

GAO

Testimony

Before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10 a.m. EST
Thursday, February 17, 2005

GAO'S 2005 HIGH-RISK UPDATE

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





Highlights of [GAO-05-350T](#), a testimony to the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

GAO's audits and evaluations identify federal programs and operations that, in some cases, are high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement. Increasingly, GAO also is identifying high-risk areas to focus on the need for broad-based transformations to address major economy, efficiency, or effectiveness challenges. Since 1990, GAO has periodically reported on government operations that it has designated as high risk. In this 2005 update for the 109th Congress, GAO presents the status of high-risk areas identified in 2003 and new high-risk areas warranting attention by the Congress and the administration. Lasting solutions to high-risk problems offer the potential to save billions of dollars, dramatically improve service to the American public, strengthen public confidence and trust in the performance and accountability of the federal government, and ensure the ability of government to deliver on its promises.

What GAO Recommends

This testimony contains GAO's views on what remains to be done for each high-risk area to bring about lasting solutions. Persistence and perseverance by the administration in implementing GAO's recommended solutions and continued oversight and action by the Congress are both essential.

www.gao.gov/cgi-bin/getrpt?GAO-05-350T.

To view the full product, click on the link above. For more information, contact George Stalcup at (202) 512-9490 or stalcupg@gao.gov.

GAO'S 2005 HIGH-RISK UPDATE

What GAO Found

In January 2003, GAO identified 25 high-risk areas; in July 2003, a 26th high-risk area was added to the list. Since then, progress has been made in all areas, although the nature and significance of progress varies by area. Federal departments and agencies, as well as the Congress, have shown a continuing commitment to addressing high-risk challenges and have taken various steps to help correct several of the problems' root causes. GAO has determined that sufficient progress has been made to remove the high-risk designation from three areas: student financial aid programs, FAA financial management, and Forest Service financial management. Also, four areas related to IRS have been consolidated into two areas.

This year, GAO is designating four new high-risk areas. The first new area is establishing appropriate and effective information-sharing mechanisms to improve homeland security. Federal policy creates specific requirements for information-sharing efforts, including the development of processes and procedures for collaboration between federal, state, and local governments and the private sector. This area has received increased attention but the federal government still faces formidable challenges sharing information among stakeholders in an appropriate and timely manner to reduce risk.

The second and third new areas are, respectively, DOD's approach to business transformation and its personnel security clearance program. GAO has reported on inefficiencies and inadequate transparency and accountability across DOD's major business areas, resulting in billions of dollars of wasted resources. Senior leaders have shown commitment to business transformation through individual initiatives in acquisition reform, business modernization, and financial management, among others, but little tangible evidence of actual improvement has been seen in DOD's business operations to date. DOD needs to take stronger steps to achieve and sustain business reform on a departmentwide basis. Further, delays by DOD in completing background investigations and adjudications can affect the entire government because DOD performs this function for hundreds of thousands of industry personnel from 22 federal agencies, as well as its own service members, federal civilian employees, and industry personnel. OPM is to assume DOD's personnel security investigative function, but this change alone will not reduce the shortages of investigative personnel.

The fourth area is management of interagency contracting. Interagency contracts can leverage the government's buying power and provide a simplified and expedited method of procurement. But several factors can pose risks, including the rapid growth of dollars involved combined with the limited expertise of some of agencies in using these contracts and recent problems related to their management. Various improvement efforts have been initiated to address this area, but improved policies and processes, and their effective implementation, are needed to ensure that interagency contracting achieves its full potential in the most effective and efficient manner.

GAO's 2005 High-Risk List

2005 High-Risk Areas

Addressing Challenges In Broad-based Transformations

- Strategic Human Capital Management^a
- U.S. Postal Service Transformation Efforts and Long-Term Outlook^a
- Managing Federal Real Property^a
- Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures
- Implementing and Transforming the Department of Homeland Security
- Establishing Appropriate And Effective Information-Sharing Mechanisms to Improve Homeland Security
- DOD Approach to Business Transformation^a
 - DOD Business Systems Modernization
 - DOD Personnel Security Clearance Program
 - DOD Support Infrastructure Management
 - DOD Financial Management
 - DOD Supply Chain Management (formerly Inventory Management)
 - DOD Weapon Systems Acquisition

Managing Federal Contracting More Effectively

- DOD Contract Management
- DOE Contract Management
- NASA Contract Management
- Management of Interagency Contracting

Assessing the Efficiency and Effectiveness of Tax Law Administration

- Enforcement of Tax Laws^{a, b}
- IRS Business Systems Modernization^c

Modernizing and Safeguarding Insurance and Benefit Programs

- Modernizing Federal Disability Programs^a
- Pension Benefit Guaranty Corporation Single-Employer Insurance Program^a
- Medicare Program^a
- Medicaid Program^a
- HUD Single-Family Mortgage Insurance and Rental Housing Assistance Programs

Other

- FAA Air Traffic Control Modernization

Source: GAO.

^aLegislation is likely to be necessary, as a supplement to actions by the executive branch, in order to effectively address this high-risk area.

^bTwo high-risk areas—Collection of Unpaid Taxes and Earned Income Credit Noncompliance—have been consolidated to make this area.

^cThe IRS Financial Management high-risk area has been incorporated into this high-risk area.

Mr. Chairman, Senator Akaka, Members of the Subcommittee:

Thank you for the opportunity to discuss GAO's 2005 high-risk update report. As you know, we periodically assemble our work for the Congress in ways we hope will help in its budget and programmatic deliberations, as well as oversight and legislative activities. The "high-risk" program was begun in 1990 under the direction of my immediate predecessor, the Honorable Charles A. Bowsher. Beginning in 1993, we have been updating this report at the onset of each new Congress. This effort, which is actively supported by your Subcommittee, as well as the full Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Government Reform, has brought a much needed focus to problems that are impeding effective government and costing the government billions of dollars each year. In fact, Chairman Voinovich and Senator Akaka, our 2005 high-risk update was issued on January 25, 2005, at a press briefing that the chairs and ranking members of our Senate and House oversight committees, as well as both of you, attended.

As this Subcommittee knows, we have made hundreds of recommendations to improve these high-risk operations. Moreover, our focus on high-risk problems contributed to the Congress's enacting a series of governmentwide reforms to address critical human capital challenges, strengthen financial management, improve information technology practices, and instill a more results-oriented government. Our high-risk status reports are provided at the start of each new Congress. This update should help you and other Members of Congress carry out your responsibilities while improving the federal government's performance and enhancing its accountability for the benefit of the American people.

During my tenure as Comptroller General, our high-risk program has increasingly focused on those major programs and operations that need urgent attention and transformation in order to ensure that our national government functions in the most economical, efficient, and effective manner possible. As in prior updates, federal programs and operations are also emphasized when they are at high risk because of their greater vulnerabilities to fraud, waste, abuse, and mismanagement.

Our report summarizes (1) progress made in correcting high-risk problems, (2) actions under way, and (3) further actions that we believe are needed. In this update, we determined that sufficient progress had been made to remove the high-risk designation from three areas, and we designated four

new areas as high risk. In addition, several prior high-risk areas have been consolidated or modified.

Our objective for the high-risk list is to bring “light” to these areas as well as “heat” to prompt needed “actions.” The Bush Administration has looked to our high-risk program to help shape various governmentwide initiatives such as the President’s Management Agenda, which has at its base many of the areas we had previously designated as high risk. To its credit, the Office of Management and Budget (OMB) has worked closely with a number of agencies that have high-risk issues, in many cases establishing action plans and milestones for agencies to complete needed actions to address areas that we have designated as high risk. In this regard, Clay Johnson, OMB’s Deputy Director for Management, recently reaffirmed the Bush Administration’s desire to refocus on GAO’s high-risk list in order to make as much progress as possible in the President’s second term. This is very encouraging. However, continued oversight by the Congress will also be key, and in the case of some areas, legislative actions will be needed.

Just yesterday, we issued another report entitled *21st Century Challenges: Reexamining the Base of the Federal Government* ([GAO-05-325SP](#)), which presented a number of illustrative questions for the Congress and other policy makers to consider as they carry out their various constitutional responsibilities. These questions span a broad range of budget categories and federal operations, including discretionary and mandatory spending, and tax policies and programs. We hope that this new report, along with the high-risk report, will be used by various congressional committees as they consider which areas of government need particular attention and reconsideration. In the final analysis, only elected officials can decide whether, when, and how best to proceed to address these important issues.

High-Risk Designations Removed

For this 2005 high-risk update, we determined that three high-risk areas warranted removal from the list because of progress made. They are the Department of Education’s (Education) Student Financial Aid Programs, Federal Aviation Administration (FAA) Financial Management, and the Department of Agriculture’s (USDA) Forest Service Financial Management. We will, however, continue to monitor these programs, as appropriate, to ensure that the improvements we have noted are sustained.

Student Financial Aid Programs

In 1990, we designated student financial aid programs as high risk. Since then, in intervening high-risk updates, we reported various problems, including poor financial management and weak internal controls, fragmented and inefficient information systems, and inadequate attention to program integrity as evidenced by high default rates and the numbers of ineligible students participating in the programs. In 1998, the Congress established Education's Office of Federal Student Aid (FSA) as the government's first performance-based organization, thus giving it greater flexibility to better address long-standing management weaknesses within student aid programs. In 2001, Education created a team of senior managers dedicated to addressing key financial and management problems throughout the agency, and in 2002, the Secretary of Education made removal from GAO's high-risk list a specific goal and listed it as a performance measure in Education's strategic plan. We reported in 2003 that Education had made important progress, but that it was too early to determine whether improvements would be sustained and that additional steps needed to be taken in several areas.

Since 2003, Education has sustained improvements in the financial management of student financial aid programs and taken additional steps to address our concerns about systems integration, reporting on defaulted loans, and human capital management. Furthermore, the agency has met many of our criteria for removing the high-risk designation. Education has demonstrated a strong commitment to addressing risks; developed and implemented corrective action plans; and, through its annual planning and reporting processes, monitored the effectiveness and sustainability of its corrective measures. Thus, while FSA needs to continue its progress and take additional steps to fully address some of our recommendations, we are removing the high-risk designation from student financial aid programs.

FSA has sustained improvements to address its financial management and internal control weaknesses. FSA received an unqualified, or "clean," opinion on its financial statements for fiscal years 2002, 2003, and 2004. In addition, the auditors indicated progress in addressing previously identified internal control weaknesses, with no material weaknesses¹

¹ A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that errors, fraud, or noncompliance in amounts that would be material to the financial statements may occur and not be detected promptly by employees in the normal course of performing their duties.

reported in FSA's fiscal year 2003 and 2004 audits. However, the auditors reported that FSA should continue to further strengthen these internal controls, which are related to the calculation and reporting of the loan liability activity and subsidy estimates, as well as its information systems controls. FSA has also established processes to address several previously reported internal control weaknesses that made FSA vulnerable to improper payments in its grant and loan programs. For example, FSA has taken steps to better ensure that grants are not awarded to ineligible students and has implemented a process to identify and investigate schools for possible fraudulent activities or eligibility-related violations. Further, FSA addressed concerns we raised about students who were underreporting family income, by working with OMB and the Department of the Treasury to draft legislation that would permit use of tax information to verify income reported on student aid applications.

FSA has taken further actions toward integrating its many disparate information systems. FSA has developed an integration strategy that focuses on achieving a seamless information exchange environment whereby users—students, educational institutions, and lenders—would benefit from simplified access to the agency's financial aid processes and more consistent and accurate data across its programs. FSA also has made progress toward establishing an enterprise architecture for guiding its systems integration efforts and has begun three efforts for reengineering its information-processing environment, which would consolidate and integrate most of its systems and move it closer to a seamless information exchange environment.

FSA also included action steps for achieving student loan default management goals in its annual plan and has taken steps to help reduce the default rate. In 2003, FSA created a work group that identified over 60 default prevention and management initiatives and established a new organizational unit to focus on mitigating and reducing the risk of loss to the taxpayer from student obligations. FSA added information to its exit counseling guide to help increase borrowers' awareness of the benefits of repaying their loans through electronic debiting accounts and prepayment options. In 2003, FSA reported a cohort default rate of 5.4 percent for 2001, and defaulted loans as a percentage of total outstanding loans declined from 9.4 percent in 2001 to 7.6 percent in 2003.

FSA is taking steps to address its human capital challenges. It developed a comprehensive human capital strategy that includes many of the practices of leading organizations and has addressed many of the issues we

previously raised. For example, FSA identified challenges that it will likely face in coming years, such as likely retirements, and discussed recognized weaknesses, such as the need to develop the skills of staff and maintain the focus of the agency's leadership on human capital issues. FSA has also prepared a succession plan that addresses some of our concerns about the pending retirement of senior employees in key positions across the agency. Additionally, FSA has established several approaches to support staff development by revising its Skills Catalog, which should enable staff to independently plan their professional development; introducing online learning tools; offering a wide variety of internal courses; and providing funds for external courses.

FAA Financial Management

We first designated FAA financial management as high risk in 1999 because the agency lacked accountability for billions of dollars in assets and expenditures due to serious weaknesses in its financial reporting, property, and cost accounting systems. These problems continued through fiscal year 2001, when FAA's financial management system required 850 adjustments totaling \$41 billion in order to prepare FAA's annual financial statements. In addition, at that time, FAA could not accurately and routinely account for property totaling a reported \$11.7 billion, and lacked the cost information necessary for decision making as well as to adequately account for its activities and major projects, such as the air traffic control modernization program. Also, while FAA received an unqualified audit opinion on its fiscal year 2001 financial statements, the auditor's report cited a material internal control weakness related to FAA's lack of accountability for its property and several other internal control weaknesses related to financial management issues.

At the time of our January 2003 high-risk report, FAA had made significant progress in addressing its financial management weaknesses, most importantly through ongoing efforts to develop a new financial management system called Delphi, including an integrated property accounting system, as well as initiatives to develop a new cost accounting system. However, these new systems were still under development and not yet operational. Therefore, it had yet to be seen whether the new systems would resolve the long-standing financial management issues that had resulted in our designation of FAA financial management as high risk. As a result, we retained FAA financial management as a high-risk area, while noting that significant progress was being made.

FAA management has continued to make progress since our January 2003 high-risk report. Subsequent auditors' reports on FAA's financial statements for fiscal years 2002 and 2003 were unqualified, but continued to cite internal control weaknesses, although less severe than in prior years, related to FAA's then existing financial management systems. In fiscal year 2004, FAA implemented its new Delphi general ledger system, including an integrated property accounting system. FAA management was able to prepare financial statements for the fiscal year ended September 30, 2004, using these new systems, and FAA's auditors gave FAA an unqualified opinion on these financial statements. While the auditors reported several internal control weaknesses related to the implementation of the new financial management systems, none of these were considered to be material weaknesses, and FAA management, in responding to the auditor's report, indicated their full commitment to addressing these issues.

While the cost accounting system is still under development, progress has been made. The cost accounting interface with Delphi was completed in fiscal year 2004, and the labor distribution interface is expected to be completed in fiscal year 2005. For the first time, some cost accounting data, while not available on a monthly basis, were available shortly after fiscal-year end for the 12 months ended September 30, 2004. FAA management has demonstrated its commitment to the full implementation of this system, devoting significant planning and resources to its completion and the monitoring of its implementation progress.

While it is important that FAA management continue to place a high priority on the cost system and, more importantly, ultimately use cost information routinely in FAA decision making, FAA's progress in improving financial management overall since our January 2003 high-risk update has been sufficient for us to remove the high-risk designation for FAA financial management.

Forest Service Financial Management

We first designated USDA's Forest Service financial management as high risk in 1999 because the agency lacked accountability over billions of dollars in its two major assets—fund balance with the Department of the Treasury (Treasury) and property, plant, and equipment. Since the Forest Service is a major component of USDA, the lack of accountability over these two major assets contributed to disclaimers of opinions on USDA's consolidated financial statements. In addition, the Forest Service continued to have material weaknesses in its accounting and reporting of accounts receivable and accounts payable. This precluded the agency from

knowing costs it had incurred and amounts owed to others throughout the year. These problems were further exacerbated by problems with the Forest Service's partial implementation of its new financial accounting system. This system was unable to produce certain critical budgetary and accounting reports that track obligations, assets, liabilities, revenues, and costs. Thus, these financial reporting weaknesses hampered management's ability to effectively manage operations, monitor revenue and spending levels, and make informed decisions about future funding needs.

The Forest Service's long-standing financial management deficiencies were also evident in the repeated negative opinions on its financial statements, including adverse opinions in fiscal years 1991, 1992, and 1995. Due to the severity of its 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. However, the Forest Service's pervasive material internal control weaknesses continued to plague the agency. In our 2001 high-risk update, we reported that the USDA Office of Inspector General was unable to determine the accuracy of the Forest Service's reported \$3.1 billion in net property, plant, and equipment, which represented 51 percent of the agency's assets. We also reported that the inspector general was unable to verify fund balances with Treasury totaling \$2.6 billion because the reconciliation of agency records with Treasury records had not been completed. Because of the severity of these and other deficiencies, the inspector general disclaimed from issuing opinions on the Forest Service's financial statements for fiscal years 1997 through 2001. In addition, we noted that the Forest Service's autonomous field structure hampered efforts to correct these accounting and financial reporting deficiencies. We also reported that the Forest Service had implemented its new accounting system agencywide. However, the system depended on and received data from feeder systems that were poorly documented, operationally complex, deficient in appropriate control processes, and costly to maintain.

In our 2003 high-risk report, while we highlighted that the Forest Service continued to have long-standing material control weaknesses, including weaknesses in its fund balance with Treasury and in property, plant, and equipment, we reported that the Forest Service had made progress toward achieving accountability by receiving its first unqualified opinion on its fiscal year 2002 financial statements. Although the Forest Service had reached an important milestone, it had not yet proved it could sustain this outcome, and had not reached the end goal of routinely producing timely,

accurate, and useful financial information. As a result, we retained Forest Service financial management as a high-risk area.

In the past 2 years, the Forest Service has made additional progress, especially with respect to addressing several long-standing material internal control deficiencies. Based on our criteria for removing a high-risk designation, which includes a demonstrated strong commitment, corrective action plan, and progress in addressing deficiencies, we believe the Forest Service's overall improvement in financial management since our January 2003 high-risk update has been sufficient for us to remove Forest Service financial management from the high-risk list at this time. The Forest Service has resolved material deficiencies related to its fund balance with Treasury and in property, plant, and equipment, thus increasing accountability over its billions of dollars in assets, and USDA and the Forest Service received unqualified opinions on their fiscal year 2004 financial statements.

This does not mean that the Forest Service has no remaining challenges. For example, while we recognized its clean opinion for fiscal year 2002 in our last update, subsequently, in fiscal year 2003, these financial statements had to be restated to correct material errors. The Forest Service also received a clean opinion for fiscal year 2003, but these financial statements had to be restated in fiscal year 2004 to again correct material misstatements. Frequent restatements to correct errors can undermine public trust and confidence in both the entity and all responsible parties. Further, the Forest Service continues to have material internal control weaknesses related to financial reporting and information technology security, and its financial management systems do not yet substantially comply with the Federal Financial Management Improvement Act of 1996.

However, the Forest Service has demonstrated a strong commitment to efforts under way or planned, that, if effectively implemented, should help to resolve many of its remaining financial management problems and move it toward sustainable financial management business processes. These efforts are designed to address internal control and noncompliance issues identified in audit reports, as well as organizational issues. For example, during fiscal year 2004, the Forest Service began reengineering and consolidating its finance, accounting, and budget processes. We believe these efforts, if implemented effectively, will provide stronger financial management, sustain positive audit results, and ensure compliance with federal financial reporting standards. Yet, it is important that USDA and Forest Service officials continue to place a high priority on addressing the

Forest Service's remaining financial management problems, and we will continue to monitor its progress.

New High-Risk Areas

Our use of the high-risk designation to draw attention to the challenges associated with the economy, efficiency, and effectiveness of government programs and operations in need of broad-based transformation has led to important progress. We will also continue to identify high-risk areas based on the more traditional focus on fraud, waste, abuse, and mismanagement. Overall, our focus will continue to be on identifying the root causes behind vulnerabilities, as well as actions needed on the part of the agencies involved and, if appropriate, the Congress. For 2005, we have designated the following four new areas as high risk: Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security, Department of Defense (DOD) Approach to Business Transformation, DOD Personnel Security Clearance Program, and Management of Interagency Contracting.

Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security

Information is a crucial tool in fighting terrorism, and the timely dissemination of that information to the appropriate government agency is absolutely critical to maintaining the security of our nation. The ability to share security-related information can unify the efforts of federal, state, and local government agencies, as well as the private sector as appropriate, in preventing or minimizing terrorist attacks.

The 9/11 terrorist attacks heightened the need for comprehensive information sharing. Prior to that time, the overall management of information-sharing activities among government agencies and between the public and private sectors lacked priority, proper organization, coordination, and facilitation. As a result, the existing national mechanisms for collecting threat information, conducting risk analyses, and disseminating warnings were at an inadequate state of development for protecting the United States from coordinated terrorist attacks.

Information sharing for securing the homeland is a governmentwide effort involving multiple federal agencies, including but not limited to the Office of Management and Budget (OMB); the Departments of Homeland Security (DHS), Justice, State, and Defense; and the Central Intelligence Agency. Over the past several years, GAO has identified potential information-sharing barriers, critical success factors, and other key management issues

that should be considered, including the processes, procedures, and systems to facilitate information sharing among and between government entities and the private sector.

Establishing an effective two-way exchange of information to detect, prevent, and mitigate potential terrorist attacks requires an extraordinary level of cooperation and perseverance among federal, state, and local governments and the private sector to establish timely, effective, and useful communications. Since 1998, GAO has recommended the development of a comprehensive plan for information sharing to support critical infrastructure protection efforts. The key components of this recommendation can be applied to broader homeland security and intelligence-sharing efforts, including clearly delineating the roles and responsibilities of federal and nonfederal entities, defining interim objectives and milestones, setting time frames for achieving objectives, and establishing performance measures.

We have made numerous recommendations related to information sharing, particularly as they relate to fulfilling federal critical infrastructure protection responsibilities.² For example, we have reported on the practices of organizations that successfully share sensitive or time-critical information, including establishing trust relationships, developing information-sharing standards and protocols, establishing secure communications mechanisms, and disseminating sensitive information appropriately. Federal agencies have concurred with our recommendations that they develop appropriate strategies to address the many potential barriers to information sharing. However, many federal efforts remain in the planning or early implementation stages.

In the absence of comprehensive information-sharing plans, many aspects of homeland security information sharing remain ineffective and fragmented. Accordingly, we are designating information sharing for homeland security as a governmentwide high-risk area because this area, while receiving increased attention, still faces significant challenges. Since

² GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, [GAO-03-1165T](#) (Washington, D.C.: Sept. 17, 2003); and *Homeland Security: Information-Sharing Responsibilities, Challenges, and Key Management Issues*, [GAO-03-715T](#) (Washington, D.C.: May 8, 2003).

2002, legislation,³ various national strategies, and executive orders have specified actions to improve information sharing for homeland security.

Earlier this month, DHS released an Interim National Infrastructure Protection Plan (NIPP),⁴ which addresses some of the key issues that GAO has previously identified. The DHS plan is intended to provide a consistent, unifying structure for integrating critical infrastructure protection (CIP) efforts into a national program. The interim NIPP identifies key stakeholders and participants in information sharing efforts related to public-private efforts to protect critical infrastructure. In addition, the plan recognizes that information sharing systems can be broadly defined as interactions of people, physical structures, information, and technologies that are designed to ensure that critical, high-quality, and productive knowledge is available to decision makers whenever and wherever it is needed. Further, the plan identifies key responsibilities for DHS, including the development, implementation, and expansion of information-sharing strategies to support infrastructure protection efforts.

The interim plan released by DHS is an important step toward improving information sharing for infrastructure protection efforts; however, extraordinary challenges remain. As the 9/11 Commission recognized, information sharing must be “guided by a set of practical policy guidelines that simultaneously empower and constrain officials, telling them clearly what is and is not permitted.”⁵ While the wide range of executive and legislative branch actions is encouraging, significant challenges remain in developing the required detailed policies, procedures, and plans for sharing homeland security-related information. For example, the Homeland Security Information Sharing Act required procedures for facilitating homeland security information sharing and established authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information. In July 2003, the President assigned these functions to the

³ *The Homeland Security Act of 2002* (P.L. 107-296); the *Intelligence Reform and Terrorism Prevention Act of 2004* (P.L. 108-458).

⁴ U.S. Department of Homeland Security, *Interim National Infrastructure Protection Plan* (Washington D.C.: February 2005).

⁵ National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, D.C.: Government Printing Office, July 22, 2004).

Secretary of Homeland Security,⁶ but no deadline was established for developing information-sharing procedures. Without clear processes and procedures for rapidly sharing appropriate information, the ability of private sector entities to effectively design facility security systems and protocols can be impeded. In addition, the lack of sharing procedures can also limit the federal government's accurate assessment of nonfederal facilities' vulnerability to terrorist attacks.

In December 2004, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required the establishment of (1) an information-sharing environment (ISE) as a means of facilitating the exchange of terrorism information among appropriate federal, state, local, and tribal entities, and the private sector; and (2) an information-sharing council to support the President and the ISE program manager with advice on developing policies, procedures, guidelines, roles, and standards necessary to implement and maintain the ISE. It will be important to ensure that the DHS information-sharing systems are coordinated with those required under the intelligence reform legislation.

Improving the standardization and consolidation of data can also promote better sharing. For example, in 2003 we found that goals, objectives, roles, responsibilities, and mechanisms for information sharing had not been consistently defined by the 9 federal agencies that maintain 12 key terrorist and criminal watch list systems. As a result, efforts to standardize and consolidate appropriate watch list data would be impeded by the existence of overlapping sets of data, inconsistent agency policies and procedures for the sharing of those data, and technical incompatibilities among the various watch list information systems. In addition, 2004 reports from the inspectors general at DHS and the Department of Justice highlight the challenges and slow pace of integrating and sharing information between fingerprint databases.⁷

A great deal of work remains to effectively implement the many actions called for to improve homeland security information sharing, including

⁶ Executive Order 13311: *Homeland Security Information Sharing* (Washington, D.C.: July 29, 2003).

⁷ U.S. Department of Homeland Security, Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, OIG-05-06 (Washington D.C.: December 2004); and U.S. Department of Justice, Office of Inspector General, *Semiannual Report to the Congress: Top Management Challenges* (Washington, D.C.: Nov. 22, 2003).

establishing clear goals, objectives, and expectations for the many participants in information-sharing efforts; and consolidating, standardizing, and enhancing federal structures, policies, and capabilities for the analysis and dissemination of information.

DOD Approach to Business Transformation

DOD spends billions of dollars each year to sustain key business operations that support our forces, including, for example, systems and processes related to human capital policies and practices, acquisition and contract management, financial management, supply chain management, business systems modernization, and support infrastructure management—all of which appear on GAO’s high-risk list. Recent and ongoing military operations in Afghanistan and Iraq and new homeland defense missions have led to newer and higher demands on our forces in a time of growing fiscal challenges for our nation. In an effort to better manage DOD’s resources, the Secretary of Defense has appropriately placed a high priority on transforming force capabilities and key business processes.

For years, we have reported on inefficiencies and the lack of adequate transparency and appropriate accountability across DOD’s major business areas, resulting in billions of dollars of wasted resources annually. Although the Secretary of Defense and senior leaders have shown commitment to business transformation, as evidenced by individual key initiatives related to acquisition reform, business modernization, and financial management, among others, little tangible evidence of actual improvement has been seen in DOD’s business operations to date. Improvements have generally been limited to specific business process areas, such as DOD’s purchase card program, and have resulted in the incorporation of many key elements of reform, such as increased management oversight and monitoring and results-oriented performance measures. However, DOD has not taken the steps it needs to take to achieve and sustain business reform on a broad, strategic, departmentwide, and integrated basis. Among other things, it has not established clear and specific management responsibility, accountability, and control over overall business transformation-related activities and applicable resources. In addition, DOD has not developed a clear strategic and integrated plan for business transformation with specific goals, measures, and accountability mechanisms to monitor progress, or a well-defined blueprint, commonly called an enterprise architecture, to guide and constrain implementation of such a plan. For these reasons, we, for the first time, are designating DOD’s lack of an integrated strategic planning approach to business transformation as high risk.

DOD's current and historical approach to business transformation has not proven effective in achieving meaningful and sustainable progress in a timely manner. As a result, change is necessary in order to expedite the effort and increase the likelihood of success. For DOD to successfully transform its business operations, it will need a comprehensive and integrated business transformation plan; people with needed skills, knowledge, experience, responsibility, and authority to implement the plan; an effective process and related tools; and results-oriented performance measures that link institutional, unit, and individual performance goals and expectations to promote accountability for results. Over the last 3 years, we have made several recommendations that, if implemented effectively, could help DOD move forward in establishing the means to successfully address the challenges it faces in transforming its business operations. For example, we believe that DOD needs a full-time chief management officer (CMO) position, created through legislation, with responsibility, authority, and accountability for DOD's overall business transformation efforts. This is a "good government" matter that should be addressed in a professional and nonpartisan manner. The CMO must be a person with significant authority and experience who would report directly to the Secretary of Defense. Given the nature and complexity of the overall business transformation effort, and the need for sustained attention over a significant period of time, this position should be a term appointment (e.g., 7 years), and the incumbent should be subject to a performance contract. DOD has agreed with many of our recommendations and launched efforts intended to implement many of them, but progress to date has been slow. In my view, it will take the sustained efforts of a CMO, as we have proposed, to make the needed progress in transforming DOD's business operations.

DOD Personnel Security Clearance Program

Delays in completing hundreds of thousands of background investigations and adjudications (a review of investigative information to determine eligibility for a security clearance) have led us to add the DOD personnel security clearance program to our 2005 high-risk list. Personnel security clearances allow individuals to gain access to classified information that, in some cases, could reasonably be expected to cause exceptionally grave damage to national defense or foreign relations through unauthorized disclosure. Worldwide deployments, contact with sensitive equipment, and other security requirements have resulted in DOD's having approximately 2 million active clearances. Problems with DOD's personnel security clearance process can have repercussions throughout the government because DOD conducts personnel security investigations and adjudications

for industry personnel from 22 other federal agencies, in addition to performing such functions for its own service members, federal civilian employees, and industry personnel. While our work on the clearance process has focused on DOD, clearance delays in other federal agencies suggest that similar impediments and their effects may extend beyond DOD.

Since at least the 1990s, we have documented problems with DOD's personnel security clearance process, particularly problems related to backlogs and the resulting delays in determining clearance eligibility. Since fiscal year 2000, DOD has declared its personnel security clearance investigations program to be a systemic weakness—a weakness that affects more than one DOD component and may jeopardize the department's operations—under the Federal Managers' Financial Integrity Act of 1982. An October 2002 House Committee on Government Reform report also recommended including DOD's adjudicative process as a material weakness. As of September 30, 2003 (the most recent data available), DOD could not estimate the full size of its backlog, but we identified over 350,000 cases exceeding established time frames for determining eligibility.

The negative effects of delays in determining security clearance eligibility are serious and vary depending on whether the clearance is being renewed or granted to an individual for the first time. Delays in renewing previously issued clearances can lead to heightened risk of national security breaches because the longer individuals hold a clearance, the more likely they are to be working with critical information and systems. Delays in issuing initial clearances can result in millions of dollars of additional costs to the federal government, longer periods of time needed to complete national security-related contracts, lost-opportunity costs if prospective employees decide to work elsewhere rather than wait to get a clearance, and diminished quality of the work because industrial contractors may be performing government contracts with personnel who have the necessary security clearances but are not the most experienced and best-qualified personnel for the positions involved.

DOD has taken steps—such as hiring more adjudicators and authorizing overtime for adjudicative staff—to address the backlog, but a significant shortage of trained federal and private-sector investigative personnel presents a major obstacle to timely completion of cases. Other impediments to eliminating the backlog include the absence of an integrated, comprehensive management plan for addressing a wide variety

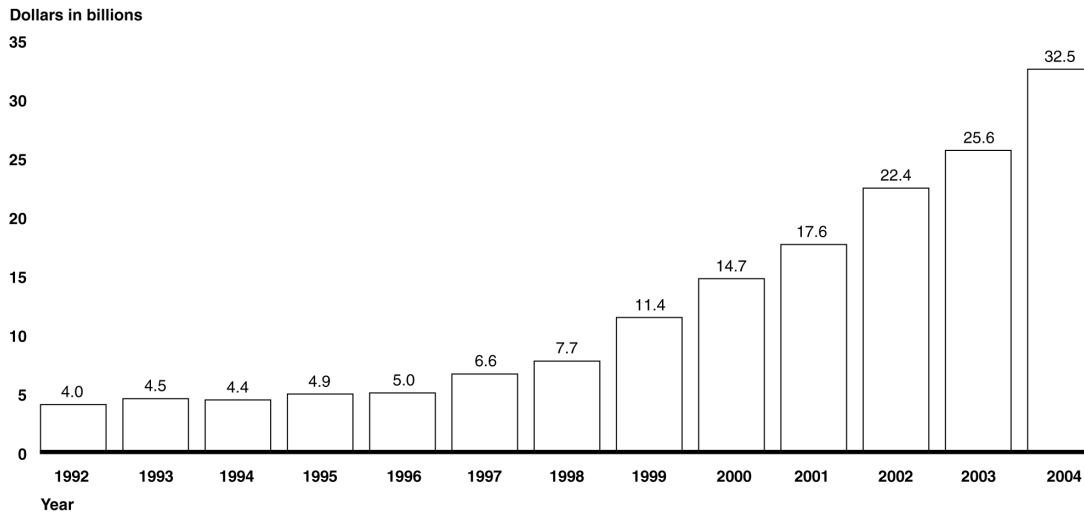
of problems identified by us and others. In addition to matching adjudicative staff to workloads and working with the Office of Personnel Management (OPM) to develop an overall management plan, DOD needs to develop and use new methods for forecasting clearance needs and monitoring backlogs, eliminate unnecessary limitations on reciprocity (the acceptance of a clearance and access granted by another department, agency, or military service), determine the feasibility of implementing initiatives that could decrease the backlog and delays, and provide better oversight for all aspects of its personnel security clearance process.

The National Defense Authorization Act for Fiscal Year 2004 authorized the transfer of DOD's personnel security investigative function and over 1,800 investigative employees to OPM. The transfer is scheduled to take place this month. While the transfer would eliminate DOD's responsibility for conducting the investigations, it would not eliminate the shortage of trained investigative personnel needed to address the backlog. Although DOD would retain the responsibility for adjudicating clearances, OPM would be accountable for ensuring that investigations are completed in a timely manner.

Management of Interagency Contracting

In recent years, federal agencies have been making a major shift in the way they procure many goods and services. Rather than spending a great deal of time and resources contracting for goods and services themselves, they are making greater use of existing contracts already awarded by other agencies. These contracts are designed to leverage the government's aggregate buying power and provide a much-needed simplified method for procuring commonly used goods and services. Thus, their popularity is gaining quickly. The General Services Administration (GSA) alone, for example, has seen a nearly tenfold increase in interagency contract sales since 1992, pushing the total sales mark up to \$32 billion (see fig. 1). Other agencies, such as the Department of the Treasury and the National Institutes of Health, also sponsor interagency contracts.

Figure 1: Multiple Award Schedule Sales, Fiscal Years 1992 through 2004



Source: GSA data.

Note: Dollar amounts are then-year dollars.

These contract vehicles offer the benefits of improved efficiency and timeliness; however, they need to be effectively managed. If they are not properly managed, a number of factors can make these interagency contract vehicles high risk in certain circumstances: (1) they are attracting rapid growth of taxpayer dollars; (2) they are being administered and used by some agencies that have limited expertise with this contracting method; and (3) they contribute to a much more complex environment in which accountability has not always been clearly established. Use of these contracts, therefore, demands a higher degree of business acumen and flexibility on the part of the federal acquisition workforce than in the past. This risk is widely recognized, and the Congress and executive branch agencies have taken several steps to address it. However, the challenges associated with these contracts, recent problems related to their management, and the need to ensure that the government effectively implements measures to bolster oversight and control so that it is well positioned to realize the value of these contracts, warrants designation of interagency contracting as a new high-risk area.

Interagency contracts are awarded under various authorities and can take many forms. Typically, they are used to provide agencies with commonly used goods and services, such as office supplies or information technology services. Agencies that award and administer interagency contracts usually

charge a fee to support their operations. These types of contracts have allowed customer agencies to meet the demands for goods and services at a time when they face growing workloads, declines in the acquisition workforce, and the need for new skill sets.

Our work, together with that of some agency inspectors general, has revealed instances of improper use of interagency contracts. For example, we recently reviewed contracts and task orders awarded by DOD and found some task orders under the GSA schedules that did not satisfy legal requirements for competition because the work was not within the scope of the underlying contracts.⁸ Similarly, the inspector general for the Department of the Interior found that task orders for interrogators and other intelligence services in Iraq were improperly awarded under a GSA schedule contract for information technology services.⁹ More broadly, the GSA inspector general conducted a comprehensive review of the contracting activities of GSA's Federal Technology Service (FTS), an entity that provides contracting services for agencies across the government, and reported that millions of dollars in fiscal year 2003 awards did not comply with laws and regulations.¹⁰ Administration officials have acknowledged that the management of interagency contracting needs to be improved.

Interagency contracting is being used more in conjunction with purchases of services, which have increased significantly over the past several years and now represent over half of federal contract spending. Agencies also are buying more sophisticated or complex services, particularly in the areas of information technology and professional and management support. In many cases, interagency contracts provide agencies with easy access to these services, but purchases of services require different approaches in describing requirements, obtaining competition, and overseeing contractor performance than purchases of goods. In this regard, we and others have reported on the failure to follow prescribed procedures designed to ensure fair prices when using schedule contracts to acquire services. At DOD, the

⁸ GAO, *Rebuilding Iraq: Fiscal Year 2003 Contract Award Procedures and Management Challenges*, [GAO-04-605](#) (Washington, D.C.: June 1, 2004).

⁹ U.S. Department of the Interior, Office of the Inspector General, *Review of 12 Procurements Placed Under General Services Administration Federal Supply Schedules 70 and 871 by the National Business Center* (Washington, D.C.: 2004).

¹⁰ U.S. General Services Administration, Office of the Inspector General, *Compendium of Audits of the Federal Technology Service's Regional Client Support Centers* (Washington, D.C.: 2004).

largest customer for interagency contracts, we found that competition requirements were waived for a significant percentage of supply schedule orders we reviewed, frequently based on an expressed preference to retain the services of incumbent contractors. DOD concurred with our recommendations to develop guidance for the conditions under which waivers of competition may be used, require documentation to support waivers, and establish approval authority based on the value of the orders.¹¹

There are several causes of the deficiencies we and others have found in the use of interagency contracts, including the increasing demands on the acquisition workforce, insufficient training, and in some cases inadequate guidance. Two additional factors are worth noting. First, the fee-for-service arrangement creates an incentive to increase sales volume in order to support other programs of the agency that awards and administers an interagency contract. This may lead to an inordinate focus on meeting customer demands at the expense of complying with required ordering procedures. Second, it is not always clear where the responsibility lies for such critical functions as describing requirements, negotiating terms, and conducting oversight. Several parties—the requiring agency, the ordering agency, and in some cases the contractor—are involved with these functions. But, as the number of parties grows, so too does the need to ensure accountability.

The Congress and the administration have taken several steps to address the challenges of interagency contracting. In 2003, the Congress sought to improve contract oversight and execution by enacting the Services Acquisition Reform Act. The act created a new chief acquisition officer position in many agencies and enhanced workforce training and recruitment. More recently, the Congress responded to the misuse of interagency contracting by requiring more intensive oversight of purchases under these contracts. In July 2004, GSA launched “Get It Right,” an oversight and education program, to ensure that its largest customer, DOD, and other federal agencies properly use GSA’s interagency contracts and its acquisition assistance services. Through this effort, GSA seeks to demonstrate a strong commitment to customer agencies’ compliance with federal contracting regulations and, among other things, improve processes to ensure competition, integrity, and transparency. Additionally, to address

¹¹ GAO, *Contract Management: Guidance Needed to Promote Competition for Defense Task Orders*, [GAO-04-874](#) (Washington, D.C.: July 30, 2004).

workforce issues, OMB, GSA, and DOD officials have said they are developing new skills assessments, setting standards for the acquisition workforce, and coordinating training programs aimed at improving the capacity of the federal acquisition workforce to properly handle the growing and increasingly complex workload of service acquisitions.

These recent actions are positive steps toward improving management of interagency contracting, but, as with other areas, some of these actions are in their early stages and others are still under development. In addition, it is too early to tell whether all of the corrective actions will be effectively implemented, although a recent limited review by the GSA inspector general found some improvement at FTS from enhanced management controls. Our work on major management challenges indicates that specific and targeted approaches are also needed to address interagency contracting risks across the government. Ensuring the proper use of interagency contracts must be viewed as a shared responsibility of all parties involved. But this requires that specific responsibilities be more clearly defined. In particular, to facilitate effective purchasing through interagency contracts, and to help ensure the best value of goods and services, agencies must clarify roles and responsibilities and adopt clear, consistent, and enforceable policies and processes that balance the need for customer service against the requirements of contract regulations. Internal controls and appropriate performance measures help ensure that policies and processes are implemented and have the desired outcomes.

In addition, to be successful, efforts to improve the contracting function must be linked to agency strategic plans. As with other governmentwide high-risk areas, such as human capital and information security, effectively addressing interagency contract management challenges will require agency management to commit the necessary time, attention, and resources, as well as the executive branch and the Congress to enhance their oversight. Making these investments has the potential to improve the government's ability to acquire high-quality goods and services in an efficient and effective manner, resulting in reduced costs, improved service delivery, and strengthened public trust.

Emerging Areas

In addition to specific areas that we have designated as high risk, there are other important broad-based challenges facing our government that are serious and merit continuing close attention. One area of increasing concern involves the need for the completion of comprehensive national threat and risk assessments in a variety of areas. For example, emerging

requirements from the changing security environment, coupled with increasingly limited fiscal resources across the federal government, emphasize the need for agencies to adopt a sound approach to establishing realistic goals, evaluating and setting priorities, and making difficult resource decisions. We have advocated a comprehensive threat and/or risk management approach as a framework for decision making that fully links strategic goals to plans and budgets, assesses values and risks of various courses of action as a tool for setting priorities and allocating resources, and provides for the use of performance measures to assess outcomes. Most prominently, two federal agencies with significant national security responsibilities—DHS and DOD—are still in the beginning stages of adopting a risk-based strategic framework for making important resource decisions involving billions of dollars annually. This lack of a strategic framework for investment decisions is one of the reasons that implementing and transforming DHS, and DOD’s approach to business transformation, have been designated as high-risk areas. At the same time, this threat/risk assessment concept can be applied to a broad range of existing federal government programs, functions, and activities.

The relatively new DHS, with an annual budget of over \$40 billion, has not completed risk assessments mandated by the Homeland Security Act of 2002 to set priorities to help focus its resources where most needed. In performing its duties to protect the nation’s critical infrastructure, DHS has not made clear the link between risk assessment and resource allocation, for example, what criteria it initially used to select assets of national importance and the basic strategy it uses to determine which assets warrant additional protective measures, and by how much these measures could reduce the risk to the nation. We have reviewed the work of several of DHS’s component agencies that have taken some initial steps towards risk management, but much remains to be done. DHS’s Immigration and Customs Enforcement (ICE), as a first step toward developing budget requests and workforce plans for fiscal year 2007 and beyond, has had its Office of Investigations field offices conduct baseline threat assessments to help identify risks. However, performance measures to assess how well a particular threat has been addressed were not used for workforce planning in ICE’s fiscal year 2006 budget request. DHS’s Customs and Border Protection (CBP) has taken steps to address the terrorism risks posed by oceangoing cargo containers. However, CBP has not performed a comprehensive set of assessments vital for determining the level of risk for oceangoing cargo containers and the types of responses necessary to mitigate that risk. The need to use a risk management approach has been a recurring theme in our previous work in transportation security. We

reported in 2003 that DHS's Transportation Security Administration (TSA) planned to adopt a risk management approach. To date, including in our most recent work on general aviation security, we have found that TSA has not fully integrated this approach, which includes assessments of threat, vulnerability, and criticality, to help it prioritize its efforts. As a result, we have recommended that TSA continue its efforts to integrate a risk management approach into its processes.

DOD, with an annual budget of over \$400 billion, exclusive of supplemental funding, is in the process of transforming its force capabilities and business processes. We have reported on limitations in DOD's strategic planning and budgeting, including the use of overly optimistic assumptions in estimating funding needs, often resulting in a mismatch between programs and budgets. In its strategic plan—the September 2001 Quadrennial Defense Review—DOD outlined a new risk management framework consisting of four dimensions of risk—force management, operational, future challenges, and institutional—to use in considering trade-offs among defense objectives and resource constraints. According to DOD, these risk areas are to form the basis for DOD's annual performance goals. They will be used to track performance results and will be linked to planning and resource decisions. As of December 2004, DOD was still in the process of implementing this approach departmentwide. It also remains unclear how DOD will use this approach to measure progress in achieving business and force transformation.

We believe that instilling a disciplined approach to identifying and managing risk has broad applicability across a wide range of federal programs, operations, and functions throughout the federal government. This will be a continuing focus of our work in the future. More generally, we will also continue to monitor other management challenges identified through our work, including those discussed in our January 2003 *Performance and Accountability Series: Major Management Challenges and Program Risks* (GAO-03-95 through GAO-03-118). While not high risk at this time, these challenges warrant continued attention. For example, at the U.S. Census Bureau, a number of operational and managerial challenges loom large as the agency approaches its biggest enumeration challenge yet, the 2010 Census. The Census Bureau will undertake an important census test and make critical 2010 Census operational and design decisions in the coming months—and we will continue to closely monitor these challenges to assist the Congress in its oversight and the Census Bureau in its decision making.

Progress Being Made in Other High-Risk Areas

For other areas that remain on our 2005 high-risk list, there have been important but varying levels of progress, although not yet enough progress to remove these areas from the list. Top administration officials have expressed their commitment to maintaining momentum in seeing that high-risk areas receive adequate attention and oversight. Since our 2003 high-risk report, OMB has worked closely with a number of agencies that have high-risk issues, in many cases establishing action plans and milestones for agencies to complete needed actions to address areas that we have designated as high risk. Such a concerted effort by agencies and ongoing attention by OMB are critical; our experience over the past 15 years has shown that perseverance is required to fully resolve high-risk areas. The Congress, too, will continue to play an important role through its oversight and, where appropriate, through legislative action targeted at the problems and designed to address high-risk areas. Examples of areas where noticeable progress has been made include the following:

- **Strategic Human Capital Management.** Recognizing that federal agencies must transform their organizations to meet the new challenges of the 21st century and that their most important asset in this transformation is their people, we first added human capital management as a governmentwide high-risk issue in January 2001 to help focus attention and resources on the need for fundamental human capital reform requiring both administrative and legislative action. Since then, the Congress and the agencies have made more progress in revising and redesigning human capital policies, processes, and systems than in the previous quarter century. The Congress has called on agencies to do a better and faster job of hiring the right people with the right skills to meet their critical missions, such as protecting the homeland, and gave the agencies new flexibilities to meet this challenge. The Congress has also granted agencies, such as DOD and DHS, unprecedented flexibility to redesign their human capital systems, including designing new classification and compensation systems, which could serve as models for governmentwide change. Therefore, effectively designing and implementing any resulting human capital systems will be of critical importance not just for these agencies, but for overall civil service reform. As part of the President's Management Agenda, the administration has also made strategic human capital management one of its top five priorities and established a system for holding agencies accountable for achieving this change. Some agencies have begun to assess their future workforce needs and implement available flexibilities to meet those needs. As a result of the ongoing

significant changes in how the federal workforce is managed, there is general recognition that there should be a framework to guide human capital reform built on a set of beliefs that entail fundamental principles and boundaries that include criteria and processes that establish checks and limitations when agencies seek and implement their authorities.

- **Federal Real Property.** Since January 2003, the administration has taken several key steps to address long-standing problems in managing federal real property. First, in an effort to provide a governmentwide focus on federal real property issues, the President added the Federal Asset Management Initiative to the President's Management Agenda and signed Executive Order 13327 in February 2004. Under the order, agencies are to designate a senior real property officer to, among other things, identify and categorize owned and leased real property managed by the agency and develop agency asset management plans. Agencies such as DOD and the Department of Veterans Affairs (VA) have taken other actions—DOD is preparing for a round of base realignments and closures in 2005, and in May 2004, VA announced a wide range of asset realignment decisions. These and other efforts are positive steps, but it is too early to judge whether the administration's focus on this area will have a lasting impact. The underlying conditions and related obstacles that led to our high-risk designation continue to exist. Remaining obstacles include competing stakeholder interests in real property decisions; various legal and budget-related disincentives to optimal, businesslike, real property decisions; and the need for better capital planning among agencies.

Other areas in which improvements have been shown include the Postal Service's transformation efforts and long-term outlook, modernizing federal disability programs, the Medicaid program, HUD's Single-Family Mortgage Insurance and Rental Housing Assistance programs, and the implementation and transformation of DHS.

Consolidation of High-Risk Areas

Collection of Unpaid Taxes and Earned Income Credit Noncompliance

We have combined our previous Collection of Unpaid Taxes and Earned Income Credit Noncompliance high-risk areas into an area titled Enforcement of Tax Laws. Collection of unpaid taxes was included in the first high-risk series report in 1990, with a focus on the backlog of uncollected debts owed by taxpayers. In 1995, we added Filing Fraud as a separate high-risk area, narrowing the focus of that high-risk area in 2001 to Earned Income Credit Noncompliance because of the particularly high incidence of fraud and other forms of noncompliance in that program. We expanded our concern about the Collection of Unpaid Taxes in our 2001 high-risk report to include not only unpaid taxes (including tax evasion and unintentional noncompliance) known to the Internal Revenue Service (IRS), but also the broader enforcement issue of unpaid taxes that IRS has not detected. We made this change because of declines in some key IRS collection actions as well as IRS's lack of information about whether those declines had affected voluntary compliance. Although the Congress dedicated a specific appropriation for Earned Income Credit compliance initiatives (both to curb noncompliance and encourage participation) in fiscal years 1998 through 2003, with the 2004 budget the Congress returned to appropriating a single amount for IRS to allocate among its various tax law enforcement efforts.

In recent years, the resources IRS has been able to dedicate to enforcing the tax laws have declined, while IRS's enforcement workload—measured by the number of taxpayer returns filed—has continually increased. As a result, nearly every indicator of IRS's coverage of its enforcement workload has declined in recent years. Although in some cases workload coverage has increased, overall IRS's coverage of known workload is considerably lower than it was just a few years ago. Although many suspect that these trends have eroded taxpayers' willingness to voluntarily comply—and survey evidence suggests this may be true—the cumulative effect of these trends is unknown because new research into the level of individual taxpayer compliance is only now being completed by IRS after a long hiatus. Based on this new research, in 2005, IRS intends to release a new estimate of noncompliance and begin to use this research to improve targeting of enforcement and other compliance resources.

Further, IRS's workload has grown ever more complex as the tax code has grown more complex. Complexity creates a fertile ground for those intentionally seeking to evade taxes and often trips others into inadvertent noncompliance. IRS is challenged to administer and explain each new provision, thus absorbing resources that otherwise might be used to enforce the tax laws.

At the same time, other areas of particularly serious noncompliance have gained the attention of IRS and the Congress—such as abusive tax shelters and schemes employed by businesses and wealthy individuals that often involve complex transactions that may span national boundaries. Given the broad decline in IRS's enforcement workforce, the resulting decreased ability to follow up on suspected noncompliance, the emergence of sophisticated evasion concerns, and the unknown effect of these trends on voluntary compliance, IRS is challenged on virtually all fronts in attempting to ensure that taxpayers fulfill their obligations. IRS's success in overcoming these challenges becomes ever more important in light of the nation's large and growing fiscal pressures. Accordingly, we believe the focus of concern on the enforcement of tax laws is not confined to any one segment of the taxpaying population or any single tax provision. Our designation of the enforcement of tax laws as a high-risk area embodies this broad concern.

IRS Business Systems Modernization and IRS Financial Management

IRS has long relied on obsolete automated systems for key operational and financial management functions, and its attempts to modernize these aging computer systems span several decades. This long history of continuing delays and design difficulties and their significant impact on IRS's operations led us to designate IRS's systems modernization activities and its financial management as high-risk areas in 1995. Since that time, IRS has made progress in improving its financial management, such as enhancing controls over hard copy tax receipts and data and budgetary activity, and improving the accuracy of property records. Additionally, for the past 5 years, IRS has received clean audit opinions on its annual financial statements and, for the past 3 years, has been able to achieve these opinions within 45 days of the end of the fiscal year. However, IRS still needs to replace its outdated financial management systems as part of its business systems modernization program. Accordingly, since the resolution of IRS's remaining most serious and intractable financial management problems largely depends upon the success of IRS's business systems modernization efforts, and since we have continuing concerns related to

this program, we are combining our two previous high-risk areas into one IRS Business Systems Modernization high-risk area.

Major Management Challenges at Federal Agencies

We recently compiled lists of products issued since January 2003 related to the major management challenges identified in the 2003 Performance and Accountability Series. These lists, accompanied by narratives describing the related major management challenges, are available on our Web site at www.gao.gov/pas/2005. As always, GAO stands ready to assist the Congress as it develops its agenda and pursues these important high-risk issues.

Mr. Chairman, Senator Akaka, and Members of the Subcommittee, this concludes my testimony. I would be happy to answer any questions you may have.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548