance and Results Act of 1993, so that its success in achieving strategic objectives and meeting annual performance goals depends on the success of these efforts.

We continue to believe, as we reported in 1995 and 1997, that these management

deficiencies, taken together, place the integrity and accountability of HUD's programs at high risk. To resolve these management deficiencies, the agency needs to ensure that the actions being taken eliminate the remaining major internal control weaknesses; strengthen the management and oversight of the efforts to integrate information and financial systems and correct systems' weaknesses; ensure that the field offices have enough staff to carry out the work assigned, including the monitoring of programs and activities and the assessment of outcomes; and ensure that all staff have the skills needed to perform their functions.

Given the severity of the management deficiencies that we and others have observed, it would not be realistic to expect that HUD would have substantially implemented its reform efforts and demonstrated success in resolving its management deficiencies in the 2 years since we issued our last report. Nevertheless, with close oversight by the Congress, HUD is making significant changes and has made credible progress since 1997 in laying the framework for improving its management. HUD's Secretary and leadership team have given top priority to addressing these

management deficiencies. This top management attention is critical and must be sustained in order to achieve real and lasting change. Importantly, given the nature and extent of the challenges facing the department, it will take time to implement and assess the impact of any related reforms. While major reforms are under way, several are in the early stages of implementation, and it is too soon to tell whether or not they will resolve the major deficiencies that we and others have identified. Therefore, in our opinion, the integrity and accountability of HUD's programs remain at high risk, as also presented in Major Management Challenges and Program Risks: Department of Housing and Urban Development (GAO/OCG-99-8, January 1999).

---

**Student Financial  
Aid Programs**

The Department of Education is responsible for more than \$150 billion in outstanding student loans, and its data systems track approximately 93 million student loans and 15 million grants. In fiscal year 1998, more than 8.5 million students received over \$48 billion in federal student financial aid through programs administered by the Department of Education.

These programs have a number of features that make them inherently vulnerable to waste, fraud, abuse, and mismanagement. For example, they provide grants and federally backed loans to high-risk population, much of which are low-income students who are not credit worthy and would not otherwise have access to the funds necessary to enter the college or university of their choice. The programs operate independently with different rules, processes, and data systems, and they have many participants including millions of students; thousands of schools; and thousands of lenders, guaranty agencies, third-party servicers, and contractors.

For example, the Federal Family Education Loan Program (formerly known as the Guaranteed Student Loan Program) is particularly vulnerable because of its size (\$20 billion in loans in fiscal year 1998) and large number of participants. In addition, the federal government bears most of the risk when students default on their loans. In fiscal year 1997, the federal government paid out over \$3.3 billion to make good its guarantee on defaulted student loans.

The department's administration of these programs has also contributed to federal

exposure to mismanagement and abuses. Audits by us and the department's Office of Inspector General have found instances in which students fraudulently obtained grants and loans, schools were inappropriately recertified to continue participating in federal student aid programs, and state-designated guaranty agencies misused federal funds in their custody.

Progress has been made on many of the issues contributing to this high-risk area. For example, in the 1998 amendments to title IV of the Higher Education Act of 1965, as amended, the Congress instructed Education and IRS to cooperate in verifying students' income to prevent fraud. The 1998 amendments also strengthened the controls over guaranty agencies' use of the federal funds they hold in reserve. The department has also improved the process by which it recertifies schools for participation in student aid programs and increased its management and oversight of the consolidation of student loans.<sup>10</sup>

The Congress and the department have taken actions to address a number of program management and oversight issues.

---

<sup>10</sup>Student Loans: Improvements in the Direct Loan Consolidation Process (GAO/HEHS-99-19R, November 10, 1998).

But Education continues to experience problems in its management of student financial aid programs. Education's information management systems often lack accurate, complete, and timely data for its managers to manage and oversee the student aid programs.<sup>11</sup> Also, the department lacks the financial information necessary to effectively budget for and manage its student aid programs or to accurately estimate the government's liabilities in a timely manner.

Additional detailed information on these matters can be found in Major Management Challenges and Program Risks: Department of Education (GAO/OCG-99-5, January 1999).

---

## Farm Loan Programs

The Department of Agriculture's (USDA) farm loan programs are intended to provide temporary financial assistance to farmers and ranchers who are unable to obtain commercial credit at reasonable rates and terms. In operating the farm loan programs, USDA faces the conflicting tasks of providing temporary credit to high-risk borrowers so they can stay in farming until they are able to secure commercial credit and of ensuring that the taxpayers' investment is protected.

---

<sup>11</sup>Student Financial Aid: Data Not Fully Utilized to Identify Inappropriately Awarded Loans and Grants (GAO/HEHS-95-89, July 11, 1995).

The unpaid principal on USDA's active direct farm loan portfolio totaled about \$9.7 billion at the end of fiscal year 1997.

In 1990, we placed USDA's farm loan programs on our high-risk list because the programs (1) had an exceptionally high rate of defaults and (2) had become a continual source of subsidized credit for nearly half of the borrowers under these programs. In 1996, the Congress made fundamental changes to the programs, such as prohibiting delinquent borrowers from obtaining direct operating loans and limiting the number of times delinquent borrowers can receive debt forgiveness. In our 1997 high-risk series, we reported that these changes, if implemented properly, would significantly reduce the financial risk associated with the farm lending programs.

In 1998, we reported that the value of farm loans held by delinquent borrowers decreased from a reported \$4.6 billion, or 40.7 percent, of USDA's total outstanding direct farm loan principal in 1995 to a reported \$2.7 billion, or 28.2 percent, in 1997.<sup>12</sup> Despite the indications of improvement in the farm loan portfolio's

---

<sup>12</sup>Farm Service Agency: Information on Farm Loans and Losses (GAO/RCED-99-18, November 27, 1998).

financial condition, the farm loan programs remain “high risk” for several reasons. First, USDA continues to carry a high level of delinquent debt and to write off large amounts of unpaid loans held by problem borrowers. Moreover, these delinquencies may increase because of the droughts and low prices for major crops and livestock in 1998. Second, the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999 (Public Law 105-277, October 21, 1998) eased some of the lending reforms initiated under the 1996 Farm Bill. For example, it expanded exceptions to the Farm Bill’s general prohibition against providing additional loans to borrowers who had prior loan losses. Finally, both we and USDA’s Inspector General have reported on continuing management problems with farm loan programs. For example, in May 1998, we reported that USDA still has problems in complying with some of its own loan servicing standards. Similarly, in December 1998, USDA’s Inspector General identified USDA’s farm loan programs as one of the department’s key problem areas and plans to expand its reviews of USDA’s loan-making and loan-servicing actions.

USDA and the Congress need to continue to monitor the effects of recent lending and

servicing reforms intended to improve the financial integrity of the farm loan programs. These matters are also presented in Major Management Challenges and Program Risks: Department of Agriculture (GAO/OCG-99-2, January 1999).

---

## **Asset Forfeiture Programs**

Since 1990, we have monitored the asset forfeiture programs operated by the Department of Justice and the Department of the Treasury.<sup>13</sup> Many improvements in property management have been made to these programs, which had assets totaling about \$1.8 billion as of September 30, 1997. For example, in 1998, we reviewed the U.S. Marshals Service's controls over certain seized property in four locations and found no material weaknesses or deficiencies in the controls we tested. Nevertheless, the programs continue to have significant weaknesses.

Justice has acknowledged that its asset forfeiture information systems had been inadequate for tracking the life cycle of an asset from its seizure through its ultimate

---

<sup>13</sup>High-Risk Program: Information on Selected High-Risk Areas (GAO/HR-97-30, May 16, 1997) and Asset Forfeiture: Historical Perspective on Asset Forfeiture Issues (GAO/T-GGD-96-40, March 19, 1996).

disposition.<sup>14</sup> In addition, auditors have found that controls were not operating effectively and timely oversight was not performed with respect to monitoring and reporting changes in seized/forfeited cash and property.<sup>15</sup>

Also, in September 1998, Justice's Inspector General reported that at most of the Immigration and Naturalization Service Border Patrol stations they visited, they found problems with the management of seized drugs.<sup>16</sup> For example, the Border Patrol (1) failed to store seized drugs in a secure manner, (2) lacked adherence to proper chain of custody procedures, and (3) did not always have an individual specifically designated as responsible for the evidence. These types of problems increase the risk of loss of seized drugs and contamination of evidence.

---

<sup>14</sup>Management Control Report: Department of Justice Report by the Attorney General on Management Controls 1997 (December 31, 1997).

<sup>15</sup>Audit Report: Asset Forfeiture Program Annual Financial Statement Fiscal Year 1997 (98-24), September 1998, prepared by the Department of Justice Office of Inspector General, Audit Division.

<sup>16</sup>Inspection Report: Border Patrol Drug Interdiction Activities on the Southwest Border (I-98-20), September 1998, prepared by the Department of Justice Office of Inspector General, Inspections Division.

Treasury and its auditors have also reported weaknesses in the accountability and reporting over seized and forfeited property. For instance, Treasury has reported material weaknesses related to seized property in its fiscal year 1997 Accountability Report.<sup>17</sup> Also, for fiscal year 1997, the Treasury Forfeiture Fund auditors have reported, among other weaknesses, that the Seized Assets and Case Tracking System did not contain accurate and sufficient data that could be relied upon to prepare the analysis of changes in forfeited and seized currency and property without substantial manual intervention and reconciliation.<sup>18</sup>

Justice and the Treasury continue to operate two similar but separate seized asset management and disposal programs without plans for consolidation despite legislation requiring them to develop a plan to consolidate postseizure administration of certain properties.<sup>19</sup> We have recommended consolidating the management and

---

<sup>17</sup>Department of the Treasury Accountability Report, Fiscal Year 1997 (March 1998).

<sup>18</sup>Audit Report: Treasury Forfeiture Fund, Audited Fiscal Years 1997 and 1996 Financial Statements (OIG-98-072), April 3, 1998, prepared by the Department of the Treasury Office of Inspector General.

<sup>19</sup>The Anti-Drug Abuse Act of 1988, Public Law No. 100-690, 21 U.S.C. 887 (1988).

disposition of all noncash seized property in order to reduce administration costs. We encourage both departments to pursue options for efficiency gains through program consolidation.

Asset forfeiture program issues are presented in Major Management Challenges and Program Risks: Department of Justice (GAO/OCG-99-10, January 1999) and Major Management Challenges and Program Risks: Department of the Treasury (GAO/OCG-99-14, January 1999).

---

## The 2000 Census

The decennial census is the nation's most comprehensive and expensive statistical data-gathering program. Accurate results are critical because, as required by the Constitution, decennial census data are used to reapportion seats in the House of Representatives and, thus, the allocation of political power in our democracy. Countless decisions affecting governments, businesses, and private citizens also depend on census data.

The Department of Commerce's Bureau of the Census has made progress in addressing some of the problems that occurred during the 1990 Census. Nevertheless, it still faces a

number of challenges and uncertainties in its efforts to conduct an accurate and cost-effective decennial census in 2000. For example, the Congress and the administration have yet to agree on the final design of the census because of congressional concerns over the legal and methodological issues surrounding the bureau's planned use of sampling and statistical estimation. In August and September 1998, federal courts ruled sampling illegal for purposes of apportionment in two separate cases.<sup>20</sup> The administration has appealed the rulings to the Supreme Court, and oral arguments were held on November 30, 1998.

Irrespective of how the controversy over the use of sampling and statistical estimation is resolved later this year, the bureau will have little time remaining to make final census design changes and implement those changes in time for the census in 2000. In that regard, our work has shown that the bureau faces a number of formidable challenges to a cost-effective, accurate, and complete census no matter which design is chosen. As we reported in our earlier work, they include the following: Mail response

---

<sup>20</sup>U.S. House of Representatives v. U.S. Department of Commerce, 11 F.Supp. 2d 76 (D.D.C. 1998) and Glavin v. Clinton, 19 F. Supp. 2d 543 (E.D. Va. 1998).

rates remain problematic, scanning equipment used to electronically record responses from census questionnaires experienced system crashes due to software flaws, and local partnerships—a key component of the bureau’s outreach and promotion strategy—had limited success.<sup>21</sup> Further, demographic, attitudinal, and other factors that adversely affected the cost and accuracy of the 1990 Census, such as concerns over privacy, may present an even greater challenge for the bureau in 2000.

These major challenges and uncertainties have led us to conclude that there is a high risk that the 2000 Census will be less accurate and more costly than previous censuses. Although it may be too late in the census cycle to substantively redesign key census-taking operations, our work suggests that at least two actions could help mitigate the risk of an unsuccessful census.

- To help ensure that key census-taking activities are operationally feasible, the bureau should ensure that its evaluation of the dress rehearsal is based on rigorous

---

<sup>21</sup>See for example, 2000 Census: Preparations for Dress Rehearsal Leave Many Unanswered Questions (GAO/GGD-98-74, March 26, 1998) and Decennial Census: Preliminary Observations on the Results to Date of the Dress Rehearsal and the Census Bureau’s Readiness for 2000 (GAO/T-GGD-98-178, July 30, 1998).

analysis and is issued promptly. Moreover, the bureau should ensure that the results are used to refine operations, help set priorities, and allocate resources as the bureau enters the final preparations for the 2000 Census.

- Consistent with our past recommendation, to alleviate congressional concerns over the design of the census, particularly its planned use of statistical sampling and estimation, the bureau should provide the Congress and other stakeholders detailed data on the expected effects of the bureau's planned initiatives on costs, accuracy, and other variables.

Further information on the 2000 Census is presented in Major Management Challenges and Program Risks: Department of Commerce (GAO/OCG-99-3, January 1999).

---

# Managing Large Procurement Operations More Efficiently

---

The federal government procures tens of billions of dollars annually in goods and services ranging from huge defense weapon systems and space exploration equipment to supplies and materials supporting operating forces around the world. Our work has shown that some of the government's largest procurement operations are not always run efficiently, and we have recommended ways to operate them better.

The federal government's reliance on the private sector as a means to carry out programs through contracts can reduce the workforce. However, it is critical that the government gets what it pays for under these contracts and that the contractors' work is done at reasonable cost. The effective oversight of contracts and control of contractor operations is essential in order to achieve these objectives.

**High-Risk  
Procurement Operations**

- *DOD Inventory Management*
- *DOD Weapon Systems Acquisition*
- *DOD Contract Management*
- *Department of Energy Contract Management*
- *Superfund Contract Management*
- *NASA Contract Management*

---

**DOD Inventory  
Management**

DOD has had inventory management problems for decades. In 1990, we identified DOD's management of secondary inventories (spare and repair parts, clothing, medical supplies, and other items to support the operating forces) as a high-risk area because levels of inventory were too high and management systems and procedures were ineffective. While some improvements have been made, these general conditions still exist.

- In 1995, we reported that DOD's strategic plans for logistics called for improving asset visibility in such areas as in-transit assets,

retail-level stocks, and automated systems. DOD will not completely implement its current plan until 2004. The lack of adequate visibility over operating materials and supplies substantially increases the risk that millions of dollars will be spent unnecessarily. For example, the Navy's fiscal year 1996 financial statements did not include information on \$7.8 billion in inventories onboard ships and at Marine Corps activities.

- DOD has not taken sufficient steps to ensure the accuracy of inventory requirements to preclude the acquisition of unneeded items. For example, in April 1998, we reported that the Navy could have eliminated about \$13 million of planned program requirements for 68 of 200 items reviewed because the requirements were also included in the reorder-level requirement. While we could not precisely quantify the overall extent of the problem, this double counting could be indicative of a larger problem because the Navy has a total of about \$3.3 billion of planned program requirements that affect purchase decisions.<sup>1</sup>
- In February 1998, we reported that DOD did not have receipts for about 60 percent of its 21 million shipments to end users in fiscal

---

<sup>1</sup>Navy Inventory Management: Improvements Needed to Prevent Excess Purchases (GAO/NSIAD-98-86, April 30, 1998).

year 1997. Later work showed that over the last 3 years, the Navy alone reportedly wrote off as lost over \$3 billion in in-transit inventory.

- The vulnerability to waste, fraud, and abuse also extends to DOD's disposal of surplus property. In October 1997, we reported that DOD destroyed and sold as scrap some usable aircraft parts in new or repairable condition that possibly could have been sold intact at higher than scrap prices. In contrast, in August 1998, we reported that DOD inadvertently sold surplus parts with military technology intact. In these cases, management controls were insufficient to preclude these conditions.<sup>2</sup>

Since 1991, we have issued 11 reports that identify significant opportunities for DOD to test and adopt, where feasible, best inventory management practices used in the private sector to improve logistics operations and lower costs. Recently, the Congress enacted legislation requiring the Defense Logistics Agency and the services to develop and submit schedules for implementing best commercial practices in its acquisition and distribution of inventory items. The legislation calls for the

---

<sup>2</sup>Defense Inventory: Action Needed to Avoid Inappropriate Sales of Surplus Parts (GAO/NSIAD-98-182, August 3, 1998).

implementation of best practice initiatives to be completed within the next 3 years in the case of the Defense Logistics Agency and 5 years for the services. In November 1997, the Secretary of Defense announced the Defense Reform Initiative, which seeks to reengineer DOD support activities and business practices by incorporating many business practices that private sector companies have used.

In the short term, DOD still needs to emphasize the efficient operation of its existing inventory systems. In the long term, DOD must establish goals, objectives, and milestones for changing its culture and adopting new management tools and practices. Unless DOD takes more aggressive actions to correct systemic problems, its inventory management problems will continue well into the next century.

Our report, Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999), further highlights DOD's inventory management problems.

---

**Weapon Systems  
Acquisition**

DOD spends about \$85 billion annually to research, develop, and acquire weapon systems. Although DOD has many acquisition

reform initiatives in process, pervasive problems persist regarding (1) questionable requirements and solutions that are not the most cost-effective available, (2) unrealistic cost, schedule, and performance estimates, (3) questionable program affordability, and (4) the use of high-risk acquisition strategies.

We have found that while the services conduct considerable analyses in justifying major acquisitions, these analyses can be narrowly focused, without full consideration of alternative solutions, including the joint acquisition of systems with the other services. In addition, because DOD does not routinely develop information on joint mission needs and aggregate capabilities, it has little assurance that decisions to buy, modify, or retire systems are sound. For example

- DOD could have met its strategic airlift requirements and achieved a significant life-cycle cost savings by buying fewer C-17s than planned and
- by increasing the total annual buy of Blackhawk helicopter derivatives for Marine Corps and other requirements, DOD could save over \$700 million in research and development and procurement costs.

Further, we continue to report on examples where program projections appear to be overly optimistic and risks excessive in light of the current budget and security environment. For example, it is doubtful that in restructuring the F-22 program, the Air Force can offset the \$13 billion projected increase in production costs because many of the cost-cutting initiatives it identified were not well defined.<sup>3</sup>

Additionally, each year for the past several years, we have reported that DOD's Future Years Defense Program could not be executed with available funds. We concluded that DOD's tendency to overestimate the funding that would be available in the future, coupled with the tendency to underestimate program costs, had resulted in the advent of more programs than could be executed as planned. We continue to find and report on numerous problems with DOD's budgeting and spending practices for weapon system acquisitions. For example, in analyzing the 1998 Future Years Defense Program, we found that funding for infrastructure activities was projected to increase while procurement funding was projected to be

---

<sup>3</sup>Tactical Aircraft: Restructuring of the Air Force F-22 Fighter Program (GAO/NSIAD-97-156, June 4, 1997).

lower than anticipated. Nonetheless, DOD is pursuing a number of major system acquisition programs on the assumption that infrastructure savings will materialize.<sup>4</sup>

We have also reported on the high-risk practice of beginning production of a weapon system before development, testing, and evaluation are complete. DOD still begins production of many major and nonmajor weapons without first providing that the systems will meet critical performance requirements. For example, DOD's approval of the Joint Surveillance Target Attack Radar System's (JSTARS) full rate production was premature and risky because the system's operational effectiveness and suitability for combat were not yet demonstrated and plans to address deficiencies and reduce program costs were not completed. In another case, the plan to develop and deploy a National Missile Defense system in only 6 years is fraught with risks, including possible schedule slippages and technical problems stemming from limited testing.

DOD continues to implement a variety of acquisition reform initiatives and is reporting some success in terms of cost savings or

---

<sup>4</sup>Future Years Defense Program: Substantial Risks Remain in DOD's 1999-2003 Plan (GAO/NSIAD-98-204, July 31, 1998).

avoidance and other benefits. We support DOD's efforts to reform its acquisition processes. However, we have concerns about the extent to which cost reductions from acquisition reform will be available to fund DOD's modernization program in the near term. We have reported that a large portion of the estimated cost reductions already identified has been used to meet needs within programs generating the reductions or has been offset by cost increases elsewhere in the programs.<sup>5</sup> The need for such offsets is partly due to optimistic planning. Such planning provides an unclear picture of defense priorities because tough decisions and trade-offs are avoided. In order for DOD to have an efficient and effective program and for the Congress to properly exercise its oversight responsibilities, it is critical that DOD present realistic assumptions and plans in its future budgets.

DOD and the Congress need to take much stronger actions to effectively control the lure of optimistic planning, particularly as DOD (1) generates and supports the acquisition of new weapon systems that do not necessarily satisfy the most critical

---

<sup>5</sup>Acquisition Reform: Effect on Weapon System Funding (GAO/NSIAD-98-31, October 29, 1997).

weapon requirements at minimal cost and (2) commits more procurement funds to programs than can reasonably be expected to be available in future defense budgets. Although many recommendations from a variety of sources have addressed these long-standing issues, DOD has taken little or no effective action on them.

Acquisition reforms and commercial practices can produce better outcomes on DOD acquisitions when they help a program succeed in its environment. Thus, the way to get lasting reform is to realign the incentives of the weapon acquisition process with desired program outcomes. Changing these incentives—that is, redefining program success—will take the efforts of the Congress as well as DOD and the services.

The issues involving DOD's weapon systems acquisition are also included in Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999).

---

**DOD Contract  
Management**

DOD spends in excess of \$100 billion a year contracting for goods and services. Over the last few years, several broad-based changes have been made to DOD contracting

processes to improve the way DOD relates to its contractors and the rules governing their relationships. These changes are by no means complete. Acquisition reform, with its emphasis on widespread reengineering of fundamental processes, continues to receive attention at the highest levels in DOD. DOD faces a number of areas where risks appear particularly acute.

- The need for DOD to achieve effective control over its payment process remains an imperative. If it does not, DOD continues to risk erroneously paying contractors millions of dollars and perpetuating other financial management and accounting control problems. Weak systems and controls also leave DOD vulnerable to fraud and improper payment.<sup>6</sup> A demonstration program to evaluate the feasibility of using private contractors to identify overpayments made to vendors has identified about \$19 million in overpayments.<sup>7</sup> While DOD is taking steps to improve its payment process and controls, it will likely take an extended period to get its payment problems under control.

---

<sup>6</sup>Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

<sup>7</sup>Contract Management: Recovery Auditing Offers Potential to Identify Overpayments (GAO/NSIAD-99-12, December 3, 1998).

- We and the DOD Inspector General have found that DOD needs to strengthen the quality of its analyses for commercial purchases. The Inspector General found that DOD had not formulated good procurement and management strategies for commercial parts in the acquisition reform environment. As a result, DOD was paying higher prices for commercial spare parts than necessary. Our work also identified cases in which limited analysis of commercially offered prices resulted in significantly higher prices than previously paid.<sup>8</sup> DOD is taking steps to improve its workforce training in commercial buying and pricing.
- DOD's implementation of health care management programs, particularly the TRICARE Program, further illustrates DOD's difficulty in managing contracts. TRICARE's implementation, entailing the award of seven competitively bid, 5-year contracts, has been fraught with problems. All seven contracts, totaling about \$15 billion, were protested. As a result, DOD and the competitors incurred added costs, and the program was significantly delayed. Three of the protests were sustained, resulting in further delays. We also identified problems with the change order process, including the protracted

---

<sup>8</sup>Defense Acquisitions: Improved Program Outcomes Are Possible (GAO/T-NSIAD-98-123, March 18, 1998).

settlement of the orders. As of November 1998, over 350 change orders to the TRICARE contracts had not been settled. DOD has set out to develop and introduce a more simplified procurement approach. Whether DOD can successfully develop and launch the new method, and whether what it designs will reduce the current volume of contract changes or control health care costs, remains to be seen.<sup>9</sup>

See Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999) for additional information related to DOD contract management weaknesses.

---

## Department of Energy Contract Management

The Department of Energy (DOE) is the largest civilian contracting agency in the federal government. In fiscal year 1997, it obligated about \$16.2 billion, or about 91 percent of its obligations, to contracts. We have reported on weaknesses in DOE's contracting practices, including noncompetitive awards and lax oversight of costs and activities.

---

<sup>9</sup>Defense Health Care: Operational Difficulties and System Uncertainties Pose Continuing Challenges for TRICARE (GAO/T-HEHS-98-100, February 26, 1998).

In 1990, we designated DOE's contracting as a high-risk area. Three years later, the Secretary of Energy established a Contract Reform Team, which reviewed DOE's contracting practices and, in February 1994, published a report with 48 recommendations to make contracting work better and cost less. Among these were recommendations to award contracts competitively, incorporate performance-based incentives, and increase the use of fixed-price contracts. While DOE was reviewing its contracting practices, it was also developing its strategic plans. Together, the contract reform and strategic planning initiatives helped to shape the framework for contract reform that DOE has since put in place. While these reforms are generally steps in the right direction, DOE has had some problems in implementing them, and, in some instances, their effectiveness will not be known for several years.

For example, since 1996, DOE has increased its use of competition in awarding contracts for managing and operating its facilities, but it could do more, particularly at its national laboratories. For fiscal year 1996 through fiscal year 1998, DOE reported that it had awarded 14 of 26 such contracts (54 percent) competitively and extended the other 12 noncompetitively. However, as we reported

in 1996, only about half of the funds spent by management and operating contractors at the national laboratories went for research and development; the remainder went for other work, such as environmental restoration. At other facilities, DOE awards contracts for environmental restoration work competitively. In our view, DOE could improve its contacts with the national laboratories by separating and competitively awarding the portion of the work that is not related to research.<sup>10</sup>

In 1994, DOE began incorporating performance-based incentives in its management and operating contracts to better link contractor's fees to the satisfactory accomplishment of specific tasks. In 1997 and 1998, DOE's Inspector General found problems in the department's implementation of these incentives, and, in 1997, a departmentwide assessment identified other concerns, such as limited guidance on developing and administering the incentives. Our July 1998 report indicated that DOE had taken steps to correct these problems, including issuing guidance, conducting training, and incorporating lessons learned into the fiscal year 1998

---

<sup>10</sup>Department of Energy: Contract Reform Is Progressing, but Full Implementation Will Take Years (GAO/RCED-97-18, December 10, 1996).

incentives. However, it was too early to assess the effectiveness of these incentives because DOE's technical, financial, and contracting personnel had not yet completed their reviews.<sup>11</sup>

To control costs and shift risks from the government to contractors, DOE has begun to use fixed-price contracts for environmental cleanups in place of the cost-reimbursement contracts that the department routinely used in the past. Under this "privatization" initiative, DOE planned to pay its contractors a fixed amount for acceptable goods and services, regardless of the costs they incurred, and shift most financial risks to the contractors. While DOE has used fixed-price contracts for some well-defined projects, such as cleaning up some contaminated soils and decontaminating workers' uniforms, it has not met its initial goals for more complex environmental cleanups.<sup>12</sup> For example:

- Pit 9, a project to clean up radioactive wastes at the Idaho National Engineering and Environmental Laboratory, incurred

---

<sup>11</sup>Department of Energy: Lessons Learned Incorporated Into Performance-Based Incentive Contracts (GAO/RCED-98-223, July 29, 1998).

<sup>12</sup>Department of Energy: Alternative Financing and Contracting Strategies for Cleanup Projects (GAO/RCED-98-169, May 29, 1998).

nearly \$200 million in cost overruns. The project, which we characterized as a failure, was at least 26 months behind schedule when we reported on it in July 1997. Issues surrounding the project, such as the type and amount of waste to be cleaned up and who will pay for the increased costs, are currently in litigation.<sup>13</sup>

- At the Hanford site in Richland, Washington, DOE planned to make the contractor fully responsible for the financial risk associated with constructing a facility to treat highly radioactive waste, currently stored in leaking underground tanks. However, because lenders told DOE that the contractor would not be able to obtain affordable financing without government backing, DOE agreed to pay much of the project debt if the contractor defaulted on its loans. The extent of the liability retained by the contractor remains uncertain. While this financial approach appears reasonable for this project, DOE faces a financial risk not initially contemplated that could be in the billions of dollars.<sup>14</sup>

---

<sup>13</sup>Nuclear Waste: Department of Energy's Project to Clean Up Pit 9 at Idaho Falls Is Experiencing Problems (GAO/RCED-97-180, July 28, 1997).

<sup>14</sup>Nuclear Waste: Department of Energy's Hanford Tank Waste Project—Schedule, Cost, and Management Issues (GAO/RCED-99-13, October 8, 1998).

These practices increase the government's costs and expose DOE to billions of dollars of financial risk. Information about these risks is presented in Major Management Challenges and Program Risks: Department of Energy (GAO/OCG-99-6, January 1999).

---

**Superfund  
Contract  
Management**

The Environmental Protection Agency (EPA) has had long-standing challenges with controlling the costs of the contractors it uses to clean up sites or to monitor private party cleanups for EPA. In the past, we found that EPA (1) relied too heavily on the contractors' own cost proposals to determine the final price for cleanup activities performed by the contractors, (2) had made little progress in improving the timeliness of contractor audits, increasing the risk for fraud, waste, and abuse by contractors, and (3) continued to pay contractors a high rate to cover their administrative support costs. Since then, EPA has increased its use of independent government cost estimates to set better contract prices for the government, but some estimates are still of questionable quality. In addition, according to EPA officials, the agency has improved the timeliness of contractor audits and has

almost eliminated the backlog of these audits. However, program support costs remain high.

In our previous reviews of these issues, we found that EPA was not preparing independent cost estimates and that most of the final prices awarded for work closely matched the contractor's—not EPA's—estimate. In our ongoing work, we found that EPA has made substantial improvements in these areas. Of the 35 contractor work assignments that we reviewed in three of EPA's regions, the agency generated independent cost estimates for each of them. Furthermore, in about half of the cases, the final price awarded for the work closely matched EPA's independent cost estimate, which, according to EPA's criteria, suggests that the estimates were fairly accurate.

However, additional improvements are needed. In nearly half of the cases, the final price varied significantly from the cost estimates. The final prices were below the estimates in 5 cases by as much as 36 percent, and were higher than the estimates in 12 cases by as much as 101 percent. EPA estimators often left critical work steps out of their estimates, and about

half of EPA's program contract management staff for these cases questioned their own ability to generate accurate estimates because of their lack of experience and historical data on actual cleanup costs as a reference point for their estimates. EPA acknowledges these problems and has designed a set of corrective measures to address them. As of November 1998, the agency was in the first steps of implementing these measures—assessing each region's cost-estimating practices.

EPA continues to experience high program support costs related to contractors. In our ongoing review of these Superfund program management issues, we found that the program support costs for 9 of 13 contracts exceeded EPA's goal of 11 percent. Program support costs ranged from 19 to 92 percent when we included initial contract start-up costs, such as setting up local offices and designing computer programs to accommodate EPA's financial reporting requirements. The costs of the remaining four contracts ranged from about 6 to 10 percent. A major reason for continued high support costs is that EPA has more contract capacity in place than work available for the contractors, even though

the agency has significantly reduced the number of new contracts.

These continuing concerns suggest that EPA may need to evaluate whether it needs to overhaul some of its contracting practices. Superfund contract management problems are discussed in Major Management Challenges and Program Risks: Environmental Protection Agency (GAO/OCG-99-17, January 1999).

---

## **NASA Contract Management**

NASA now spends over \$12 billion annually for goods and services, mostly on contracts with businesses and other organizations. In 1990, we identified NASA's contract management as an area at high risk. In 1992, we reported that the agency had ineffective systems and processes for overseeing contractors' activities and that NASA field centers had failed to comply with contract management requirements.

In July 1998, we reported that NASA was developing systems to provide it with the oversight and information needed to improve its contract management.<sup>15</sup> However, we found the following.

---

<sup>15</sup>NASA Procurement: Status of Efforts to Improve Oversight (GAO/NSIAD-98-198R, July 13, 1998).

- NASA had delayed agencywide implementation of its integrated financial management system from July 1, 1999, to June 1, 2000. The system, which is intended to fix problems associated with NASA's nonstandard, nonintegrated systems, offers the promise of providing reliable and timely information—such as the status of procurement requests and contracts.
- NASA had not implemented its new system for measuring procurement performance. In March 1997, we reported on NASA's need to produce accurate and reliable procurement-related information.<sup>16</sup> NASA had started a procurement quality assessment initiative involving the development of measurable performance metrics, the benchmarking of these metrics, and the development of procurement customer surveys. This initiative is intended to provide information to help procurement managers measure and improve the performance of their organizations.
- NASA had not yet completed an initiative to evaluate its field centers' procurement activities based on international quality standards and its own procurement surveys. NASA's procurement evaluations will include (1) external evaluations of NASA field centers'

---

<sup>16</sup>NASA Procurement: Contract Management Oversight (GAO/NSIAD-97-114R, March 18, 1997).

compliance with quality contract management standards and (2) internal surveys of the centers' procurement management activities.

Since the July report, NASA has made progress in correcting weaknesses in contract management. NASA is currently implementing its new system for measuring procurement performance. By the end of fiscal year 1999, NASA plans for all field centers to be certified that their procurement activities meet the international quality standards. On September 30, 1998, NASA issued guidance to the centers' procurement officers for internal semiannual random procurement surveys.

However, a critical component of evaluating NASA's ability to manage contacts is the establishment of a financial management system and its integration with full cost accounting. Until the financial management system is developed and operational, performance assessments relying on cost data may be incomplete. Because implementation of the financial management system has been delayed, we believe that NASA's contract management should remain a high-risk area. The current status of NASA's

---

**Managing Large Procurement  
Operations More Efficiently**

---

efforts to improve contract management is highlighted in Major Management Challenges and Program Risks: National Aeronautics and Space Administration (GAO/OCG-99-18, January 1999).

---

# Chronology of High-Risk Designations

---

## 1999 HIGH-RISK AREAS AND THE YEAR THEY WERE DESIGNATED HIGH RISK

**Addressing Urgent Year 2000 Computing Challenge**      *1997*

**Resolving Serious Information Security Weaknesses**      *1997*

**Ensuring Major Technology Investments Improve  
Services**

- *Air Traffic Control Modernization*      *1995*
- *Tax Systems Modernization*      *1995*
- *National Weather Service Modernization*      *1995*
- *DOD Systems Development and  
Modernization Efforts*      *1995*

**Providing Basic Financial Accountability**

- *DOD Financial Management*      *1995*
- *Forest Service Financial Management*      *1999*
- *FAA Financial Management*      *1999*
- *IRS Financial Management*      *1995*
- *IRS Receivables*      *1990*

---

**Appendix I  
Chronology of High-Risk Designations**

---

**1999 HIGH-RISK AREAS AND THE YEAR THEY WERE DESIGNATED  
HIGH RISK (Continued)**

**Reducing Inordinate Program Management Risks**

- *Medicare* 1990
- *Supplemental Security Income* 1997
- *IRS Tax Filing Fraud* 1995
- *DOD Infrastructure Management* 1997
- *HUD Programs* 1994
- *Student Financial Aid Programs* 1990
- *Farm Loan Programs* 1990
- *Asset Forfeiture Programs* 1990
- *The 2000 Census* 1997

**Managing Large Procurement Operations More  
Efficiently**

- *DOD Inventory Management* 1990
- *DOD Weapon Systems Acquisition* 1990
- *DOD Contract Management* 1992
- *Department of Energy Contract Management* 1990
- *Superfund Contract Management* 1990
- *NASA Contract Management* 1990

---

**Appendix I  
Chronology of High-Risk Designations**

---

**HIGH-RISK DESIGNATIONS REMOVED**

<u>High-Risk Area</u>	<u>Year Added</u>	<u>Year Removed</u>
• <i>Pension Benefit Guaranty Corporation</i>	<i>1990</i>	<i>1995</i>
• <i>State Department Management of Overseas Real Property</i>	<i>1990</i>	<i>1995</i>
• <i>Federal Transit Administration Grant Management</i>	<i>1990</i>	<i>1995</i>
• <i>Bank Insurance Fund</i>	<i>1991</i>	<i>1995</i>
• <i>Resolution Trust Corporation</i>	<i>1990</i>	<i>1995</i>
• <i>Customs Service Financial Management<sup>1</sup></i>	<i>1991</i>	<i>1999</i>

<sup>1</sup>*Originally part of a broader high-risk area designated as Managing the Customs Service.*

---

# Key Contacts for High-Risk Areas

---

Addressing  
Urgent Year 2000  
Computing  
Challenge

Joel C. Willemsen, Director  
Civil Agencies Information Systems  
Accounting and Information Management  
Division  
(202) 512-6408  
willemsenj.aimd@gao.gov

---

Resolving Serious  
Information  
Security  
Weaknesses

Jack L. Brock, Jr., Director  
Governmentwide and Defense Information  
Systems  
Accounting and Information Management  
Division  
(202) 512-6240  
brockj.aimd@gao.gov

---

Air Traffic  
Control  
Modernization

Joel C. Willemsen, Director  
Civil Agencies Information Systems  
Accounting and Information Management  
Division  
(202) 512-6408  
willemsenj.aimd@gao.gov

John H. Anderson, Director  
Transportation Issues  
Resources, Community, and Economic  
Development Division  
(202) 512-2834  
andersonj.rced@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**Tax Systems  
Modernization**

Jack L. Brock, Jr., Director  
Governmentwide and Defense Information  
Systems  
Accounting and Information Management  
Division  
(202) 512-6240  
brockj.aimd@gao.gov

---

**National Weather  
Service  
Modernization**

Joel C. Willemsen, Director  
Civil Agencies Information Systems  
Accounting and Information Management  
Division  
(202) 512-6408  
willemsenj.aimd@gao.gov

---

**DOD Systems  
Development and  
Modernization  
Efforts**

Jack L. Brock, Jr., Director  
Governmentwide and Defense Information  
Systems  
Accounting and Information Management  
Division  
(202) 512-6240  
brockj.aimd@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**DOD Financial  
Management**

Lisa G. Jacobson, Director  
Defense Audits  
Accounting and Information Management  
Division  
(202) 512-9095  
jacobsonl.aimd@gao.gov

---

**Forest Service  
Financial  
Management**

Linda M. Calbom, Director  
Resources, Community, and Economic  
Development Accounting and  
Financial Management Issues  
Accounting and Information Management  
Division  
(202) 512-9508  
calboml.aimd@gao.gov

---

**FAA Financial  
Management**

Linda M. Calbom, Director  
Resources, Community, and Economic  
Development Accounting and  
Financial Management Issues  
Accounting and Information Management  
Division  
(202) 512-9508  
calboml.aimd@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**IRS Financial  
Management**

Gregory D. Kutz, Associate Director  
Governmentwide Accounting and Financial  
Management Issues  
Accounting and Information Management  
Division  
(202) 512-9505  
kutzg.aimd@gao.gov

---

**IRS Receivables**

James R. White, Director  
Tax Policy and Administration Issues  
General Government Division  
(202) 512-9110  
whitej.ggd@gao.gov

Gregory D. Kutz, Associate Director  
Governmentwide Accounting and Financial  
Management Issues  
Accounting and Information Management  
Division  
(202) 512-9505  
kutzg.aimd@gao.gov

---

**Medicare**

William J. Scanlon, Director  
Health Financing and Systems Issues  
Health, Education, and Human Services  
Division  
(202) 512-7114  
scanlonw.hehs@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**Supplemental  
Security Income**

Cynthia M. Fagnoni, Director  
Income Security Issues  
Health, Education, and Human Services  
Division  
(202) 512-7215  
fagnonic.hehs@gao.gov

---

**IRS Tax Filing  
Fraud**

James R. White, Director  
Tax Policy and Administration Issues  
General Government Division  
(202) 512-9110  
whitej.ggd@gao.gov

---

**Defense  
Infrastructure  
Management**

David R. Warren, Director  
Defense Management Issues  
National Security and International Affairs  
Division  
(202) 512-8412  
warrend.nsiad@gao.gov

---

**HUD Programs**

Judy A. England-Joseph, Director  
Housing and Community Development Issues  
Resources, Community, and Economic  
Development Division  
(202) 512-7631  
englandjosephj.rced@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**Student Financial  
Aid Programs**

Carlotta C. Joyner, Director  
Education and Employment Issues  
Health, Education, and Human Services  
Division  
(202) 512-7014  
joynerc.hehs@gao.gov

---

**Farm Loan  
Programs**

Larry Dyckman, Director  
Food and Agriculture Issues  
Resources, Community, and Economic  
Development Division  
(202) 512-5138  
dyckmanl.rced@gao.gov

---

**Asset Forfeiture  
Programs**

Norman J. Rabkin, Director  
Administration of Justice Issues  
General Government Division  
(202) 512-8777  
rabkinn.ggd@gao.gov

---

**The 2000 Census**

J. Christopher Mihm, Associate Director  
Federal Management and Workforce Issues  
General Government Division  
(202) 512-8676  
mihmj.ggd@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**DOD Inventory  
Management**

David R. Warren, Director  
Defense Management Issues  
National Security and International Affairs  
Division  
(202) 512-8412  
warrend.nsiad@gao.gov

---

**DOD Weapon  
Systems  
Acquisition**

Louis J. Rodrigues, Director  
Defense Acquisition Issues  
National Security and International Affairs  
Division  
(202) 512-4841  
rodriguesl.nsiad@gao.gov

---

**DOD Contract  
Management**

Louis J. Rodrigues, Director  
Defense Acquisition Issues  
National Security and International Affairs  
Division  
(202) 512-4841  
rodriguesl.nsiad@gao.gov

---

**Department of  
Energy Contract  
Management**

Victor S. Rezendes, Director  
Energy, Resources, and Science Issues  
Resources, Community, and Economic  
Development Division  
(202) 512-3841  
rezendesv.rced@gao.gov

---

**Appendix II**  
**Key Contacts for High-Risk Areas**

---

**Superfund  
Contract  
Management**

Peter F. Guerrero, Director  
Environmental Protection Issues  
Resources, Community, and Economic  
Development Division  
(202) 512-6111  
guerrerop.rced@gao.gov

---

**NASA Contract  
Management**

Louis J. Rodrigues, Director  
Defense Acquisition Issues  
National Security and International Affairs  
Division  
(202) 512-4841  
rodriguesl.nsiad@gao.gov

Allen Li, Associate Director  
Defense Acquisition Issues  
National Security and International Affairs  
Division  
(202) 512-4841  
lia.nsiad@gao.gov

---

**Overall GAO  
High-Risk  
Program**

George H. Stalcup, Associate Director  
Defense Audits  
Accounting and Information Management  
Division  
(202) 512-9095  
stalcupg.aimd@gao.gov

---

## **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 & 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](mailto:info@www.gao.gov)**

**or visit GAO's World Wide Web Home Page at:  
<http://www.gao.gov>**

---

-

---