United States General Accounting Office

GAO

High-Risk Series

February 1997

Information Management and Technology

GAO/HR-97-9

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

Comptroller General
of the United States

February 1997

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

In 1990, the General Accounting Office began a special effort to review and report on the federal program areas its work identified as high risk because of 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 and Oversight, brought a much-needed focus on problems that were costing the government billions of dollars.

In December 1992, GAO issued a series of reports on the fundamental causes of problems in high-risk areas, and in a second series in February 1995, it reported on the status of efforts to improve those areas. This, GAO's third series of reports, provides the current status of designated high-risk areas.

This report focuses on major, multibillion dollar information system development and modernization efforts at the Internal Revenue Service, the Federal Aviation Administration, the Department of Defense, and the National Weather Service. These efforts are having serious trouble meeting cost, schedule, and/or performance goals. Such problems are all too common in federal automation projects. Agencies have obligated over $145 billion during the past 6 years building, buying,

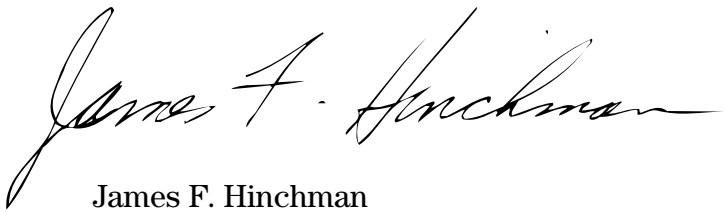
and maintaining computer systems and networks. Yet this vast investment has yielded poor returns in reducing federal operating costs, improving performance, supporting sound financial management, achieving mission results, and providing quality service to the American public.

In addition, we discuss two governmentwide information management issues. The first is information security. Despite the sensitivity and criticality of federal information systems, they are not being adequately protected from unauthorized access. The second issue involves the need to change computer systems so that they can accommodate dates after the year 1999. Unless corrected, computer programs that use dates to perform calculations, comparisons, and sorting may generate incorrect results when working with the years 2000 and beyond.

As dependence on computers grows and new high-risk areas emerge, federal agencies need to adopt modern practices to correct underlying management problems that impede effective system development and operations. In reviewing technology budget proposals, the 105th Congress should determine whether agencies are implementing recently enacted reform legislation—the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996. This legislation, which incorporates best practices of successful organizations, is designed to strengthen executive leadership in information management and institute sound capital

investment decision-making for maximizing the potential benefits from information systems.

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



James F. Hinchman
Acting Comptroller General
of the United States

Contents

Overview

The federal government's dependence on computer systems, networks, and electronic records to carry out its work continues to accelerate. Information systems are now integral to nearly every aspect of over $1.5 trillion in annual federal government operations and spending—from national defense and air traffic control to revenue collection and benefit payments. Yet, despite years of experience in developing systems, agencies across government continue to have chronic problems harnessing the full potential of information technology to improve performance, cut costs, and enhance responsiveness to the public.

The Problem

During the past 6 years, agencies have obligated over $145 billion building up and maintaining their information technology infrastructure. The benefits from this vast expenditure, however, have frequently been disappointing. GAO reports and congressional hearings have chronicled numerous system development efforts that suffered from multimillion dollar cost overruns, schedule slippages measured in years, and dismal mission-related results. At the same time, the public has become accustomed to high levels of quality and service from leading private sector organizations. They are increasingly

frustrated by the fact that they cannot get comparable performance from their national government.

This poor return on information technology investments has also left the Congress and executive branch severely handicapped by the lack of reliable data for measuring the costs and results of agency operations and making well-informed decisions. For instance, agencies are still a long way from demonstrating the most basic fiscal accountability to the public—such as passing the test of an independent audit—largely due to inadequate financial management and accounting systems.

Progress to Date

Recognizing the urgent need for improvement, the 104th Congress passed landmark reforms in information technology management. The Paperwork Reduction Act of 1995 is the overarching statute dealing with the acquisition and management of information resources—including information technology—by federal agencies. It emphasizes that agencies need to acquire and apply such resources to effectively support the accomplishment of agency missions and the delivery of services to the public. The Clinger-Cohen Act of 1996

repeats this theme and elaborates on requirements for agencies to follow when acquiring information technology.

Together, these acts direct agencies to implement a framework of modern technology management—one based on practices followed by leading public-sector and private-sector organizations that have successfully used technology to dramatically improve performance and meet strategic goals.

Among their many provisions, the reforms emphasize involving senior executives in information management decisions, appointing qualified senior-level Chief Information Officers, establishing appropriate agencywide technology standards, imposing much-needed discipline over technology spending, redesigning inefficient work processes, and using performance measures to assess technology's contribution in achieving mission results for the American people.

These management practices provide proven, practical methods for addressing the federal government's information management problems, maximizing benefits from technology spending, and controlling

the risks of system acquisition and development efforts. The challenge now is for agencies to apply this framework to their own technology efforts, particularly those with questionable returns, high risks, and high costs.

The importance of quickly implementing these reforms is emphasized by the fact that all four multibillion-dollar information technology efforts listed in our 1995 High-Risk Series[1] remain at high risk of being late, running over cost, and/or falling short of promised benefits. They are (1) the Internal Revenue Service's (IRS) Tax Systems Modernization, (2) the Federal Aviation Administration's (FAA) Air Traffic Control modernization, (3) the Department of Defense's Corporate Information Management initiative, and (4) the National Weather Service's (NWS) modernization. Each of these continues to suffer from one or more problems, such as unsound investment control, poor project management, and ongoing technical weaknesses—areas specifically addressed by the new legislation. Corrective measures are underway on many fronts, but our prior recommendations have not yet been fully implemented.

[1]GAO High-Risk Series, An Overview (GAO/HR-95-1, Feb. 1995).

Along with these four agency-specific efforts, we are including two new high-risk areas that touch virtually every major aspect of government operations. The first is information security. Despite the sensitivity and criticality of federal information systems, they are not being adequately protected from unauthorized access. Security weaknesses abound, creating serious pervasive risks for the federal government, such as potential disclosure of sensitive data, loss of assets worth billions of dollars due to fraud, and disruption of critical operations.

The second area involves the need for computer systems to be changed to accommodate dates beyond the year 1999. This "year 2000" problem stems from the common practice of abbreviating years by their last two digits. Computer systems could interpret "00" as the year 1900 instead of the year 2000, "01" as 1901, and so on. The resulting miscalculations involving dates and the computation of elapsed time could cascade through all kinds of activities, such as loans, mortgages, pensions, tax records, and benefit payments. Federal agencies need to take steps quickly to assess and correct this problem before time runs out.

Outlook for the Future

Will the picture be any different in another 2 years? A great deal depends on leadership by agency heads, their Chief Information Officers, and senior program executives.

Agencies need to establish goals for using information technology to enhance the productivity, efficiency, and effectiveness of their operations. Progress toward these goals should be measured and reported in annual budget submissions. In addition, agencies need to improve work processes used to carry out programs, develop and implement an integrated agencywide technology architecture, and strengthen their staffs' capabilities to manage information resources, deal with emerging technology issues, and develop needed systems. Each agency must also establish a structured process for selecting, controlling, and evaluating their capital investments in technology in order to maximize mission-related benefits and control risks.

The Congress also will need to be vigilant in overseeing agencies' information technology investments and project management. The recently enacted reforms could easily dissipate unless congressional committees use the full range of their budget, appropriations, and oversight functions to

hold agency leaders accountable for implementing them promptly.

The Congress should assure itself that agency heads are working to identify strengths and weaknesses in their information management practices. Congressional committees should expect agencies to provide hard data on how technology spending is being used to improve mission performance and reduce operating costs. And there should be clear evidence that each agency has implemented a sound technology investment control process. The Congress should also see to it that the Office of Management and Budget (OMB) is carrying out its critical role in guiding the agencies in implementing investment reforms and that OMB is enforcing accountability for achieving improvements through the executive branch budget process.

High-Risk System Development and Modernization Efforts

Our 1995 High-Risk Series included four multibillion-dollar modernization efforts that were having serious trouble meeting their cost, schedule, and/or performance goals.[1] In our ongoing work, we have continued to make specific recommendations for mitigating risks in areas such as investment control, system development, and technical infrastructure. These agencies have made some progress. Still, the level of improvement has not yet been enough to bring the problems under control. After 2 years, all four remain on our high-risk list.

IRS' Tax Systems Modernization

Over the last decade, IRS has been attempting to overhaul its timeworn, paper-intensive approach to tax return processing. In 1995, we identified serious management and technical weaknesses in the modernization program that jeopardize its successful completion, recommended many actions to fix the problems, and added IRS' modernization to our high-risk list. Since then, IRS and Treasury have together taken several steps to implement our recommendations, but much remains to be done. At stake is the over $3 billion that IRS has spent or obligated on this modernization

[1]GAO/HR-95-1, Feb. 1995.

since 1986, as well as any additional funds that IRS plans to spend on modernization.

In July 1995,[2] we reported that IRS (1) did not have a comprehensive business strategy to cost effectively reduce paper tax return filings and (2) had not yet fully developed and put in place the requisite management, software development, and technical infrastructure necessary to successfully implement its ambitious, world-class modernization. We also reported that IRS lacked an overall systems architecture, or blueprint, to guide the modernization's development and evolution.

At that time, we made over a dozen recommendations to the IRS Commissioner to address these weaknesses. Collectively, the recommendations called for IRS to (1) formulate a comprehensive business strategy for maximizing electronic filings, (2) improve its strategic information management by implementing a process for selecting, prioritizing, controlling, and evaluating the progress and performance of all major information systems and investments, (3) implement disciplined, consistent procedures for software

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

requirements management, quality assurance, configuration management, and project planning and tracking, and (4) complete and enforce an integrated systems architecture and security and data architectures. IRS agreed to implement our recommendations.

In May 1996, Treasury reported to the House and Senate Appropriations Committees on steps under way and planned to exert greater management oversight of IRS' modernization efforts.[3] For example, it established a Modernization Management Board as the primary review and decision-making body for modernization and for policy and strategic direction. In addition, Treasury scaled back the overall size of the modernization by approximately $2 billion and is working with IRS to obtain additional contractor help to accomplish the modernization.

Pursuant to congressional direction, we assessed IRS' actions to correct its management and technical weaknesses, as delineated in Treasury's report on tax systems modernization. We reported in June and September 1996 that IRS had initiated

[3]Report to House and Senate Appropriations Committees: Progress Report on IRS's Management and Implementation of Tax Systems Modernization, Department of the Treasury, May 6, 1996.

many activities to improve its modernization efforts but had not yet fully implemented any of our recommendations. Consequently, in order to minimize the risk attached to continued investment in systems modernization, we suggested to the Congress that it consider limiting modernization funding exclusively to cost-effective efforts that (1) support ongoing operations and maintenance, (2) correct IRS' pervasive management and technical weaknesses, (3) are small, represent low technical risk, and can be delivered quickly, and (4) involve deploying already developed and fully tested systems that have proven business value and are not premature given the lack of a completed architecture.

To help oversee IRS' modernization, the Congress in the fiscal year 1997 Omnibus Consolidated Appropriations Act[4] directed IRS to (1) submit by December 1, 1996, a schedule for transferring a majority of its modernization development and deployment to contractors by July 31, 1997, and (2) establish a schedule by February 1, 1997, for implementing our recommendations by October 1, 1997. In its conference report on the act, the Congress directed the Secretary

[4]P.L. 104-208, Sept. 30, 1996.

of the Treasury to (1) provide quarterly reports on the status of IRS' corrective actions and modernization spending[5] and (2) submit by May 15, 1997, a technical architecture for the modernization that has been approved by Treasury's Modernization Management Board. Additionally, the Board was directed to prepare a request for proposals by July 31, 1997, to acquire a prime contractor to manage modernization deployment and implementation.

IRS has continued to take steps to address our recommendations and respond to congressional direction. For example, IRS hired a new Chief Information Officer. It also created an investment review board to select, control, and evaluate its information technology investments. Thus far, the board has reevaluated and terminated selected major modernization development projects, such as the Document Processing System (DPS).

Additionally, IRS (1) provided a November 26, 1996, report to the Congress that set forth IRS' strategic plan and schedule for shifting

[5]H.R. Report No. 863, 104th Cong., 2d sess. (1996). The Congress also included the requirement that Treasury provide a milestone schedule for developing and implementing all modernization projects in Treasury's fiscal year 1996 appropriations act (P.L. 104-52, Nov. 19, 1995).

modernization development and deployment to contractors, (2) is finalizing a comprehensive strategy to maximize electronic filing that is scheduled for completion in early 1997, and (3) is updating its system development life cycle methodology and working across various IRS organizations to define disciplined processes for software requirements management, quality assurance, configuration management, and project planning and tracking. Additionally, IRS is developing a technical architecture for the modernization and plans to provide this to the Congress by May 15, 1997. Further, IRS is preparing a schedule for implementing our recommendations and plans to provide it to the Congress in February 1997.

While we recognize IRS' and Treasury's actions to address these problems, we remain concerned. Much remains to be done to fully implement essential improvements. Increasing the use of contractors, for example, will not automatically increase the likelihood of successful modernization because IRS does not have the technical capability needed to manage all of its current contractors. As a case in point, IRS' Cyberfile—a system development effort led by contractors to enable taxpayers to

personally prepare and file their tax returns electronically—exhibited many undisciplined software acquisition practices as well as inadequate financial and management controls. Eventually, IRS canceled the Cyberfile project after spending over $17 million and without fielding any of the system's promised capabilities. Therefore, if IRS is to use additional contractors effectively, it will have to first strengthen and improve its ability to manage those contractors.

In addition, IRS needs to continue to make concerted, sustained efforts to fully implement our recommendations and respond effectively to the requirements outlined by the Congress. It will take both management commitment and technical discipline for IRS to do this effectively. Accordingly, we plan to continue assessing IRS' progress in its critical endeavor to modernize.

FAA's Air Traffic Control Modernization

Faced with rapidly growing air traffic volumes and aging air traffic control equipment, the FAA in 1981 initiated an ambitious air traffic control (ATC) modernization program. This effort, which is expected to cost $34 billion through fiscal

year 2003, mostly involves investments in a multitude of software-intensive computer systems.

Over the past 15 years, the modernization program has experienced cost overruns, schedule delays, and performance shortfalls of large proportions—particularly in the $7.6 billion former centerpiece of the modernization known as the Advanced Automation System, which FAA restructured in 1994. The acquisition of that system failed because FAA did not recognize the technical complexity of the effort, realistically estimate the resources required, adequately oversee its contractors' activities, or effectively control system requirements.[6] With $11 billion planned to be spent on the ATC program from fiscal years 1998 through 2003, and billions more surely to follow, it is critical that FAA overcome the weaknesses that threaten this effort.

To its credit, FAA has made progress in acquiring an interim replacement for its outage-plagued system that processes data into displayable images on controllers'

[6]Advanced Automation System: Implications of Problems and Recent Changes (GAO/T-RCED-94-188, Apr. 13, 1994).

screens.[7] Although key acquisition milestones, events, and risks remain, FAA is currently on track to deliver promised capabilities ahead of schedule and within budget. Further, when we recommended that two risks associated with system testing—contention for human test resources and test baseline configuration change control—be formally managed, FAA officials agreed to do so.

Still, serious problems remain. The many systems comprising the modernization effort have long proceeded without the benefit of a complete systems architecture, or overall blueprint, to guide development and evolution.[8] The result has been unnecessarily higher spending to buy, integrate, and maintain hardware and software. For example, the number of application programming languages used on existing systems has been left unchecked, growing to 53. This has needlessly increased software maintenance costs and hindered software reuse among systems. We have recommended that FAA develop and enforce a complete systems architecture and

[7]Air Traffic Control: Good Progress on Interim Replacement for Outage-Plagued System, but Risks Can Be Further Reduced (GAO/AIMD-97-2, Oct. 17, 1996).

[8]Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, Feb. 3, 1997).

implement a management structure for doing so that is similar to the Chief Information Officers provisions of the Clinger-Cohen Act of 1996.

Exacerbating the modernization's problems is unreliable cost information—both future estimates of costs and accumulations of actual costs.[9] According to the Clinger-Cohen Act of 1996, the selection of information technology investments should be based on competing projects' estimated costs, benefits, and risks. To effectively manage these investments, their actual cost performance must be measured against their cost estimates. However, FAA lacks the adequate cost estimating processes and cost accounting practices needed to do so, leaving it at risk of making ill-informed decisions on critical multimillion, even billion, dollar air traffic control systems. We recommended that FAA institutionalize defined processes for estimating projects' cost, and develop and implement a managerial cost accounting capability.

FAA must also address problems in its organizational culture, which does not reflect a strong enough commitment to

[9]Air Traffic Control: Improved Cost Information Needed to Make Billion Dollar Modernization Investment Decisions (GAO/AIMD-97-20, Jan. 22, 1997).

mission focus, accountability, coordination, and adaptability.[10] For example, project officials established unrealistic cost estimates in order to obtain funding and suppressed news about setbacks in order to avoid heightened managerial oversight. Without strong leadership to promote the desired organizational behavior, the modernization effort's problems will be difficult to overcome. We recommended that FAA develop a comprehensive strategy for addressing this issue.

To further pinpoint the root causes of FAA's modernization problems, we have a review underway to determine whether FAA's software acquisition capability is sufficiently mature to successfully modernize the highly complex, real-time ATC system.

Defense's Corporate Information Management Initiative

The Department of Defense's Corporate Information Management (CIM) initiative, started in 1989, was expected to save billions of dollars by streamlining operations and implementing standard information systems supporting such important business areas as supply distribution, materiel management, personnel, finance, and transportation.

[10]Aviation Acquisition: A Comprehensive Strategy Is Needed for Cultural Change at FAA (GAO/RCED-96-159, Aug. 22, 1996).

However, 8 years after beginning CIM, and after spending about $20 billion, Defense's savings goal has not been met because the Department has not yet implemented sound management practices.

We have made numerous recommendations for improving the Department's management of CIM, including (1) better linking system modernization projects to business process improvement efforts, (2) establishing plans, performance measures, and clearly defined roles and responsibilities for implementing CIM, (3) improving controls over information technology investments, and (4) not initiating system improvement projects without sound economic and technical analyses.[11]

But Defense has yet to successfully implement these recommendations. Instead, it continues to spend billions of dollars on system migration projects with little sound

[11]Defense Management: Stronger Support Needed for Corporate Information Management Initiative to Succeed (GAO/AIMD/NSIAD-94-101, April 12, 1994); Defense Management: Selection of Depot Maintenance Standard System Not Based on Sufficient Analyses (GAO/AIMD-95-110, July 13, 1995); Defense Transportation: Migration Systems Selected Without Adequate Analysis (GAO/AIMD-96-81, August 29, 1996); and Defense IRM: Critical Risks Facing New Material Management Strategy (GAO/AIMD-96-109, September 6, 1996).

analytical justification.[12] Rather than relying on a rigorous decision-making process for information technology investments—as used in leading private and public sector organizations that we studied—Defense is making system migration decisions without

- appropriately analyzing costs, benefits, and technical risks;
- establishing realistic project schedules; or
- considering how business process improvements could affect technology investments.

Further, in some cases, Defense has denied its own decisionmakers the opportunity to evaluate the progress of technology investments over time by forgoing its established oversight process.

Not surprisingly, the results of Defense's major technology investments have been meager. For example, in the transportation area, it has made some investments that are likely to result in a negative return on investment. For materiel management, it has abandoned its system modernization strategy after spending over $700 million. For depot maintenance, Defense expects to

[12]A migration system is an automated information system which replaces several systems that perform similar functions.

spend over $1 billion to develop a standard system that will achieve less than 2.3 percent in reduced operational costs over a 10-year period.

The Department estimates that additional spending on system migration projects between now and the year 2000 will total more than $11 billion. As part of its Clinger-Cohen Act implementation efforts, the Department is establishing a framework for better managing this investment using its planning, programming, and budgeting system. While a step in the right direction, this initiative is just beginning. We have ongoing and planned work—including reviews of the Department's system modernization strategy and investment controls—aimed at helping Defense managers make well-informed business decisions based on an accurate picture of the costs of technology investments, their related benefits, and an appreciation for how they fit into the Department's long-term and short-term goals.

National Weather Service's Modernization

NWS decided almost 15 years ago to leverage the power of information technology to "do more with less." Promising better weather forecasts and downsized operations, NWS has

been acquiring new observing systems—such as radars, satellites, and ground-based sensors—as well as powerful forecaster workstations, at a combined cost of about $4.5 billion. Although NWS acknowledges that key problems confront the new systems, it has found that the new radars and satellites have improved forecasts and warnings. How successful NWS will ultimately be in this endeavor, however, partly depends on how quickly it can address several key problems that we have identified.

Although the development and deployment of the observing systems associated with NWS' modernization are nearing completion, unresolved issues remain concerning the observing systems' operational effectiveness and efficient maintenance. To illustrate, we reported that the new radars are not always up and running when severe weather is threatening,[13] and that the ground-based sensors fall short of performance and user

[13]Weather Forecasting: Radar Availability Requirements Not Being Met (GAO/AIMD-95-132, May 31, 1995) and Weather Forecasting: Radars Far Superior to Predecessors, but Location and Availability Questions Remain (GAO/T-AIMD-96-2, Oct. 17, 1995).

expectations, particularly when the weather is active.[14]

We recommended that NWS correct shortfalls in radar performance and define and prioritize all ground-based sensor corrections needed to meet user needs. NWS addressed some of our radar and ground-based sensor performance concerns, but others remain. Also, we recently reported that NWS has not managed this massive investment through sound decision-making processes.[15] For instance, NWS lacks a means by which to ensure that systems provide promised returns on investments. Currently, only the radars have had their benefits analyzed. In addition, the sizable staff reductions that the modernization promised will not be realized. For example, we reported in 1995 that NWS originally planned to reduce staff by 21 percent, but now the goal has been scaled back to 8 percent.[16] NWS attributes the reduced goal primarily to needing more staff

[14]Weather Forecasting: Unmet Needs and Unknown Costs Warrant Reassessment of Observing System Plans (GAO/AIMD-95-81, April 21, 1995).

[15]Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks (GAO/AIMD-96-64, Sept. 30, 1996).

[16]Weather Service Modernization Staffing (GAO/AIMD-95-239R, Sept. 26, 1995).

than originally envisioned to operate new systems and to unanticipated requirements that were beyond NWS' control.

Further, the centerpiece of the modernization—the forecaster workstations that will integrate observing systems' data and support forecaster decision-making—is far from providing all promised capabilities, for several reasons. These workstations have been delayed and become more expensive because of design problems and management shortcomings. In addition, workstation development continues without all the technical process capabilities advocated by the Software Engineering Institute (SEI), although NWS did improve some of its capabilities based on our recommendation to do so.[17] Also, NWS has not demonstrated that all proposed capabilities will result in mission improvements, thereby increasing the risk

[17]Weather Forecasting: Improvements Needed in Laboratory Software Development Processes (GAO/AIMD-95-24, Dec. 14, 1994). SEI, part of Carnegie Mellon University, has developed generally recognized standards for gauging an organization's ability to develop or acquire software.

that spending will be wasted on unneeded system capabilities.[18]

In 1996, we made several recommendations that, if implemented, will strengthen NWS' ability to manage the acquisition of these workstations. Specifically, we recommended that NWS

- validate all workstation requirements on the basis of mission impact,
- improve its process to test software,
- establish a software quality assurance program, and
- obtain an independent cost assessment since NWS does not have reliable project cost information.[19]

As we reported in our 1995 high-risk series, the modernization and evolution of this major systems initiative has long begged for a guiding systems architecture. NWS has acknowledged that this technical blueprint is needed and is currently developing one to address our March 1994 recommendation to

[18]Weather Forecasting: NWS Has Not Demonstrated that New Processing System Will Improve Mission Effectiveness (GAO/AIMD-96-29, Feb. 29, 1996). Weather Forecasting: New Processing System Faces Uncertainties and Risks (GAO/T-AIMD-96-47, Feb. 29, 1996).

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

do so. In the meantime, however, NWS will continue to incur higher system development and maintenance costs and reduced performance until the systems architecture is developed and enforced.[20]

[20]Weather Forecasting: Systems Architecture Needed for National Weather Service Modernization (GAO/AIMD-94-28, Mar. 11, 1994).

Governmentwide High-Risk Issues

One sign of the federal government's growing dependence on information technology is the emergence of high-risk issues that are critical to operations at all agencies. This year, we are designating two governmentwide information management issues as high risk: information security and the Year 2000 problem. These issues require not only agency-specific actions, but also cooperative efforts among the executive branch and the Congress to manage risks and develop solutions.

Information Security

Malicious attacks on computer systems are an increasing threat to our national welfare. We rely heavily on interconnected systems to control critical functions, such as communications, financial services, transportation, and utilities. Though greater use of interconnected systems promises significant benefits in improved business and government operations, such systems are much more vulnerable to anonymous intruders, who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations.

At the federal level, system interconnectivity, combined with poor security management, is putting billions of

dollars worth of assets at risk of loss and vast amounts of sensitive data at risk of unauthorized disclosure. In addition, the increasing reliance on networked systems and electronic records has elevated concerns that critical federal operations are vulnerable to serious disruption. This is because automated systems and electronic records are fast replacing manual procedures and paper documents, which in many cases are no longer available as "backup" if automated systems fail. Further, although such disruption could be precipitated by natural disasters or accidents, there is evidence that some organizations are developing strategies and tools for conducting premeditated attacks on information systems.

Many federal operations that rely on computer networks are attractive targets for individuals or organizations with malicious intentions. Examples include law enforcement, import entry processing, various financial transactions, payroll, defense operational plans, electronic benefit payments, and electronically submitted medicare claims.

Despite their sensitivity and criticality, federal systems and data are not being

adequately protected. Since June 1993, we have issued over 30 reports describing serious information security weaknesses at major federal agencies.

For example, in May 1996, we reported that tests at the Department of Defense showed that Defense systems may have experienced as many as 250,000 attacks during 1995, that about 64 percent of attacks were successful at gaining access, and that only a small percentage of these attacks were detected.[1] In September 1996, we reported that, during the previous 2 years, serious information security control weaknesses had been reported for 10 of the 15 largest federal agencies.[2] For half of these agencies, the weaknesses had been reported repeatedly for 5 years or longer. Several of our most disturbing reports on information security are for limited official use and, therefore, cannot be discussed here because of the risk that unscrupulous individuals may attempt to exploit reported weaknesses.

[1]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996); Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996); and Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996).

[2]Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, Sept. 24, 1996).

Many of the federal information security weaknesses and causal factors reported over the last few years were identified as a direct result of the annual financial statement audits initiated under the Chief Financial Officers Act of 1990. Although these audits pertain primarily to financial management systems, they generally include a review of computer-based controls that affect a significant portion of an agency's broader operations.

In addition to describing information security weaknesses, our reports contain dozens of recommendations to individual agencies for improvement. Agencies have acted on many of these recommendations, and, in early 1996, OMB issued updated guidance to agencies on the security of federal automated information resources. However, several underlying factors need to be addressed to help ensure that federal agencies adequately protect their systems and data on a continuing basis. These factors include:

- insufficient awareness and understanding of information security risks among senior agency officials,

- poorly designed and implemented security programs that do not adequately monitor controls or proactively address risk,
- a shortage of personnel with the technical expertise needed to manage controls in today's sophisticated information technology environment, and
- limited oversight of agency practices at a governmentwide level.

In light of the increasing importance of information security and the pattern of widespread problems that has emerged, stronger central leadership is needed. Our previously cited September 1996 report[3] concluded that OMB needs to play a more proactive role in promoting awareness and in monitoring agency practices—a role that was recently reemphasized in the PRA and Clinger-Cohen Act. In particular, we recommended that OMB engage assistance from private contractors and others with appropriate expertise to assist in monitoring agency information security programs. Also, as chair of the Chief Information Officers Council, OMB should encourage council members to adopt information security as one of their top priorities and develop a strategic plan for addressing the root causes

[3]GAO/AIMD-96-110, Sept. 24, 1996.

of agency security problems. Such a plan could include

- developing information on existing and emerging information security risks,
- establishing a program for reviewing the adequacy of individual agency security programs using interagency teams of reviewers, and
- developing or identifying training and certification programs that could be shared among agencies.

OMB reported in December 1996 that it has begun efforts to improve its oversight of federal agencies' activities in information security by holding a training session for program examiners to increase their understanding of this management issue and its implications. In addition, the CIO Council has included information security as one of its priorities. However, at present, it is too early to assess the adequacy of OMB's or the Council's response to our concerns.

The Year 2000 Problem

At 12:01 on New Year's morning of the year 2000, many computer systems could either fail to run or malfunction—thereby producing inaccurate results—simply because the equipment and software were

not designed to accommodate the change of date to the new millennium.

The Year 2000 problem is rooted in the way dates are recorded and computed in many computer systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, in order to conserve on electronic data storage and reduce operating costs. With this two-digit format, however, the year 2000 is indistinguishable from 1900, 2001 from 1901, and so on. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999.

Unless this problem is resolved ahead of time, widespread operational and financial impacts could affect federal, state, and local governments; foreign governments; and private-sector organizations worldwide. At the federal level, scenarios like these are possible:

- IRS' tax systems could be unable to process returns, which in turn could jeopardize the collection of revenue and the entire tax processing system.

- Payments to veterans with service-connected disabilities could be severely delayed because Veterans Affairs' compensation and pension system either halts or produces checks that are so erroneous that the system must be shut down and the checks processed manually.
- Social Security Administration's disability insurance process could experience major disruptions because the interface with various state systems fails, thereby causing delays and interruptions in disability payments to citizens.
- Federal systems used to track student education loans could produce erroneous information on loan status, such as indicating that an unpaid loan had been satisfied.

While the date issue will reach a crescendo at the end of the century, date-related problems have been manifesting themselves for some time. For example, the Defense Department had medical benefits computational problems in 1980 with its Defense Entitlement Eligibility Report System (DEERS). Had the system not been corrected, people who were 45 years old, or younger, would have been erroneously terminated from receiving their entitlement benefits.

Other problems are just beginning to show up. Recently, a Defense Logistics Agency system marked 3-year contracts as delinquent even though they had not yet been let. Defense has also uncovered date-related problems in its Space Defense Operations Center involving a system that supports its Integrated Tactical Warning and Attack Assessment community. Testing revealed 10 date-related discrepancies that would have caused a significant operational impact.

Other federal agencies face similar operational risks and impacts. Resolving the date problem will involve extensive, resource-intensive efforts due to the large scale of many federal systems and the numerous dependencies and interactions they often have with systems of both private-sector organizations and state agencies.

To complicate matters further, many government computer systems were originally designed and developed 20 to 25 years ago, are poorly documented, and use a wide variety of computer languages—many of which are old or obsolete. The systems consist of tens or hundreds of computer programs, each with thousands, tens of

thousands, or even millions of lines of code, which must be examined for date problems. Moreover, the government's computer systems, like private sector systems, have numerous components—hardware, firmware, operating systems, communications applications, and database software—that are affected by the date problem.

Given that every federal agency is at risk of system failures, the 104th Congress held hearings to determine the severity of the problem and the progress that agencies were making to deal with it. For instance, in April 1996, the House Government Reform and Oversight Committee surveyed 24 departments and agencies. They found that only 9 had developed plans for addressing the problem.

With the year 2000 less than 3 years away, much work must be done, and done quickly. Ensuring that systems are Year 2000 compliant represents the widest-scale system and software conversion effort ever attempted. Agencies must immediately assess their Year 2000 risk exposure, and plan and budget for achieving Year 2000 compliance for all of their mission critical systems. This will involve identifying and

analyzing mission-critical computer systems, developing date conversion strategies and plans, and dedicating sufficient resources to convert the computer systems by early 1999 in order to allow 1 year for additional testing and error correction. Agencies will also need to develop contingency plans for those systems that they are unable to change in time.

In 1995, OMB formed an interagency working group on the year 2000 issue, which is now under the President's recently established Chief Information Officers Council. The basic federal strategy for resolving the year 2000 problem relies on Chief Information Officers to raise management awareness of the problem at their agencies, and then direct work to assess the scope of the changes needed, renovate the systems that need to be changed, test the changed systems, and then implement them. OMB is currently working with agencies to establish time frames for completing these steps. Regulatory action has also been taken to assist agencies in acquiring information products and systems that are already year 2000 compliant, whenever possible.

We are currently working with the Congress and the executive branch to identify specific

recommendations for resolving the Year 2000 problem. In this regard, we plan to review efforts at the Department of Defense, IRS, the Social Security Administration, FAA, Veterans Affairs, and the Health Care Financing Administration. In addition, we are developing a set of audit templates for use by the audit community and agencies to identify their risk areas.

Further Action Needed

The high-risk system development and modernization problems described above are common across the government—and have been for many years. A broad set of solutions is needed to help agencies prevent high risks and maximize the benefits of technology for improving performance and reducing costs. Similarly, there is a need to strengthen federal agencies' ability to effectively address emerging technology issues and problems on a governmentwide basis.

To improve this situation, we have worked closely with the Congress since our 1995 high-risk report to fundamentally revamp and modernize federal information management practices. Our study of leading public and private sector organizations showed how they applied an integrated set of management practices to create the information technology infrastructures they needed to dramatically improve their performance and achieve mission goals.[1] These practices provide federal agencies with essential lessons on how to overcome the root causes of their chronic information management problems.

[1]Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology—Learning from Leading Organizations (GAO/AIMD-94-115, May 1994).

The 104th Congress used these lessons to create the first significant reforms in information technology management in over a decade: the 1995 PRA and the Clinger-Cohen Act of 1996.[2] These laws, discussed below, focus sharply on building a foundation for sustained improvement by (1) establishing strong agency-level leadership in technology issues and (2) implementing sound processes for approving and managing investments in technology.

Strong Agency Leadership in Information Management Is Critical

Senior executives in the successful organizations we studied were personally committed to improving the management of technology. Agency leaders likewise must recognize the urgent need to improve their agencies' information management practices and create and maintain the momentum for implementing reform.

Both PRA and the Clinger-Cohen Act make agency heads directly responsible for effective information management. Among their key duties, agency heads are to

[2]The Omnibus Consolidated Appropriations Act, 1997, renamed both the Federal Acquisition Reform Act of 1996 and the Information Technology Management Reform Act of 1996 as the "Clinger-Cohen Act of 1996."

- establish goals for improving the use of information technology in enhancing the productivity, efficiency, and effectiveness of agency operations and service to the public;
- measure the actual performance and contribution of technology in supporting agency programs; and
- include with their agencies' OMB budget submission a report on the progress being made in meeting operational improvement goals through the use of technology.

In short, rather than leaving technology issues to mid-level specialists, agency heads must incorporate strategic information management into an executive-level general management framework—one that incorporates the agency's budget process and a set of solid performance measures.

To help them carry out these new responsibilities, the heads of agencies are to designate a Chief Information Officer (CIO). The CIO is to be much more than a senior technology manager. As a top-level executive reporting directly to the agency head, the CIO is responsible for achieving mission results through technology by

- working with the agency head and senior managers on effective information

management to achieve the agency's strategic performance goals;
- promoting improvements to work processes used to carry out programs;
- increasing the value of the agency's information resources by developing and implementing an integrated agencywide technology architecture; and
- strengthening the agency's knowledge, skills, and capabilities to effectively manage information resources, deal with emerging technology issues, and develop needed systems.

As we learned from appointments to the Chief Financial Officer positions, getting the right people in place will make a real difference in implementing lasting management reforms. The reforms simply will not work without qualified, effective leadership. OMB is monitoring the agencies' CIO appointments at 28 federal agencies and has found mixed progress. According to OMB, as of November 1996, many agencies had CIOs or acting CIOs who had limited operational and technical experience, unclear roles, additional duties besides information resources management, and/or did not report directly to the agency head. OMB is continuing to evaluate these situations as agencies take further actions.

Along with the top executives and CIOs, program managers have critical leadership responsibilities for information management. In successful organizations we studied, managers work with the CIOs to define information needs for their programs and develop strategies, systems, and capabilities to meet those needs. The reform legislation calls for program officials to take ownership of technology projects and be held accountable for their results. This represents a major shift away from the common practice of delegating system development projects to technical specialists.

Controlling Investments in Information Technology

A key practice identified in our study of leading organizations is that they manage information technology projects as investments. Top executives periodically assess all major projects—proposed, under development, and operational—then prioritize them and make funding decisions based on factors such as cost, risk, return on investment, and support of mission-related outcomes. Once projects are selected for funding, executives monitor them continually, taking quick actions to resolve development problems and mitigate risks. After a project is implemented, executives evaluate actual versus expected results and

revise their investment management process based on lessons learned.

PRA and the Clinger-Cohen Act incorporate these features into new requirements on how technology-related projects are to be selected and managed. The heads of agencies are to design and implement a structure for maximizing the value and managing the risk of technology investments, including

- establishing a process to select, control, and evaluate information technology investments using quantitative and qualitative criteria and data;
- modernizing inefficient administrative and mission-related work processes before making significant technology investments to support them;
- mitigating the risks of acquiring large, complex systems by building them in a modular fashion; and
- monitoring project progress and performance using up-to-date data.

Current federal practices fall far short of these expectations. For example, in our report on the technology investment practices at five federal agencies, only one had defined decision criteria for cost, risk,

and return.[3] In the absence of such information, investment decisions were disproportionately based on subjective, qualitative factors. Generally, data on a project's cost, schedule, risks, and returns were not documented, defined, or kept current, and in many cases was not used to make investment decisions. Instead, agencies focused on justifying funding for new technology projects rather than managing all projects as a portfolio of competing investments. Once a project was approved, the agency exerted little effort to ensure that information on it was kept accurate and up to date. Rarely were data used to manage a project's progress throughout its life cycle.

Under the new legislation, OMB has significant leadership responsibility in directing agencies to implement investment reforms. In our information technology investment report, cited above, we recommended that OMB develop guidance for agencies on implementing a technology investment decision-making process, including advising agencies on the minimum quality standards for data used to assess cost, benefit, and risks. We also

[3]Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks (GAO/AIMD-96-64, Sept. 30, 1996).

recommended that OMB ensure that agencies' investment control processes are in compliance with such guidance by assessing their strengths and weaknesses, and developing remedial actions and timetables for any needed improvements.

Strong Congressional Oversight Is Essential to Successful Reform

Controlling and preventing high risks will depend largely on how well federal agencies implement PRA and the Clinger-Cohen Act. From our past experience with the implementation of the Chief Financial Officers Act, for which important progress has been made, we know that the early days following the passage of reform legislation are telling. The level of interest shown by the 105th Congress in driving and overseeing the implementation of the reforms will send a strong signal to the agencies that they should move vigorously to implement them. Congressional oversight should focus on progress being made in the following four areas.

(1) Executive Accountability: The Congress should assure itself that agency heads are educating their agencies about the reforms and putting in place the management structure to implement them. Agency heads should currently be devoting

time, talent, and resources to analyzing the strengths and weaknesses of their information management practices. Our own experience in assisting agencies with such self-assessments has identified many fundamental problems that must be quickly addressed, such as poor performance measures, vaguely defined customer needs, and weak integration of technology investment into the planning, budgeting, and evaluation processes.

Members of Congress should expect agency heads to provide hard numbers and facts on their information technology spending and how it is being used to improve mission performance. As noted earlier, the reform legislation requires annual reports by agency heads to OMB on the program performance benefits achieved from capital investments in information technology and how these benefits relate to the achievement of the agency's goals. Probing discussions of these reports should be a regular feature of congressional budget, appropriations, and oversight hearings.

(2) CIO responsibilities: The Congress should closely monitor the progress that agency heads are making in appointing well-qualified CIOs who have sound

expertise, practical experience, and proven track records in information technology and strategic management.

Each CIO should be positioned as a senior management partner, reporting directly to the agency head. In addition to strong sponsorship from agency heads, CIOs need active support from other senior executives in setting up effective information management practices that meet the intent of the reform legislation. CIO responsibilities should focus sharply on strategic information management issues, and not be burdened with other activities, such as administrative services, personnel, and contracting—as has often happened in the past. Similarly, the CIO and Chief Financial Officer positions should not be combined under one person, since the problems associated with financial and information management are very significant and require full-time attention by separate individuals with appropriate talent, skills, and experience in each area.

The Congress should expect to see CIOs making clear progress in defining and implementing information management policies, guidelines, and standards consistent with the reform legislation. They should be

establishing a sound information technology architecture at their agencies to provide a framework for integrating current and new systems. And they should be active in identifying the technical skills and capabilities that their agencies need to acquire and manage information resources in a disciplined manner to better control risk and achieve desired outcomes. Ultimately, these actions should result in measurable improvements in mission performance.

(3) Interagency Actions: Building on the agency-level CIO positions established under the reform legislation, the President has established a CIO Council to develop recommendations on governmentwide information technology policies, procedures, and standards. This Council will be a critical test of the efficacy of CIOs in taking concerted action to address and control governmentwide technology risks. Initially, the Congress should focus on the Council's progress in promoting effective federal technology investment reforms at their agencies and dealing with the governmentwide information security and Year 2000 issues.

(4) Investment Oversight and OMB Leadership: Given the federal government's

long-standing record of poor investments in information technology, a much higher level of oversight should be applied to agencies' investment management processes and the actual results achieved. The Congress should closely monitor how well agencies are institutionalizing processes to select, control, and evaluate their technology projects. By now, heads of agencies should be well on their way to defining and implementing the elements of an investment decision-making process called for by the legislation. One measure of progress is to review the effectiveness of agencies' actions in bringing under control the high-risk modernization efforts described in this report.

As part of this oversight effort, the Congress should also assess the effectiveness of OMB's leadership in two areas:

- establishing guidance and policies for agencies to follow in implementing the investment reforms and
- evaluating the results of agency technology investments and enforcing accountability for results through the executive branch budget process.

In the first area, OMB has been proactive in drafting new policies and procedures to assist agencies in establishing technology investment decision-making processes. For example, OMB has issued a guide on evaluating information technology investments for use by its own staff and the agencies.[4] It is important that OMB continue to clearly define expectations for agencies and for itself in this key area.

As for OMB's oversight of agency technology portfolios, we recommended in our previously cited technology investment report that OMB

- develop recommendations for the President's budget on funding levels for technology projects that take account of an agency's track record in delivering performance improvements from technology investments and
- develop an approach for determining whether OMB itself is having an impact on reducing the risk or increasing the returns on agency information technology investments.

[4]Evaluating Information Technology Investments: A Practical Guide, version 1.0 (S/N 041-001-00460-2, Nov. 1, 1995).

To its credit, OMB issued an October 25, 1996, memorandum to heads of executive departments and agencies laying out decision criteria that OMB will use in evaluating major information system investments proposed for funding under the President's fiscal year 1998 budget. The criteria strongly reinforce the provisions of the reform legislation. In the memorandum, OMB states that as a general presumption, it will recommend new and continued funding only for those major system investments that satisfy these criteria.

OMB's effectiveness will depend greatly on its ability to marshall the resources and expertise that its staff needs to produce sound evaluations of agencies' technology investment portfolios. Given existing workloads and the resilience of the OMB culture, OMB will have little impact on the quality of technology investment decision-making without a determined effort to build the necessary assessment skills.

Finally, as part of its review of the budget proposals for FY 1998, the Congress should look for clear evidence that the soundness of an agency's investment process, along with its track record in achieving performance

improvements from technology, is being considered in executive branch funding requests for information systems.

Related GAO Reports

Strategic Information Management

Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks (GAO/AIMD-96-64, Sept. 30, 1996).

NASA Chief Information Officer: Opportunities to Strengthen Information Resources Management (GAO/AIMD-96-78, Aug. 15, 1996).

Information Management Reform: Effective Implementation Is Essential for Improving Federal Performance (GAO/T-AIMD-96-132, July 17, 1996).

Government Reform: Using Reengineering and Technology to Improve Government Performance (GAO/T-OCG-95-2, Feb. 2, 1995).

Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994).

Internal Revenue Service

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

IRS Operations: Critical Need to Continue Improving Core Business Practices (GAO/T-AIMD/GGD-96-188, Sept. 10, 1996).

Internal Revenue Service: Business Operations Need Continued Improvement (GAO/AIMD/GGD-96-152, Sept. 9, 1996).

Tax Systems Modernization: Cyberfile Project Was Poorly Planned and Managed (GAO/AIMD-96-140, Aug. 26, 1996).

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996).

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

IRS Automation: Controlling Electronic Filing Fraud and Improper Access to Taxpayer Data (GAO/T-AIMD/GGD-94-183, July 19, 1994).

Tax Systems Modernization: Automated Underreporter Project Shows Need for Human Resource Planning (GAO/GGD-94-159, July 8, 1994).

Tax Systems Modernization: Status of Planning and Technical Foundation (GAO/T-AIMD-GGD-94-104, March 2, 1994).

FAA Air Traffic Control Modernization

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

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

Air Traffic Control: Good Progress on Interim Replacement for Outage-Plagued System, but Risks Can Be Further Reduced (GAO/AIMD-97-2, Oct. 17, 1996).

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

Air Traffic Control: Status of FAA's Modernization Program (GAO/RCED-95-175FS, May 26, 1995).

Advanced Automation System: Implications of Problems and Recent Changes (GAO/T-RCED-94-188, Apr. 13, 1994).

Defense Corporate Information Management

Defense IRM: Strategy Needed for Logistics Information Technology Improvement Efforts (GAO/AIMD-97-6, Nov. 14, 1996).

DOD Accounting Systems: Efforts to Improve Systems for Navy Need Overall Structure (GAO/AIMD-96-99, Sept. 30, 1996).

Defense IRM: Critical Risks Facing New Materiel Management Strategy (GAO/AIMD-96-109, Sept. 6, 1996).

Defense Transportation: Migration Systems Selected Without Adequate Analysis (GAO/AIMD-96-81, Aug. 29, 1996).

Defense Management: Selection of Depot Maintenance Standard System Not Based on Sufficient Analyses (GAO/AIMD-95-110, July 13, 1995).

Defense Management: Impediments Jeopardize Logistics Corporate Information Management (GAO/NSIAD-95-28, Oct. 21, 1994).

Defense Management: Stronger Support Needed for Corporate Information Management Initiative to Succeed (GAO/AIMD/NSIAD-94-101, April 12, 1994).

National Weather Service Modernization

NOAA Satellites (GAO/AIMD-96-141R, Sept. 13, 1996).

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

Weather Forecasting: New Processing System Faces Uncertainties and Risks (GAO/T-AIMD-96-47, Feb. 29, 1996).

Weather Forecasting: NWS Has Not Demonstrated That New Processing System Will Improve Mission Effectiveness (GAO/AIMD-96-29, Feb. 29, 1996).

Weather Forecasting: Radars Far Superior to Predecessors, but Location and Availability Questions Remain (GAO/T-AIMD-96-2, Oct. 17, 1995).

Weather Service Modernization Staffing (GAO/AIMD-95-239R, Sept. 26, 1995).

Weather Forecasting: Radar Availability Requirements Not Being Met (GAO/AIMD-95-132, May 31, 1995).

Weather Forecasting: Unmet Needs and Unknown Costs Warrant Reassessment of

Observing System Plans (GAO/AIMD-95-81, April 21, 1995).

Weather Service Modernization Questions (GAO/AIMD-95-106R, March 10, 1995).

Weather Service Modernization: Despite Progress, Significant Problems and Risks Remain (GAO/T-AIMD-95-87, Feb. 21, 1995).

Meteorological Satellites (GAO/NSIAD-95-87R, Feb. 6, 1995).

Weather Forecasting: Improvements Needed in Laboratory Software Development Processes (GAO/AIMD-95-24, Dec. 14, 1994).

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

Weather Forecasting: Important Issues on Automated Weather Processing System Need Resolution (GAO/IMTEC-93-12BR, Jan. 6, 1993).

Information Security

Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, Sept. 24, 1996).

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements (GAO/AIMD-96-101, July 11, 1996).

Information Security: Computer Hacker Information Available on Internet (GAO/T-AIMD-96-108, June 5, 1996).

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

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996).

Security Weaknesses at IRS' Cyberfile Data Center (GAO/AIMD-96-85R, May 9, 1996).

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1994 and 1993 (GAO/AIMD-96-22, Feb. 26, 1996).

Department of Energy: Procedures Lacking To Protect Computerized Data (GAO/AIMD-95-118, June 5, 1995).

Information Superhighway: An Overview of Technology Challenges (GAO/AIMD-95-23, Jan. 23, 1995).

Financial Audit: Examination of Customs' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-119, June 15, 1994).

HUD Information Resources: Strategic Focus and Improved Management Controls Needed (GAO/AIMD-94-34, April 14, 1994).

IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, Sept. 22, 1993).

1997 High-Risk Series

An Overview (GAO/HR-97-1)

Quick Reference Guide (GAO/HR-97-2)

Defense Financial Management (GAO/HR-97-3)

Defense Contract Management (GAO/HR-97-4)

Defense Inventory Management (GAO/HR-97-5)

Defense Weapon Systems Acquisition (GAO/HR-97-6)

Defense Infrastructure (GAO/HR-97-7)

IRS Management (GAO/HR-97-8)

Information Management and Technology (GAO/HR-97-9)

Medicare (GAO/HR-97-10)

Student Financial Aid (GAO/HR-97-11)

Department of Housing and Urban Development (GAO/HR-97-12)

Department of Energy Contract Management (GAO/HR-97-13)

Superfund Program Management
(GAO/HR-97-14)

The entire series of 14 high-risk reports can be ordered using the order number GAO/HR-97-20SET.

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 6015
Gaithersburg, MD 20884-6015

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 (301) 258-4066, or TDD (301) 413-0006.

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

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

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100