United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Science, State, Justice, Commerce, and Related Agencies, House of Representatives

For Release on Delivery
Expected at 10:30 a.m. EDT
Wednesday, September 14, 2005

INFORMATION TECHNOLOGY

FBI Is Building Management Capabilities Essential to Successful System Deployments, but Challenges Remain

Statement of Randolph C. Hite, Director
Information Technology Architecture and Systems Issues

September 14, 2005

INFORMATION TECHNOLOGY

FBI Is Building Management Capabilities Essential to Successful System Deployments, but Challenges Remain

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-05-1014T, a testimony before the Subcommittee on Science, State, Justice, Commerce, and Related Agencies, House of Representatives

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) is in the process of modernizing its information technology (IT) systems. Replacing much of its 1980s-based technology with modern system applications and supporting technical infrastructure, this modernization is intended to enable the FBI to take an integrated, agencywide approach to performing its critical missions, such as federal crime investigation and terrorism prevention. At the request of the Congress, GAO has conducted a series of reviews of the FBI's modernization management.

GAO was requested to testify on the bureau's progress to date in several areas of IT management. In addition, GAO discusses the importance of these areas for maximizing the prospects for success of the bureau's ongoing and future IT system investments, including the FBI's flagship Sentinel program; this program replaces the bureau's failed Virtual Case File project and aims to acquire and deploy a modern investigative case management system.

In this testimony, GAO relied extensively on its previous work on the FBI's management of its IT processes, human capital, and tools, and it obtained updates on these efforts through reviews of documentation and interviews with responsible FBI officials, including the Chief Information Officer (CIO).

www.gao.gov/cgi-bin/getrpt?GAO-05-1014T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

Over the last 18 months, the FBI has made important progress in establishing IT management controls and capabilities that GAO's research and experience show are key to exploiting technology to enable transformation. These include centralizing IT responsibility and authority under the CIO and establishing and beginning to implement management capabilities in the areas of enterprise architecture, IT investment management, systems development and acquisition life cycle management, and IT human capital.

- The FBI has developed an initial version of its enterprise architecture and is managing its architecture activities in accordance with many key practices, but it has yet to adopt others (such as ensuring that the program office has staff with appropriate architecture expertise).
- The FBI is in the process of defining and implementing investment management policies and procedures. For example, it is performing assessments of existing systems to determine if any can be better used, replaced, outsourced, or retired, but these assessments have yet to be completed.
- The bureau has issued an agencywide standard life cycle management directive, but it has yet to fully implement this directive on all projects. Also, certain key practices, such as acquisition management, require further development.
- The FBI has taken various steps to bolster its IT workforce, but it has yet to create an integrated plan based on a comprehensive analysis of existing and needed knowledge, skills, and abilities. According to the CIO, he intends to hire a contractor to perform this and develop an implementation plan. The CIO also intends to establish a management structure to carry out the plan.

The challenge now for the FBI is to build on these foundational capabilities and implement them effectively on the program and project investments it has under way and planned, none of which is more important than the Sentinel program. The success of this program will depend on how well the FBI defines and implements its new IT management approaches and capabilities, particularly those associated with acquiring a system made up of commercial components, which Sentinel is to be. In this regard, it will be crucial for the FBI, among other things, to understand and control Sentinel requirements in the context of (1) its enterprise architecture, (2) the capabilities and interoperability of commercially available products, and the (3) bureau's human capital and financial resource constraints. It will also be important for the FBI to prepare users for the impact of the new system on how they do their jobs. To the extent that the FBI does not take these steps, it will introduce program risks that could lead to problems similar to those that contributed to the failure of the Virtual Case File project.

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to participate in the Subcommittee's hearing on the efforts of the Federal Bureau of Investigation (FBI) to transform itself in the wake of the attacks of September 11, 2001. As you are aware, a vital part of this transformation is the modernization of the FBI's information technology (IT) systems to support an agencywide approach to performing critical mission operations, such as the bureau's expanding intelligence activities and its long-standing criminal investigation and law enforcement efforts. To this end, the bureau has been investing more than a billion dollars in projects to replace its aging, inefficient IT environment with more modern networks and integrated data and application systems. Unfortunately, it has been challenged in doing so, leading in some cases to less than successful outcomes on key mission critical systems.

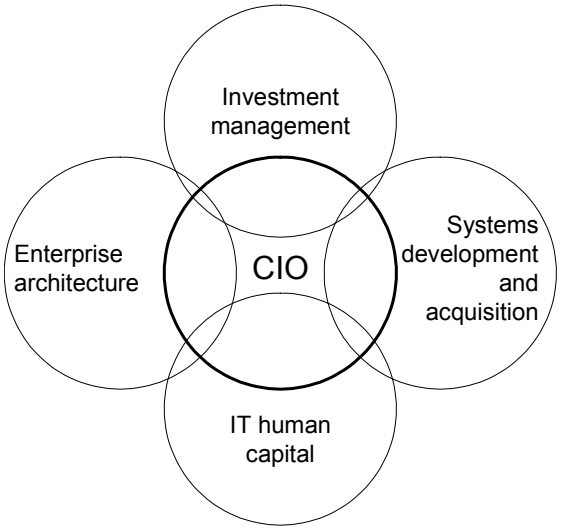
The key to an agency's success in modernizing its IT systems, as our research and experience at federal agencies has shown, is institutionalizing a set of interrelated IT management controls and capabilities, including

- centralizing responsibility, accountability, and authority for key IT management functions with the agency's Chief Information Officer (CIO);
- developing and using an agencywide enterprise architecture,[1] or modernization blueprint, to guide and constrain IT investments;
- establishing and following a portfolio-based approach to selecting and controlling IT investments;
- defining and implementing a disciplined system acquisition/development life cycle management approach; and
- building and sustaining an IT workforce with the necessary knowledge, skills, and abilities to execute this range of IT management functions.

[1] An enterprise architecture is a set of descriptive models (e.g., diagrams and tables) that define, in business terms and in technology terms, how an organization operates today, how it intends to operate in the future, and how it intends to invest in technology to transition from today's operational environment to tomorrow's.

All these areas are interdependent and interrelated, as shown in figure 1. If effectively established and implemented, they are keys to success in modernizing systems.

Figure 1: Interrelated Keys to Successful IT Management



Source: GAO.

Note: Figure shows topics addressed in this testimony, not all key IT management areas.

Under the sponsorship of your Subcommittee and other congressional clients, we have conducted a series of reviews at the FBI over the last 4 years that have addressed these key areas, and have made recommendations for improvement. Just last week, for example, we completed the latest in this series of reviews when we issued to your Subcommittee a report on the state of the FBI's enterprise architecture program.[2] Our testimony today summarizes what we have reported relative to each of these areas; in addition, we discuss the importance of these capabilities for maximizing the prospects for success in the bureau's ongoing and future IT system programs and projects, such as the recently undertaken Sentinel

[2] GAO, *Information Technology: FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished*, GAO-05-363 (Washington, D.C.: Sept. 9, 2005).

program, which aims to acquire and deploy a modern investigative case management system.

In preparing for this testimony, we drew extensively from our previous work[3] on the FBI's management of its IT processes, human capital, and tools. In addition, we reviewed documentation and interviewed responsible FBI officials, including the CIO, to update our work. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Over the last 18 months, the FBI has made important progress in establishing key IT modernization management controls and capabilities. These include centralizing IT responsibility and authority under the CIO and establishing and beginning to implement management capabilities in the areas of enterprise architecture, IT investment management, systems development and acquisition, and IT human capital. For example, the FBI is now managing development of its enterprise architecture program in accordance with many best practices (such as establishing a program office to develop the architecture and issuing a written and approved policy to govern this development) but it has yet to adopt others (such as providing adequate human capital for the program office).

The challenge now for the FBI is to build on these foundational capabilities and effectively implement them on the many program and project investments it has under way and planned. In so doing,

[3] GAO, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO-03-959 (Washington, D.C.: Sept. 25, 2003); *Federal Bureau of Investigation's Comments on Recent GAO Report on its Enterprise Architecture Efforts*, GAO-04-190R (Washington, D.C.: Nov. 14, 2003); *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004); and GAO, *Information Technology: FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished*, GAO-05-363 (Washington, D.C.: Sept. 9, 2005).

the FBI will be better positioned to accomplish the end goal: effectively leveraging technology to accomplish its transformation priorities.

Background

The FBI's mission responsibilities include investigating serious federal crimes, protecting the nation from foreign intelligence and terrorist threats, and assisting other law enforcement agencies. Approximately 12,000 special agents and 16,000 analysts and mission support personnel are located in the bureau's Washington, D.C., headquarters and in more than 450 offices in the United States and 45 offices in foreign countries.

Mission responsibilities at the bureau are divided among the following five major organizational components.

- Administration: manages the bureau's personnel programs, budgetary and financial services, records, information resources, and information security.
- Counterterrorism and Counterintelligence: identifies, assesses, investigates, and responds to national security threats.
- Criminal Investigations: investigates serious federal crimes and probes federal statutory violations involving exploitation of the Internet and computer systems.
- Intelligence: collects, analyzes, and disseminates information on evolving threats to the United States.
- Law Enforcement Services: provides law enforcement information and forensic services to federal, state, local, and international agencies.

The components are further organized into subcomponents, such as divisions, offices, and other groups (hereafter referred to as "divisions"). Table 1 lists the components and briefly describes their respective divisions.

Table 1: FBI Components and Divisions and Their Mission Responsibilities

Component/division	Mission responsibilities
Administration	
Administrative Services Division	Develop and administer personnel programs and services, including recruiting, conducting background investigations, and other administrative activities
Finance Division	Administer budget and fiscal matters, including financial planning, payroll services, property management, and procurement activities
Office of Strategic Planning	Manage the bureau's strategic planning activities and provide organizational resource allocation and management services
Records Management Division	Provide direction and oversight for all records policy and functions, including records maintenance and disposition, records review and dissemination, and Freedom of Information and Privacy Acts
Security Division	Ensure safe and secure work environment, including preventing the compromise of national security information
Counterterrorism and Counterintelligence	
Counterintelligence Division	Identify and neutralize ongoing national security threats, including conducting foreign counterintelligence investigations, coordinate investigations with the U.S. intelligence community, and investigate violations of federal espionage statutes
Counterterrorism Division	Prevent, disrupt, and defeat terrorist operations before they occur; pursue sanctions for those who have conducted, aided, and abetted terrorist acts; and provide crisis management following acts of terrorism against the U.S. and U.S. interests
Criminal Investigations	
Criminal Investigative Division	Investigate serious federal crimes, including those associated with organized crime, violent crime, white-collar crime, government and business corruption, and civil rights violations
Cyber Division	Probe federal statutory violations involving exploitation of the Internet and computer systems for criminal, foreign intelligence, and terrorism purposes
Intelligence	
Office of Intelligence	Collect and analyze information on evolving threats to the United States and ensure its dissemination within the FBI, to the U.S. intelligence community, and to law enforcement
Law Enforcement Services	
Criminal Justice Information Services Division	Provide information services on fingerprint identification, stolen automobiles, criminals, crime statistics, and other information to state, local, federal, and international law enforcement
Critical Incident Response Group	Respond to and manage crisis incidents such as terrorist activities, child abductions, and other repetitive violent crimes
Investigative Technology Division	Provide leadership and technical support to FBI investigative efforts, including ensuring the operational availability of modern technologies and the application of forensic examination services related to the collection, processing, and exploitation of digital evidence
Laboratory Division	Perform forensic examinations in support of criminal investigations and prosecutions, including crime scene searches, DNA testing, photographic surveillance, expert court testimony, and other technical services
Office of International Operations	Promote relations with both foreign and domestic law enforcement and security services, facilitate investigative activities where permitted, and provide managerial support of the Legal Attaché Program

Component/division	Mission responsibilities
Office of Law Enforcement Coordination	Improve coordination and information sharing with state and local law enforcement and public safety agencies
Training Division	Train agents and support personnel as well as state, local, international, and other federal law enforcement personnel in crime investigation, law enforcement, and forensic investigative techniques

Source: GAO analysis of FBI data.

To execute its mission responsibilities, the FBI relies extensively on IT, and this reliance is expected to grow. For example, the bureau operates and maintains hundreds of computerized systems, networks, databases, and applications, such as

- the Combined DNA Index System, to support forensic examinations;
- the National Crime Information Center and the Integrated Automated Fingerprint Identification System, to help state and local law enforcement agencies identify criminals;
- the Automated Case Management System, to manage information collected on investigative cases;
- the Investigative Data Warehouse, to aggregate data in a standard format from disparate databases to facilitate content management and data mining; and
- the Terrorist Screening Database, to consolidate identification information about known or suspected international and domestic terrorists.

According to the FBI, it also has almost 500 systems, applications, databases, and networks that are in operation, undergoing enhancement, or being developed or acquired. In particular, it has identified 18 new or enhancement projects that support its intelligence, investigative, and analyst activities. Included in these 18 is its Sentinel program, the FBI's effort to deliver—using commercially available software and hardware components—a modern automated capability for investigative case management and information sharing, with the goal of helping field agents and analysts to perform their jobs more effectively and efficiently.

As we have previously reported,[4] these ongoing and planned IT programs and projects are part of the FBI's systems modernization program. This program is based both on the bureau's long-standing recognition of its antiquated, nonintegrated systems environment and its awareness of the importance of modern, integrated IT systems to its transformation efforts in the wake of the September 11 attacks. Currently, the FBI reports that it will spend approximately $484 million on modernization projects in fiscal year 2005 out of a total IT budget of $1.07 billion.

Effective IT Management Is Critical to FBI's Ability to Successfully Transform

Technology can be a valuable tool in helping organizations transform and better achieve mission goals and objectives. Our research on leading private and public sector organizations, as well as our past work at federal departments and agencies, shows that successful organizations embrace the central role of IT as an enabler for enterprisewide transformation.[5] These leading organizations develop and implement institutional or agencywide system modernization management controls to ensure that the vast potential of technology is effectively applied to achieving mission outcomes. Among these management controls are

- assigning IT responsibility and providing commensurate authority centrally with the agency's CIO,
- using a well-defined enterprise architecture as a systems modernization blueprint,

[4] GAO, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO-03-959 (Washington, D.C.: Sept. 25, 2003); *Federal Bureau of Investigation's Comments on Recent GAO Report on its Enterprise Architecture Efforts*, GAO-04-190R (Washington, D.C.: Nov. 14, 2003); *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004); and *Information Technology: FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished*, GAO-05-363 (Washington, D.C.: Sept. 9, 2005).

[5] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001); *Architect of the Capitol: Management and Accountability Framework Needed for Organizational Transformation*, GAO-03-231 (Washington, D.C.: January 2003).

- following a portfolio-based approach to selecting among competing IT programs and projects and controlling investment in each during their life cycles,
- adhering to a structured and disciplined system development and acquisition life cycle management methodology, and
- employing sufficient and qualified IT human capital.[6]

We have observed that without these types of controls and capabilities, organizations increase the risk that system modernization projects will (1) experience cost, schedule, and performance shortfalls and (2) lead to systems that are redundant and overlap. They also risk not achieving their aim of increased interoperability and effective information sharing. All told, this means that technology will not effectively and efficiently support agency mission performance and help realize strategic mission outcomes and goals.

The FBI Director has recognized the importance of IT to transformation, and accordingly made it one of the bureau's top 10 priorities.[7] Consistent with this, the FBI's strategic plan contains explicit IT-related strategic goals, objectives, and initiatives (near-term and long-term) to support the collection, analysis, processing, and dissemination of information.

However, as we have previously reported,[8] the bureau's long-standing approach to managing IT has not always been fully consistent with leading practices. The effects of this approach can be seen in, for example, the cost and schedule shortfalls experienced on a key infrastructure and applications modernization

[6] Other important IT management controls are not addressed in this testimony, such as effective information security management.

[7] For example, see statement of Robert S. Mueller III, Federal Bureau of Investigation, before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, House of Representatives (June 2002).

[8] GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004).

program, Trilogy, and particularly on one of its projects (the Virtual Case File), which was recently terminated by the bureau. Reviews of this project identified management weaknesses as the cause for its cost, schedule, and performance shortfalls. Among these weaknesses were lack of integration planning, inadequately defined requirements, project management deficiencies, and frequent turnover of key personnel.[9]

In place of the Virtual Case File project, the FBI launched its Sentinel program in early 2005 to develop what the bureau describes as its next-generation electronic information management system. According to the FBI, the system is planned to consolidate and replace its existing case management capabilities with an integrated, paperless file management and workflow system.

FBI Is Making Progress in Establishing Key IT Modernization Management Capabilities

The FBI is making progress in establishing institutional IT modernization management capabilities. It has centralized IT responsibility and authority under the CIO, and it is establishing and beginning to implement management capabilities in the areas of enterprise architecture, IT investment management, systems development and acquisition, and IT human capital. Before it can effectively leverage technology to transform itself, the FBI will have to build on these capabilities and effectively implement them on its system investments.

[9] U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Implementation of Information Technology Recommendations*, Audit Report 03-36 (Washington, D.C., September 2003); *Federal Bureau of Investigation's Management of Information Technology Investments*, Audit Report 03-09 (Washington, D.C.: December 2002); and *Action Required on Audit Report 03-09* (Washington, D.C.: September 2003). Statement of Glenn A. Fine, Inspector General, Department of Justice, before the Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and the Judiciary (Mar. 23, 2004).

FBI Has Centralized Responsibility and Authority for IT

Our research on leading private and public sector organizations, as well as our past work at federal departments and agencies, shows that successful organizations adopt a corporate, or agencywide, approach to managing IT under the leadership and control of a senior executive—commonly called a chief information officer—who operates as a full partner with the organizational leadership team in charting the strategic direction and making informed IT investment decisions. The Clinger-Cohen Act[10] also mandates that major federal departments and agencies establish the position of CIO. As the focal point for IT management within an agency, the CIO is positioned to oversee the establishment and implementation of agencywide capabilities in IT management.

In the FBI, responsibility for managing IT was historically decentralized and diffused. For example, we testified in March 2004[11] that the FBI had not provided its CIO with bureauwide IT management authority and responsibility, vesting these instead in the bureau's divisions. This is part of the reason that the FBI's IT environment at the time consisted of nonintegrated applications residing on different servers, each of which had its own unique databases, unable to share information with other applications or with other government agencies. To address this, we discussed with the Director in 2003 the importance of centralizing IT management responsibility and authority under the CIO, and we subsequently recommended that the CIO be provided with the responsibility and authority for managing IT bureauwide, including budget management control and oversight of IT programs and initiatives.[12]

The FBI has since taken steps to strengthen the scope and influence of the CIO Office. In particular, the CIO was assigned agencywide

[10] Clinger-Cohen Act of 1996, 40 U.S.C. 11101-11703.

[11] GAO, *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities*, GAO-04-578T (Washington, D.C.: Mar. 23, 2004).

[12] GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004).

responsibility, authority, and control over IT resources, including responsibility for preparing the bureau's IT strategic plan and operating budget; operating and maintaining existing systems and networks; developing and deploying new systems; defining and implementing IT management policies, procedures, and processes; and developing and maintaining the bureau's enterprise architecture.

To fulfill these responsibilities, the CIO's office has begun the process of developing and implementing a corporatewide approach to managing IT. For example, the FBI reorganized the CIO Office, establishing four offices[13] to carry out key institutional management functions, and issued an IT strategic plan in September 2004 that outlined ongoing and planned efforts to strengthen policies and procedures by standardizing them across the bureau and incorporating best practices. Among other things, this plan provided for building capabilities in a number of key IT management areas, including the following four areas: enterprise architecture, IT investment management, systems development and acquisition, and IT human capital.

FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Work Remains To Be Done

As our research and evaluations have shown, it is risky to attempt to modernize an IT environment without using an architecture, or blueprint, to guide and constrain the definition, design, and development of IT programs and projects. An enterprise architecture provides systematic structural descriptions—in useful models, diagrams, tables, and narrative—of how a given entity operates today and how it plans to operate in the future, and it includes a road map for transitioning from today to tomorrow. Our experience with federal agencies has shown that attempting to modernize systems without having an enterprise architecture often results in systems that are duplicative, not well integrated,

[13] The four offices are the Offices of IT Policy and Planning, IT Program Management, IT Systems Development, and IT Operations.

unnecessarily costly to maintain, and limited in terms of optimizing mission performance.[14]

To assist agencies in effectively developing, maintaining, and implementing an enterprise architecture, we published a framework for architecture management, grounded in federal guidance and recognized best practices.[15] In 2002 and again in 2003, we reported that the FBI did not have either an architecture to guide and constrain its IT investments or the means in place to develop and implement one. We further reported that the development of an architecture was not being given the priority that it deserved. Accordingly, we recommended that the Director make it an institutional priority, and provided a series of recommendations for building an architecture management foundation, developing and completing the architecture, and using it to inform IT investment decision making.

In the last 12 months, the bureau has made important progress in developing its architecture. Last week we issued a congressionally mandated report on the state of the FBI's enterprise architecture efforts.[16] In summary, we found that the FBI is now managing its enterprise architecture program in accordance with many best practices, but it has yet to adopt others. Examples of best practices that the bureau has implemented include the following:

- the bureau has established a program office that is responsible for the development of the architecture;

[14] See for example, GAO, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458, (Washington, D.C.: February 2003); *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: August 2000).

[15] GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: April 2003).

[16] GAO, *Information Technology: FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished*, GAO-05-363 (Washington, D.C.: Sept. 9, 2005).

- it has issued a written and approved policy governing architecture development; and
- it has ongoing efforts to complete a target architecture.[17]

We ascribed this important progress, in part, to the demonstrated commitment of the FBI's top management to the enterprise architecture program. Nonetheless, we recognized that much remains to be accomplished before the FBI's enterprise architecture program will be mature. For example, we reported that the architecture program office did not yet have appropriate human resources with architecture expertise and that the bureau was not following a defined methodology for developing its architecture, both of which are foundational items. Also, the bureau's current and target architectures were not yet complete. (For instance, the program office had not completed mapping FBI data structures, classifications, and exchanges to the business processes that use the data, nor has it finished defining how the various IT applications currently interrelate.) Further, the bureau had not yet begun to develop its investment plans for transitioning from the current to the target architectural states.

We also reported that the FBI had not employed effective contract management controls in developing its enterprise architecture, which is risky because the bureau is relying heavily on contractor support in this effort. (We discuss this contract management issue further in the section of this testimony dealing with system development and acquisition.)

Because we had already made comprehensive recommendations regarding the FBI's enterprise architecture program, we made no additional recommendations in this area. However, because of the FBI's heavy reliance on contractor assistance in developing its architecture and the state of its contract management controls, we recommended that the FBI employ performance-based contracting

[17] A target or "to be" architecture describes an enterprise's goals for its future business, performance, information/data, application/service, and technology environments. A current or "as is" architecture describes an enterprise's current business, performance, information/data, application/service, and technology environments.

on all further architecture contract actions (to the maximum extent practicable) and follow effective contract tracking and oversight practices.

In response, the FBI stated that it would continue to strive to develop a robust enterprise architecture program supported by effective contract management practices and cited steps under way to strengthen its architecture management foundation. For example, since our report was issued, the FBI provided us with a document that the bureau stated defines its enterprise architecture methodology. In addition, the bureau reported that it is very close to hiring staff with architecture expertise (four senior level technologists) for the program office. Further, the FBI stated that it was taking steps to increase its use of performance-based contracting.

FBI Is Beginning to Apply Its New Investment Management Approach, but More Remains to Be Done

Based on our research at successful private and public sector organizations, we have issued an IT investment management (ITIM) framework[18] that encompasses the best practices, including investment selection and control policies and procedures, of successful public and private sector organizations. Our ITIM framework is consistent with the Clinger-Cohen Act of 1996[19] and identifies, among other things, effective policies and procedures for developing and using an enterprisewide collection—or portfolio—of investments; using such portfolios enables an organization to determine priorities and make decisions among competing options across investment categories based on analyses of the relative organizational value and risks of all investments. Portfolios should include three types of IT investments:

[18] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Exposure Draft, GAO/AIMD-10.1.23 (Washington, D.C.: May 2000); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

[39]Clinger-Cohen Act of 1996, 40 U.S.C. §§11101-11703.

- planned (proposed systems or system enhancements),
- under way (systems being developed or acquired), and
- completed (existing systems being operated and maintained).

The FBI's progress over the last 3 years to define and refine an IT investment approach has been slow. In 2002, the bureau first focused on developing an approach that addressed solely IT investments and in 2003 expanded the approach's scope to include all capital investments.[20] In 2004, under the leadership of the current CIO, the bureau redirected its investment selection, control, and evaluation activities back to include IT investments only. In September 2004, we reported that this redirected approach included one set of processes for new investments that are planned and under way and another set for the operation and maintenance of existing systems.[21] At that time, the process for investments in new systems was still being defined, while a process for allocating operations and maintenance resources across existing systems had been developed. We also reported that the bureau was to pilot test its developed process on different types of investments (systems, applications, databases, and networks) with the goal of subsequently implementing the process enterprisewide. In our view, it was important that the implemented process be in accordance with key IT investment decision-making best practices (such as our ITIM framework). Accordingly, we made recommendations aimed at expediting implementation of ITIM-compliant policies and procedures.

Since then, the FBI has taken a number of steps to strengthen its capability to manage IT investments. For example, in November 2004, the FBI established an investment review board, composed of senior executives, that meets about every 2 weeks to review proposed and ongoing investments in new systems. The CIO stated that the board recently completed its first evaluation of the bureau's

[20] The bureau did not complete either of these two earlier efforts.

[21] GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004).

89 ongoing IT investments to, among other things, establish cost, schedule, and performance baselines and to begin the process of having the CIO and other senior executive review the projects at critical development milestones. The CIO also reported that the bureau has reviewed over 37 new proposals and is using the results in preparing its fiscal year 2007 IT budget request. Further, to establish a more defined structure to support the board's activities, the CIO's office recently issued an ITIM guide, which defines, among other things, the processes that the board is to follow in selecting and controlling these investments.

In addition, the CIO's office is in the process of assessing the performance of existing systems (i.e., those in the operations and maintenance phase of their life cycle). Using cost and other criteria, these assessments are designed to determine which systems can be better used, replaced, outsourced, or retired. According to the CIO, the program recently completed a pilot assessment of projects in one FBI division, and it is currently preparing to perform similar assessments in the other divisions, which are scheduled to be completed by April 2006.

Notwithstanding these efforts, until the FBI fully implements processes for selecting, controlling, and evaluating all its IT investments, it will not be able to ensure that it is applying its resources to the best mix of investments to meet the goals of modernizing IT and transforming itself.

The Bureau Has Moved to Standardize System Development and Acquisition Life Cycle Processes that Were Inconsistent across FBI Components

Having rigorous and disciplined IT system development and acquisition life cycle processes is an important component of IT management. The Clinger-Cohen Act recognizes the importance of such effective processes, and the Software Engineering Institute's

(SEI) Capability Maturity Models™[22] define a suite of such processes. Five process areas associated with systems acquisition (which collectively are composed of 30 key practice areas) are configuration management, project management, quality assurance, requirements development and management, and risk management. In combination with other process areas, these five provide a foundation for managing software-intensive systems in a manner that minimizes risks and increases the chances of systems delivering required system capabilities and benefits on time and within budget.

In September 2004, we reported that the life cycle management policies and procedures then in place at the FBI for these five areas varied widely by division.[23] On the one hand, for example, the policies and procedures for the six divisions that we examined generally addressed all the practices associated with the project management process area (see table 2); this process area involves management of project office activities so that projects are timely, efficient, and effective.

Table 2: Use of Project Management Practices by Six FBI Divisions

Project management best practice	Number of divisions with policies and procedures in place
Identifying project management roles and responsibilities	6 of 6
Developing a project management plan	6 of 6
Baselining and tracking the status of project cost, schedule, and performance, including associated risks	5 of 6
Establishing a process to identify, record, track, and correct problems discovered during the acquisition	5 of 6

[22] Carnegie Mellon University's Software Engineering Institute has developed criteria, known as the *Software Acquisition Capability Maturity Model*, CMU/SEI-99-TR-002 (April 1999) and *Key Practices of the Capability Maturity Model*, CMU/SEI-93-TR-25 (February 1993) for determining organizations' software acquisition management and development effectiveness or maturity. Capability Maturity Model and CMM are registered in the U.S. Patent and Trademark Office.

[23] GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004).

Project management best practice	Number of divisions with policies and procedures in place
Periodically reviewing and communicating the status of project management activities and commitments with management and affected groups	6 of 6

Source: GAO.

On the other hand, for example, the policies and procedures for these six divisions generally did not address the key practices associated with requirements development and management process area (see table 3); this process area involves establishing and maintaining agreement on system requirements. We would note that according to the CIO, it was a lack of bureau rigor and discipline in this area that in part caused the Virtual Case File project to be terminated.

Table 3: Use of Requirements Development and Management Practices by Six FBI Divisions

Requirements development and management best practice	Number of divisions with policies and procedures in place
Identifying requirements development and management roles and responsibilities	3 of 6
Involving end users in development of and changes to requirements	3 of 6
Having a requirements management plan	1 of 6
Developing and baselining requirements, and controlling changes to them	2 of 6
Appraising changes to requirements for their impact on the project or IT environment	0 of 6
Maintaining traceability among requirements and other project deliverables	3 of 6
Periodically reviewing the status of requirements activities with management	2 of 6

Source: GAO.

Examples of requirements development and management practices that most divisions did not adequately address are (1) appraising changes to requirements for their impact on the project or the IT environment, which is important because it allows management and the project team to determine whether the benefits of changes to the requirements would be worth the likely cost and effect of making the changes, and (2) developing and baselining requirements and

maintaining them under change control, which is important to ensuring that requirements are completely and correctly defined and that uncontrolled changes, commonly referred to as "requirements creep," are avoided.

In our September 2005 report, we addressed another key process area associated with system acquisition life cycle management—contract management. Federal acquisition regulations and relevant IT acquisition management guidance recognize the importance of effectively managing contractor activities. According to the Federal Acquisition Regulation (FAR), for example, agencies are to use performance-based contracting to the maximum extent practicable when acquiring most services.[24] Under the FAR, performance-based contracting includes, among other things, defining the work to be performed in measurable, results-oriented terms and specifying performance standards (quality and timeliness). The FAR and associated regulations[25] also require government oversight of contracts to ensure that the contractor performs the requirements of the contract, and the government receives the service as intended. Although the regulations do not prescribe specific methods for this oversight, other acquisition management guidance[26] describes a number of practices associated with this activity.[27]

However, the FBI's approach to managing its enterprise architecture contract did not include most of the performance-based contracting features described in the FAR. For example, the contract's statement of work did not specify the products in results-oriented, measurable terms. In addition, the bureau did not have plans for assuring the quality of the contractor's work; instead, according to

[24] See Federal Acquisition Regulation, section 37.102(a).

[25] See Federal Acquisition Regulation, Part 46, "Quality Assurance."

[26] See, for example, Carnegie Mellon Software Engineering Institute, *Software Acquisition Capability Maturity Model*, CMU/SEI-99-TR-002 (April 1999).

[27] For example, two of these are establishing a written policy for contract tracking and oversight and using approved contractor planning documents as a basis for tracking and overseeing the contractor.

bureau officials, they worked with the contractor to determine whether each deliverable was acceptable.

In addition, in overseeing its contractor, the FBI has not employed the kind of effective practices specified in relevant guidance. For example, the bureau does not have a written policy to govern its tracking and oversight activities, has not designated responsibility or established a group for performing contract tracking and oversight activities, and has not developed an approved contractor monitoring plan.

To address weaknesses in the FBI's systems development and acquisition life cycle processes, we have recommended that the FBI establish effective policies and procedures for such systems acquisition and development areas as configuration management, project management, quality assurance, requirements development and management, risk management, and contract tracking and oversight.

Recognizing the need to strengthen and standardize its IT requirements and development management capabilities, the FBI has issued a bureauwide standard life cycle management directive with the aim of achieving consistent processes in the systems acquisition and development areas mentioned above. A second goal is to integrate these processes with other key IT disciplines, including those discussed in this testimony as well as others, such as information security management. CIO officials told us that they recently began implementing parts of the life cycle management directive across all projects. According to the CIO, the directive is to be fully defined and implemented by the end of 2006.

The FBI acknowledges that the directive needs to be enhanced and extended to adequately address all relevant process areas. For example, FBI officials stated that they are still working to define effective contract management controls, such as procedures for the use of performance-based contracting methods and the establishment of tracking and oversight structures, policies, and processes. For other key practices, procedures have been drafted but require further development.

FBI Has Developed Strategic IT Human Capital Management Policies and Procedures and Is Taking Steps to Implement Them

A strategic approach to human capital management includes viewing people as assets whose value to an organization can be enhanced by investing in them,[28] and thus increasing both their value and the performance capacity of the organization. Based on our experience with leading organizations, we issued a model[29] encompassing strategic human capital management, in which strategic human capital planning was one cornerstone.[30] Strategic human capital planning enables organizations to remain aware of and be prepared for current and future needs as an organization, ensuring that they have the knowledge, skills, and abilities needed to pursue their missions. We have also issued a set of key practices for effective strategic human capital planning.[31] These practices are generic, applying to any organization or component, such as an agency's IT organization. They include

- involving top management, employees, and other stakeholders in developing, communicating, and implementing a strategic workforce plan;
- determining the critical skills and competencies needed to achieve current and future programmatic results;
- developing strategies tailored to address gaps between the current workforce and future needs;
- building the capability to support workforce strategies; and
- monitoring and evaluating an agency's progress toward its human capital goals and the contribution that human capital results have

[28] See GAO, *Human Capital: Attracting and Retaining a High-Quality Information Technology Workforce*, GAO-02-113T (Washington, D.C.: Oct. 4, 2001); *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002); *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[29] GAO-02-373SP.

[30] The other three are leadership; acquiring, developing, and retaining talent; and results-oriented organizational culture.

[31] GAO-04-39.

made to achieving programmatic goals.

As we have reported,[32] the FBI's enterprisewide strategic human capital plan, issued in March 2004, includes policies and procedures for IT human capital.[33] These IT policies and procedures are in alignment with the key practices discussed above. More specifically, they call for the following.

- Top management stakeholders (e.g., the CIO, the head of the Office of Strategic Planning, and the head of Administration) and other stakeholders (e.g., section and unit chiefs) are to be involved with the development, communication, and implementation of the policies and procedures.
- A detailed data bank is to be developed to store critical skills needed in the development and selection of personnel, including IT staff.
- Strategies are to be defined to address workforce gaps, including recruiting programs that provide for tuition assistance and cooperative education.
- An IT center is to be established to support workforce strategies and train existing personnel for future competencies and skills that will be needed.
- The agency's progress is to be monitored and evaluated by tracking implementation plans to ensure that results are achieved on schedule.

Since that time, the CIO stated that his office is taking steps to enhance its IT human capital capability. For example, it is working with the bureau's Training Division to identify the skills and abilities of the existing IT workforce and to provide training to enhance these skills and abilities, including having program and project managers work toward becoming certified in their respective

[32] GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004).

[33] Federal Bureau of Investigation, *FBI Strategic Human Capital Plan* (Washington, D.C.: March 2004).

disciplines. In addition, the CIO said that as part of reorganizing the CIO's office, he has created 12 senior executive and 4 senior level technical positions and is in the process of filling them with experienced and qualified staff. According to the CIO, the bureau has hired 8 senior executives and is in the process of hiring the others as well as the 4 senior technical staff.

However, the bureau has yet to create an integrated plan of action that is based on a comprehensive analysis of the human capital roles and responsibilities needed to support the IT functions established under the CIO office's reorganization. Such an analysis should include an assessment of core competencies and essential knowledge, skills, and abilities, as well as linking current human capital strengths and weaknesses to permit gaps to be identified between current capabilities and those needed to perform the established IT functions. The plan should then describe actions needed to fill the identified gaps (that is, the planned combination of hiring, training, contractor support, and so on), along with time frames, resources, performance measures, and accountability structures. According to the CIO, he is in the process of hiring a contractor with human capital expertise to help identify gaps between existing skills and abilities and those that will be needed to successful modernize the bureau's IT. The CIO intends to have this effort completed, including the development of an implementation plan to address any gaps, by the end of calendar year 2005. As part of this effort, the CIO stated that he is planning to implement a formal management structure within the Deputy CIO's office to monitor and evaluate human capital initiatives to ensure that results are achieved on schedule.

Notwithstanding the initiatives under way and planned, the FBI's IT human capital situation remains a work in progress, and this is a significant challenge. As we have previously reported,[34] when organizations implement a strategic approach to human capital management, how this is done, when it is done, and the basis on which it is done can make all the difference. With successful

[34] GAO, *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities*, GAO-04-578T (Washington, D.C.: Mar. 23, 2004).

implementation, the bureau can better position itself to ensure that it has the right people, in the right place, at the right time to effectively modernize IT and transform the organization.

Success of New IT Investments, Like Sentinel, Will Depend on How Well the FBI Implements its New IT Management Approaches

The success of the FBI in using IT to support its transformation efforts and in achieving its mission goals and outcomes will depend on how well it actually implements and institutionalizes the IT management structures, processes, and controls that have been or are currently being put in place. When the bureau's IT investments have been successfully delivered, and operational assets and tools are available to analysts and field agents to help them do their jobs better, only then can the mission value of technology be fully realized.

The FBI has identified several ongoing new or enhanced system projects that in our view will need to employ these kinds of IT management capabilities in order for each to be successfully defined, designed, developed or acquired, and deployed. For example, the FBI reports that it currently has 18 IT investments that support its "investigative, intelligence, and analytical" line of business, which is a major component of how the bureau accomplishes its mission. According to the bureau, each of these 18 investments is benefiting from the bureau's newly established IT management approach and capabilities.

Included in these 18 investments is Sentinel, the FBI's program to deliver an automated case management and information sharing capability; this is the successor to the Virtual Case File, the failed component of the Trilogy program. According to the FBI, Sentinel is to leverage commercially available technologies to consolidate and replace the bureau's existing case management capabilities with an integrated, paperless file management and workflow system, and to enhance information access and promote information sharing with both the law enforcement and intelligence communities. Thus far, the bureau reports it has developed detailed system requirements, a

concept of operations, an acquisition strategy and schedule, and a notional development and deployment strategy involving four increments delivered over 4 years. In August 2005, the FBI issued a request for vendor proposals to more than 40 eligible companies under a National Institutes of Health governmentwide contracting vehicle. According to the CIO, the request also was provided to over 500 eligible subcontractors. Vendor proposals are due later this month; the goal is to issue a contract in November 2005.

As an FBI flagship program, Sentinel can serve as a barometer of how well the FBI defines and implements its new IT management approaches and capabilities, particularly with regard to a system that is to rely extensively on commercially available components (software and hardware). As we discuss above (and have previously reported[35]), there are a number of IT system management practices related to architecture, investment, acquisition/development, and human capital that are critical to delivering promised system capabilities and benefits, on time and within budget. Moreover, these include management practices that are critical to any system, whether custom-developed or built from commercial components, as well as certain practices unique to systems based on commercial components.

Although each of these practices is relevant to Sentinel, there are several that we believe to be especially germane given the FBI's experience on the Virtual Case File, particularly with regard to requirements management and the bureau's reported efforts and plans going forward. Specifically, it is critical for the FBI to examine and control its requirements in the context of what capabilities are to be addressed through enterprise-provided services (e.g., records management and security) and what capabilities are to be provided through Sentinel. At the same time, it is essential that the bureau examine its requirements in the context of which capabilities can be provided by commercially available products and which cannot, and for those that cannot, how such requirements will be satisfied, if at

[35] For example, see GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 30, 2004).

all. As we and others have reported,[36] this examination involves continuous but controlled analyses of trade-offs among stated system requirements, commercial product availability, and enterprise architecture constraints; it also involves such practical constraints as human capital and financial resources.

Another area that is critical with respect to Sentinel is ensuring that decisions about the use of commercial components are based on an approach that includes deliberate and thorough research, analysis, and evaluation of components' dependencies. In this regard, it will be important for the FBI to ensure that it understands the behavioral interaction and compatibility of commercial off-the-shelf (COTS) components in order to select components that can be integrated in a predictable and standard way. We have found based on our research and past work[37] that doing so requires an effective methodology to gain and apply such knowledge; without such a methodology, building a COTS-based system can quickly lapse into trial and error, which is fraught with risks. For example, a trial and error approach can lead to expensive, ad hoc modifications, customized solutions, or unnecessary increases in the number and complexity of interfaces—all of which increases costs, delays delivery, and postpones realization of expected benefits. An

[36] For example, see GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 30, 2004). Also see Carnegie Mellon University Software Engineering Institute, *Capability Maturity Model® Integration for Systems Engineering and Software Engineering*, *Version 1.1* (Pittsburgh, Pa.: December 2001) and *The Capability Maturity Model: Guidelines for Improving the Software Process* (Addison Wesley Longman, Inc.: 1994); Jonathan Adams, Srinivas Koushik, Guru Vasudeva, and George Galambos, *Patterns for e-Business: A Strategy for Reuse* (IBM Press: 2001); B. Craig Meyers and Patricia Oberndorf, *Managing Software Acquisition: Open Systems and COTS Products* (Addison-Wesley: 2001); Jeffrey A. Hoffer, Joey F. George, and Joseph S. Valacich, *Modern Systems Analysis and Design* (Addison Wesley Longman, Inc.: 1999); and Kurt Wallnau, Scott Hissam, and Robert Seacord, *Building Systems from Commercial Components* (Addison-Wesley: 2002).

[37] For example, see Carnegie Mellon University Software Engineering Institute, *Capability Maturity Model® Integration for Systems Engineering and Software Engineering*, *Version 1.1* and *The Capability Maturity Model: Guidelines for Improving the Software Process*; Adams, Koushik, Vasudeva, and Galambos, *Patterns for e-Business: A Strategy for Reuse*; Meyers and Oberndorf, *Managing Software Acquisition: Open Systems and COTS Products*; Hoffer, George, and Valacich, *Modern Systems Analysis and Design*; and Wallnau, Hissam, and Seacord, *Building Systems from Commercial Components*.

effective approach would include (1) performing gap analysis between requirements and component capabilities, as mentioned above, (2) allocating requirements among the various products for a given system design option, (3) defining the interactions that need to occur among the components, (4) documenting decisions, and (5) using iterative prototyping to assess the interactions among the components.

Another very important area particularly relevant to Sentinel is ensuring that the project's plans explicitly provide the necessary time and resources for (1) integrating the commercial components with the FBI's existing systems and (2) preparing users for the impact that the business processes embedded in the COTS products will have on how the users will be expected to do their jobs, including potentially new roles and responsibilities. Available research suggests that insufficient attention to this organization change management issue has been a major cause of COTS solution implementations failing to live up their expectations.[38]

Other management practices relevant to commercial component-based systems will be important on Sentinel, including (1) discouraging the modification of COTS products; (2) managing the systems configuration in a way that provides for evaluation, acquisition, and implementation of new, often frequent, releases of COTS products; and (3) ensuring that contractors are experienced in implementing COTS-based system solutions.

In light of the importance of these and other areas, we have just initiated a review of Sentinel at the request of the Chairman and Ranking Member of the House Judiciary Committee; as part of this review, we plan to address many of these keys to project success.

In closing, the FBI has made important progress, particularly in the last 12 months under the new CIO's leadership, in establishing

[38] For example, see GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 30, 2004).

certain IT management and control capabilities that our research and evaluations show are key to exploiting technology to enable transformation. But although the bureau has come a long way from where it was just 18 months ago, establishing these capabilities is not enough. For the FBI to effectively use technology to transform itself and accomplish its goals, it will need to ensure that its capabilities are appropriately enhanced and extended and, most important, effectively implemented on all IT programs and projects. Nowhere will this be more crucial than on the Sentinel program. Because of the FBI's stated approach to building Sentinel, it will be particularly important for the bureau to ensure that it follows the kind of acquisition management practices that our work has shown to be critical for commercial component-based systems to be successful. If it does not, the FBI increases the likelihood that Sentinel will encounter the same cost, schedule, and performance shortfalls as its predecessor, the Virtual Case File.

Mr. Chairman, this concludes our statement. We would be happy to answer any questions that you or members of the Subcommittee may have at this time.

Contact and Acknowledgments

If you should have any questions about this testimony, please contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov. Other major contributors to this testimony included Gary Mountjoy, Assistant Director; Justin Booth; Barbara Collier; Kush Malhotra; Lori Martinez; Teresa Neven; Warren Smith; and Teresa Tucker.

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