United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2004

INFORMATION TECHNOLOGY

Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements

GAO

Accountability ★ Integrity ★ Reliability

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-842, a report to congressional requesters

September 2004

INFORMATION TECHNOLOGY

Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) is investing more than a billion dollars over 3 years to modernize its information technology (IT) systems. The modernization is central to the bureau's ongoing efforts to transform the organization. GAO was asked to determine whether the FBI has (1) an integrated plan for modernizing its IT systems and (2) effective policies and procedures governing management of IT human capital, systems acquisition, and investment selection and control.

What GAO Recommends

To help the bureau better manage its systems modernization risks, GAO is making several recommendations to the Director, including that the FBI limit its near-term investments in IT systems until the bureau develops an integrated systems modernization plan and effective policies and procedures for systems acquisition and investment management. GAO is also recommending that the Director provide the Chief Information Officer (CIO) with the responsibility and authority to effectively manage IT across the bureau. In the FBI's written comments on a draft of this report, the bureau agreed that steps are being taken to lay the foundation for improving IT operations, and that much work remains to institutionalize IT management improvements. The FBI also described recent actions and plans to address our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-842.

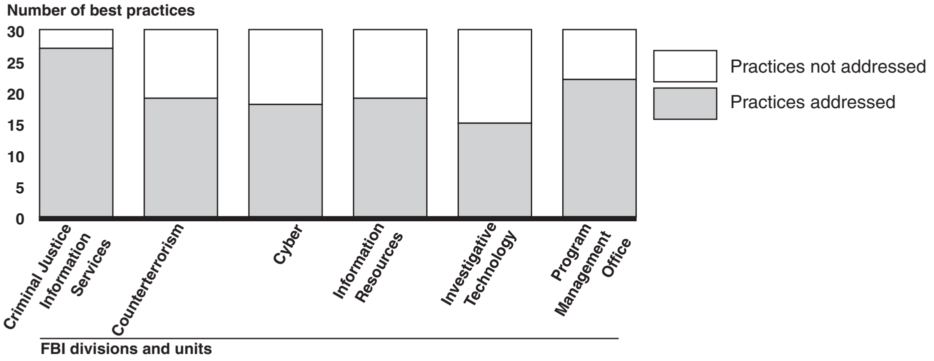
To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

Although improvements are under way and planned, the FBI does not currently have an integrated plan for modernizing its IT systems. Each of the bureau's divisions and other organizational units that manage IT projects performs integrated planning for its respective IT projects. However, the plans do not provide a common, authoritative, and integrated view of how IT investments will help optimize mission performance, and they do not consistently contain the elements expected to be found in effective systems modernization plans. FBI officials attributed the state of modernization planning to, among other things, the bureau's lack of a policy requiring such activities, which is due in part to the fact that the responsibility for managing IT—including modernization planning—has historically been diffused and decentralized. The FBI's CIO recognizes these planning shortfalls and has initiated efforts to address them. Until they are addressed, the bureau risks acquiring systems that require expensive rework to be effectively integrated, thus hampering organizational transformation.

The FBI has established policies and procedures governing IT human capital that are consistent with best practices used by leading private and public organizations. However, the bureau's policies and procedures governing systems acquisition, which are developed on a decentralized basis by the divisions and other units that manage IT projects, include some but not all best practices (see figure). In addition, the bureau's investment management policies and procedures, which started in 2001, have been evolving and progressing slowly toward alignment with best practices. According to FBI officials, the state of the bureau's acquisition and investment management policies and procedures is due to a number of factors, including diffused and decentralized IT management authority. The CIO recognizes these problems and has efforts planned and under way to strengthen policies and procedures. Until these efforts are completed, the bureau increases the risk that it will experience problems delivering promised IT investments on time and within budget, which, in turn, could adversely affect systems modernization and organizational transformation.

IT Systems Acquisition Best Practices Addressed in FBI Divisions' Policies and Procedures



Source: GAO analysis of FBI data.

Contents

Appendixes

Tables

Figures

Abbreviations

CIO	chief information officer
CJIS	Criminal Justice Information Services
FBI	Federal Bureau of Investigation
IT	information technology
OMB	Office of Management and Budget

United States Government Accountability Office
Washington, D.C. 20548

September 10, 2004

The Honorable Jane Harman
Ranking Minority Member
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Bob Graham
United States Senate

The Honorable Richard C. Shelby
United States Senate

The Honorable Porter J. Goss
House of Representatives

The Federal Bureau of Investigation (FBI) is in the midst of investing more than a billion dollars over 3 years to modernize its information technology (IT) systems, including its aging infrastructure (e.g., networks) and its mission operations and supporting administrative systems. The modernization is one of the bureau's top 10 priority initiatives and is central to its ongoing efforts to transform the organization. Our research has shown that effective IT modernization management plans, policies, and procedures are important contributors to an effective systems modernization program. Accordingly, you requested that we examine whether the FBI has (1) an integrated plan for modernizing its IT systems and (2) effective policies and procedures governing management of IT human capital, systems acquisition, and investment selection and control. We performed our work in accordance with generally accepted government auditing standards. Details of our objectives, scope, and methodology are in appendix I.

Results in Brief

Integrated project planning is not yet occurring across the bureau, but improvements are planned for the near future. Specifically, the bureau does not have an integrated plan or set of plans for modernizing its IT systems. Instead, the bureau's divisions, offices, and other groups that manage IT projects are responsible for integrated planning of their respective projects. Accordingly, the plans do not provide a common, authoritative, and integrated view of how IT investments will help optimize mission performance, and they do not consistently satisfy the elements expected to be found in effective systems modernization plans. For example, while two of six component organizations included the majority of key elements, the other four included few of them. FBI officials attributed the state of modernization planning to, among other things, the bureau's lack of a policy requiring integrated planning, which is due in part to the fact that the responsibility for managing IT, including modernization planning, has historically been decentralized and diffused. The FBI's Chief Information Officer (CIO) recognizes these planning shortfalls and has efforts planned and under way to address them. For instance, the CIO is developing a proposal for director approval that merges responsibility and authority for IT management, including integration planning, within the CIO's office. The longer the bureau continues to invest in systems without an integrated bureauwide view, the greater the risk that these systems will be duplicative and will require expensive rework to be integrated, thus hampering efforts to transform the organization. This risk has become a reality on five key ongoing infrastructure projects where, according to the bureau, it has found significant overlap due to the lack of integrated planning.

The bureau has established policies and procedures governing IT human capital that are consistent with best practices used by leading private and public organizations. Conversely, the bureau's policies and procedures governing systems acquisition and investment selection and control are not consistent with best practices, although efforts are planned and under way to remedy this. For example, systems acquisition policies and procedures, which are developed on a decentralized basis by the FBI's divisions and other organizations that manage IT projects, varied in their use of key practices of leading organizations. In addition, the bureau's investment management policies and procedures, which started in 2001, have been evolving and progressing slowly toward alignment with best practices. According to FBI officials, including the CIO, the state of the bureau's acquisition and investment management policies and procedures is due to a number of factors, including diffused and decentralized IT management authority and the bureau's past history of inattention to IT management. The CIO has actions planned and under way to strengthen policies and procedures in each of these critical areas. For example, the CIO is developing a systems life cycle management approach for bureauwide use that is to be fully consistent with the practices of leading organizations. Until this and other CIO efforts are completed, the bureau increases the risk that it will experience problems delivering promised IT investments on time and within budget, which could, in turn, adversely affect the bureau's systems modernization and organizational transformation.

To help the bureau better manage these systems modernization risks, we are making several recommendations to the FBI Director, including limiting the bureau's near-term investment in new and existing IT systems until it develops, among other things, an integrated systems modernization plan and effective policies and procedures for systems acquisition and investment management. We are also recommending that the Director provide the CIO with the responsibility and authority to effectively manage IT across the bureau.

In the FBI's written comments, which were signed by the CIO, on a draft of this report, the bureau agreed that it is taking steps to lay a foundation for improving IT operations. It further agreed that while progress is being made, much work remains to implement and institutionalize planned and ongoing IT management improvements. The FBI also described recent actions and plans for addressing our recommendations.

Background

The FBI is the primary investigative agency within the Department of Justice. Its missions 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 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.

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

- Administration: manages the bureau's personnel programs, budgetary and financial services, records, information resources, and information security.

Each component is headed by an executive assistant director who reports to the Deputy Director, who, in turn, reports to the Director. 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
Information Resources Division	Manage and plan for the use of IT resources
Office of Strategic Planning	Manage the bureau's strategic planning activities and provide organizational resource allocation and management services
Program Management Office	Support effective and efficient planning, design, development, and deployment of projects, including IT projects
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 United States 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

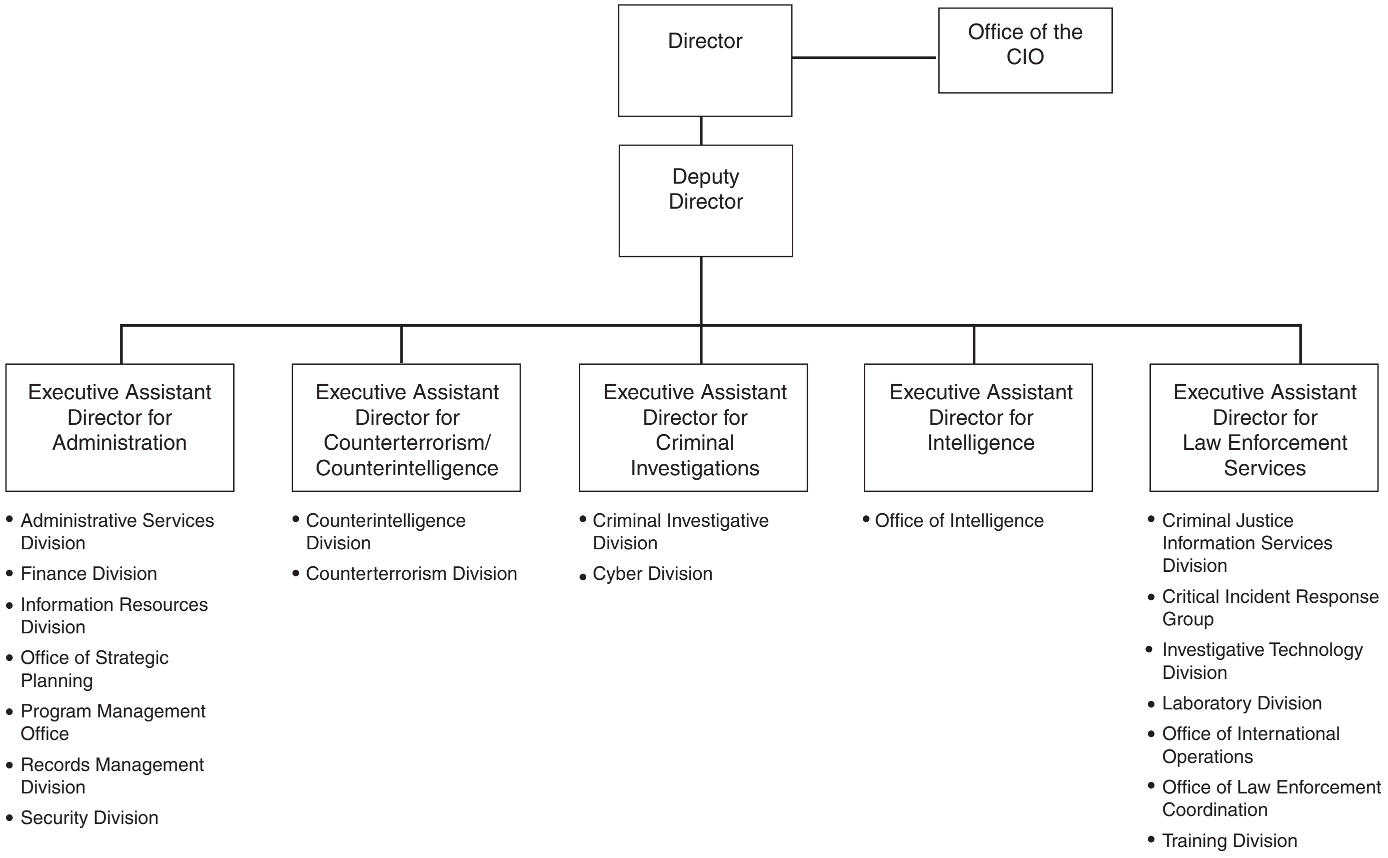
(Continued From Previous Page)

Component/division	Mission responsibilities
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
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.

Supporting the divisions are various staff offices, including the Office of the CIO. The CIO's responsibilities include, for example, development of the bureau's IT strategic plan and operating budget; development of IT investment management policies, processes, and procedures; and development and maintenance of the bureau's enterprise architecture. The CIO reports directly to the Director. Figure 1 shows a simplified organizational chart of the components, divisions, Office of the CIO, and respective reporting relationships.

Figure 1: Simplified FBI Organizational Chart



Director
Office of the CIO
Deputy Director
Executive Assistant Director for Administration
Executive Assistant Director for Counterterrorism/ Counterintelligence
Executive Assistant Director for Criminal Investigations
Executive Assistant Director for Intelligence
Executive Assistant Director for Law Enforcement Services
• Administrative Services Division
• Finance Division
• Information Resources Division
• Office of Strategic Planning
• Program Management Office
• Records Management Division
• Security Division
• Counterintelligence Division
• Counterterrorism Division
• Criminal Investigative Division
• Cyber Division
• Office of Intelligence
• Criminal Justice Information Services Division
• Critical Incident Response Group
• Investigative Technology Division
• Laboratory Division
• Office of International Operations
• Office of Law Enforcement Coordination
• Training Division

Source: GAO analysis of FBI data.

To execute its mission responsibilities, the FBI relies extensively on IT. For example, the Criminal Justice Information Services (CJIS) division uses the National Crime Information Center 2000 to process approximately 4 million criminal identification inquiries and other related transactions for civilian, homeland security, and law enforcement agencies each day. Similarly, the Laboratory division stores records of known criminals on the Combined DNA[1] Index System to compare with DNA evidence submitted by federal, state, and local law enforcement agencies. The FBI reports that it collectively manages hundreds of systems, networks, databases, applications, and associated IT tools at an average annual cost of about $800 million. As we have previously reported,[2] the FBI's IT environment is composed of outdated, nonintegrated systems that do not optimally support mission operations.

FBI Has Initiated a Wide Range of IT Modernization Projects

To address its strategic IT needs, the bureau began modernizing its systems environment in the mid-1990s. Currently, the FBI reports that eight divisions will spend approximately $1 billion on 18 major[3] IT modernization initiatives between fiscal years 2003 and 2005. These initiatives, such as Trilogy and the Investigative Data Warehouse, are to introduce new systems infrastructure and applications. For example, Trilogy is to establish an enterprise network to enable communications among hundreds of domestic and foreign FBI locations. According to the FBI, the first two segments of the project—the Transportation Network Component and the Information Presentation Component—were implemented as of April 2004. The third segment—the User Applications Component, commonly called the Virtual Case File—has been delayed and a new schedule is being determined. In addition, the Investigative Data Warehouse initiative is to provide the capability to search and share counterterrorism and criminal investigative information across the bureau;

[1] Deoxyribonucleic acid.

[2] GAO, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO-03-959 (Washington, D.C.: Sept. 25, 2003).

[3] Using Department of Justice guidance, the FBI defines a major system as one that has an annual cost greater than $10 million, a total life cycle cost greater than $50 million, or an annual cost greater than $500,000 for financial information systems; is mandated for departmentwide use; has significant multiple component impact for the department; has legal requirements or designation as a congressional line item; or is high risk or politically sensitive, as determined by the Justice CIO.

the FBI reports it is in the process of acquiring the warehouse and has plans for full deployment by the end of fiscal year 2004.

Some divisions—such as CJIS, Cyber, and Investigative Technology—plan to spend over $70 million each on IT modernization in fiscal year 2005 alone. For instance, the Investigative Technology Division plans to spend approximately $83 million in fiscal year 2005 on three major IT initiatives: Digital Collection, Electronic Surveillance Data Management System, and the Computer Analysis Response Team. Table 2 shows, by FBI division, the major initiatives and their anticipated modernization spending. A description of each initiative is provided in appendix II.

Table 2: Major IT Modernization Initiatives for Fiscal Years 2003-2005 by Division

Dollars in millions

Division/major IT modernization initiatives[a]	Anticipated spending for fiscal years 2003-2005
Counterterrorism	
Foreign Terrorism Tracking Task Force	$15.3
Criminal Justice Information Services	
Integrated Automated Fingerprint Identification System	190.8
National Crime Information Center 2000	14.7
National Instant Criminal Background Check System	104.9
Cyber	
Special Technologies Applications Section	149.4
Information Resources	
Collaborative Capabilities	1.0
Legat/International Infrastructure	10.5
Sensitive Compartmented Information Operational Network	20.2
Investigative Technologies	
Computer Analysis Response Team	105.1
Digital Collection	93.3
Electronic Surveillance Data Management System	26.6
Laboratory	
Combined DNA Index System	22.8
Office of the CIO	
Aurora	8.0

(Continued From Previous Page)

Dollars in millions	
Program Management Office	
Investigative Data Warehousing and Virtual Knowledge Base	53.0
Joint Terrorism Task Force, Information Sharing Initiative	6.5
Trilogy	110.9
Security	
IT Security/Information Assurance	121.2
Security Management Information System	12.6
Total for all major IT modernization initiatives	**$1,066.8**

Source: GAO analysis of FBI data.

[a] Includes modernization initiatives that the FBI designated as major in its budget requests for fiscal years 2003, 2004, or 2005.

Integrated Project Planning and Effective Policies and Procedures Are Essential to Effectively Managing IT Modernization Efforts

Integrated planning across related IT projects and effective policies and procedures for managing IT human capital, systems acquisitions, and investment activities are recognized hallmarks of successful public and private organizations, and they are essential ingredients for effectively managing large modernization efforts. Our research and experience with federal agencies has shown that executing modernization projects without these and other IT management controls increases the chances of implementing systems that are not well integrated and do not provide promised capabilities on time and within budget.[4]

[4] See GAO, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: Feb. 28, 2003); *Business Systems Modernization: IRS Needs to Better Balance Management Capacity with System Acquisition Workload*, GAO-02-356 (Washington, D.C.: Feb. 28, 2002); and *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001).

The Congress and the Office of Management and Budget (OMB) have recognized the importance of these and other IT management controls. The Clinger-Cohen Act,[5] for example, provides a framework for effective IT management that includes systems integration planning, human capital management, acquisition management, and investment selection and control. In addition, OMB has issued guidance on integrated IT modernization planning and effective IT human capital, acquisition, and investment management.[6] Further, organizations such as Carnegie Mellon University's Software Engineering Institute have also issued guidance on effective acquisition management practices for areas such as configuration management, project management, quality assurance, requirements development and management, and risk management.

Prior Reviews Have Identified Challenges Facing the FBI in Modernizing Its IT Environment

Over the past several years, reviews of the FBI's efforts to leverage IT to support transformation efforts have identified management weaknesses. In particular, a December 2001 report[7] initiated by the Department of Justice identified weaknesses with, for example, the bureau's systems acquisition and human capital management processes. The weaknesses included not having (1) a policy that ensures consistent implementation of configuration management activities, (2) processes to ensure adequate definition of system requirements, and (3) an agencywide systems life cycle methodology. The report also noted that the FBI had not assessed the current skills of its employees on an ongoing basis, and it did not have a systematic approach for identifying the skills and abilities needed for the future.

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

[6] See Office of Management and Budget, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C., Nov. 28, 2000) and *Planning, Budgeting, Acquisition, and Management of Capital Assets*, Circular A-11, Part 7 (Washington, D.C., July 2003).

[7] Arthur Andersen, LLP, *Management Study of the Federal Bureau of Investigation* (Dec. 14, 2001).

In December 2002, Justice's Office of the Inspector General reported[8] that the FBI was not effectively managing its IT investments. Specifically, the Inspector General reported that the bureau did not have a complete process for selecting new IT investments and was not following a disciplined process for controlling ongoing projects. To address this, the Inspector General made a series of recommendations aimed at implementing the processes and practices defined in our IT investment management framework.[9] In a January 2004 follow-on report,[10] the Inspector General stated that, while the bureau had developed plans to address these recommendations, full development and implementation of the plans—and thus the establishment of effective investment management processes—remained to be completed.

[8] U.S. Department of Justice Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report 03-09 (Washington, D.C., December 2002).

[9] 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). In March 2004, GAO updated this version: *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

[10] U.S. Department of Justice Office of the Inspector General, *Action Required on the Federal Bureau of Investigation's Management of Information Technology Investments, Audit Report Number 03-09*, (Washington, D.C., January 2004).

More recently, between September 2003 and March 2004, we reported[11] on the challenges the FBI faced in establishing effective IT modernization management. For example, we reported in September 2003 (and again in November) that the bureau had not yet developed a modernization blueprint—commonly referred to as an enterprise architecture[12]—to guide and constrain modernization efforts. Accordingly, we made recommendations to help the bureau establish the architecture management capabilities needed to develop, implement, and maintain an enterprise architecture. The FBI agreed with our recommendations and is in the process of implementing them. In addition, in March 2004,[13] we reported that the FBI has not benefited from having sustained IT management leadership with bureauwide authority. Specifically, the bureau's key leadership and management positions, including the position of the CIO, had experienced frequent turnover, and the position of the CIO lacked bureauwide authority over IT. We found that historically much of the responsibility and authority for managing IT—including modernization planning, human capital management, systems acquisition management, and investment selection and control—was dispersed among the bureau's divisions. We did not make recommendations in these areas at that time because our work to fully evaluate these areas had not yet been completed.

[11] 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); and *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] An enterprise architecture can be viewed as a blueprint that defines, in logical or business terms and in technology terms, how an organization, for example, operates today, how it intends to operate in the future, and how it intends to invest in technology to transition to this future state.

[13] GAO-04-578T.

Shortfalls in the FBI's Centerpiece Systems Modernization Project Are Linked to IT Management Weaknesses

Reviews of the bureau's centerpiece systems modernization project, Trilogy, have identified management weaknesses as the cause for cost, schedule, and performance shortfalls that have been experienced by the project. For example, over the past several years, the Justice Inspector General issued several reports[14] on the FBI's management of Trilogy. According to the Inspector General's September 2003 report,[15] Trilogy funding grew from an original estimate of $379.8 million to $596 million, due in part to the lack of integration planning for one of the three components of Trilogy. In addition, the Inspector General reported that the original delivery date for Trilogy's first two components (Transportation Network Component and Information Presentation Component) slipped 8 months, in part due to inadequately defined requirements. In March 2004, the Inspector General testified[16] that the continued series of missed completion estimates and associated cost growth were due to, among other things, poorly defined requirements, project management deficiencies, frequent turnover of FBI IT managers, and the FBI's focus on its other important law enforcement challenges.

In addition, in September 2003, we reported[17] that the bureau lacked an enterprise architecture—a key component in developing and modernizing systems. We found that the absence of the architecture contributed to unnecessary rework to integrate several modernization initiatives, including Trilogy. In March 2004, we testified[18] that the bureau's weaknesses in IT management controls, such as investment management and enterprise architecture, contributed to Trilogy schedule delays of at least 21 months and cost increases of about $120 million.

[14] 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), Audit Report 03-09, and Action Required on Audit Report 03-09.

[15] Inspector General Audit Report 03-36.

[16] U.S. Department of Justice Office of the Inspector General, *Statement of Glenn A. Fine*, *Inspector General*, *before the Senate Committee on Appropriations*, *Subcommittee on Commerce*, *Justice*, *State and the Judiciary*, (Washington, D.C., Mar. 23, 2004).

[17] GAO-03-959.

[18] GAO-04-578T.

Moreover, the National Research Council reported[19] in May 2004 that the bureau was experiencing significant challenges in developing and implementing Trilogy. For example, the council found that the bureau did not have a permanent CIO with the technical knowledge to provide the strong direction needed for the Trilogy program. In addition, it found that modernization initiatives, such as Trilogy, were not closely linked to a coherent view of the bureau's mission and operational needs. Based on its findings, the council concluded that the bureau was not on the path to success in its IT modernization program. In a follow-on letter,[20] the council cited substantial progress on these fronts. In particular, it said that the bureau had hired a permanent CIO, and the CIO had identified the development of an enterprise architecture as a high priority.

Integrated Project Planning across the FBI Is Not Yet Occurring, but Improvements Are Planned

The Clinger-Cohen Act[21] requires the use of effective IT management practices such as organizationwide planning for the integration of interrelated systems. In addition, OMB provides guidance to federal agencies on such planning.[22] As part of this planning, agencies are supposed to identify, understand, and manage interdependencies within and across individual IT systems modernization projects. Key elements of effective integrated project planning include

- linking all IT projects to the organization's mission and related strategic goals;
- identifying and demonstrating gaps in mission performance due to, among other things, weak or nonexistent integration among existing projects, services, systems, databases, networks, or tools;
- defining interdependencies among IT projects, including the business processes to be supported and technical system interface requirements;

[19] National Research Council, *A Review of the FBI's Trilogy Information Technology Modernization Program*, (Washington, D.C., May 10, 2004).

[20] National Research Council, follow-on report to *A Review of the FBI's Trilogy Information Technology Modernization Program*, (Washington, D.C., June 7, 2004).

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

[22] See Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130 (Washington, D.C., Nov. 28, 2000) and *Planning, Budgeting, Acquisition, and Management of Capital Assets*, Circular No. A-11, Part 7 (Washington, D.C., July 2003).

- assigning responsibilities and management structures for coordinating and overseeing IT project interdependencies;
- identifying the risks associated with project interdependencies and developing strategies to mitigate the risks; and
- ensuring that affected organizations provide input and commitment to plan development and implementation.

Addressing these elements, among other things, identifies the points where systems are to be integrated and establishes common ground for interproject planning and management, which is essential to ensuring that project plans—and thus system solutions—are effectively integrated. Our prior reviews at federal agencies and research on IT management have shown that attempting to modernize IT systems without performing such planning increases the risk of investing in system solutions that are duplicative, are not well integrated, are unnecessarily costly to maintain and interface, and do not effectively optimize mission performance. Accordingly, until agencies develop integrated approaches, we have recommended[23] limiting IT spending to cost-effective efforts that are congressionally directed; are near-term, relatively small, and low-risk opportunities to leverage technology in satisfying a compelling agency need; support operations and maintenance of existing mission-critical systems; involve deploying an already developed and fully tested system; or support establishing integrated planning and other modernization management controls and capabilities.

The FBI does not have a bureauwide integrated plan or set of plans for its many systems modernization projects. Instead, divisions have developed modernization plans covering solely those IT projects that are within their respective lines of authority. These plans include (1) division plans that describe to varying degrees how IT projects are to be executed to support the accomplishment of division-specific objectives and (2) capital asset plans and business cases—commonly referred to as budget Exhibit 300s—that justify the resources needed for the division's major IT projects. However, these plans are not integrated and do not consistently

[23] See GAO, *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems*, GAO-04-509 (Washington, D.C.: May 21, 2004), and *Tax Systems Modernization: Blueprint Is a Good Start, but Not Yet Sufficiently Complete to Build or Acquire Systems*, GAO/AIMD/GGD-98-54 (Washington, D.C.: Feb. 24, 1998).

demonstrate the elements of integrated IT project planning. Specifically, of the six FBI divisions we examined, two divisions—Cyber and CJIS—included the majority of the elements of integrated project planning, while the other four divisions each incorporated two or fewer of the elements. Table 3 summarizes our analysis.

Table 3: Extent to Which Divisions' Plans Address Modernization Planning Elements

	Division					
	Cyber	CJIS	Information Resources	Investigative Technology	Program Management Office	Security
Link projects to mission and strategic goals	✔				✔	
Identify and demonstrate performance gaps		✔				✔
Define interdependencies among projects	✔	✔				
Assign responsibility for managing project interdependencies		✔				✔
Identify risks with interdependencies and develop strategies to mitigate the risks	✔	✔		✔	✔	
Ensure affected organizations provide input and are committed	✔	✔				

Source: GAO analysis of FBI data.

Note: ✔ indicates criteria met.

More specifically, our analysis for each of the modernization planning elements showed the following:

- With respect to the first element, two divisions—Cyber and the Program Management Office—consistently linked their projects to either the bureau's strategic plan or its top 10 priorities. The other divisions linked at least some of their individual projects to bureau-level strategy. Linking individual projects to the FBI's strategic plan is an essential step to ensuring that the bureau IT initiatives do not overlap or leave gaps in mission functions and goals.

- Only two divisions (CJIS and Security) identified and demonstrated gaps in existing capabilities. CJIS undertook an analysis of system deficiencies and technology trends to identify and specify improvements to its law enforcement systems. Security relied on prior reviews of security incidents and comparisons of existing practices with best practices to identify needed improvements in system security requirements. Other divisions largely stated the need for improvements in system capabilities and capacity without corresponding data on current or projected mission shortfalls. This is crucial because without supporting data to derive performance gaps, proposed improvements may be unnecessary, insufficient, or not identified at all. In addition, our research and experience[24] with federal IT modernizations show that projects with inadequately defined improvements are likely to require more resources to plan and manage—including planning and management of interdependencies—than those that have been based on reliable performance data and thorough analysis.

- All of the divisions addressed the third element, in part, but only two divisions—Cyber and CJIS—fully identified interdependencies for all of their projects. For example, CJIS identified interrelationships among business processes, systems, databases, networks, components, and tools. The Investigative Technology Division, on the other hand, did not consistently identify interdependencies for tools, networks, or security. In addition, Security did not fully identify technical and programmatic interdependencies. Identifying project interdependencies is essential for recognizing the points of integration of projects and systems and for establishing common ground for interproject planning and management.

- The CJIS and Security divisions had the most robust mechanisms for coordinating their project interdependencies with other parts of the bureau and with external organizations. CJIS relies on its Advisory Policy Board to identify needed improvements, assess impacts to customers and their systems, and coordinate schedules and interfaces. Security collaborates with system owners and managers through

[24] See, for example, GAO, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: Feb. 28, 2003); *Business Systems Modernization: IRS Needs to Better Balance Management Capacity with System Acquisition Workload*, GAO-02-356 (Washington, D.C.: Feb. 28, 2002); and *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001).

division configuration and change control boards, the security certification and accreditation process, and other mechanisms to integrate its security projects and information assurance objectives. Both divisions have well-defined responsibilities for their project team members. Other divisions focused on coordination within individual project teams or a single division, leaving mechanisms for interacting with other divisions, systems, and technologies poorly defined. This is important because vague responsibilities and processes for managing project integration efforts can lead to omissions and conflicts in system interfaces and project activities.

- The fifth element was satisfied by four of the six divisions. Specifically, Cyber, CJIS, Investigative Technology, and the Program Management Office consistently addressed integration risks in their capital asset plans and business cases. Doing this is important because it allows for the systematic identification of risks associated with project interdependencies and management action to mitigate those risks.

- Finally, the CJIS and Cyber divisions enlisted participation and commitment from organizations affected by their projects and related system improvements. For instance, CJIS partnered with the advisory boards and councils, the vendor community, and the nation's criminal justice community in successfully developing its systems. Other divisions, such as Investigative Technology and the Program Management Office, fell short of meeting this criterion because they did not consistently specify a means for project personnel to collaborate with other stakeholders on the development of integrated project plans. Establishing such a means for knowledgeable personnel to contribute to planning for interdependencies in areas such as project requirements, interfaces, and timetables is key to ensuring stakeholder commitment to project integration plans and their execution.

FBI officials from each of the divisions agreed with the results of our analyses of their respective planning efforts and attributed the state of their planning to several factors. First, as we previously reported,[25] the FBI does not have an enterprise architecture, and thus business processes and IT systems have been viewed parochially, rather than as corporate resources that must be planned and managed on a bureauwide basis. Second, no bureau policy exists for divisions to develop integrated IT project plans.

[25] GAO-03-959.

Instead, existing policy assigns responsibility for IT planning, including planning for modernization projects, to divisions. Third, the bureau has not assigned responsibility and authority for ensuring that integrated bureauwide planning occurs. While the divisions are responsible for project planning, no organization is responsible for reviewing and approving the divisions' plans to ensure that mission gaps across the bureau are fully addressed and project dependencies and overlap are minimized.

According to the CIO, several efforts are underway and planned to address these underlying weaknesses and strengthen modernization planning. Consistent with our prior recommendations, the FBI has established a program to develop an enterprise architecture. In doing so, the bureau has, among other things, (1) established a program office to manage the effort, (2) assigned a chief architect and supporting personnel, (3) established an architecture governance board that includes representatives from all divisions to review and identify projects that are inconsistent with the existing IT environment and inhibit internal and external information sharing, and (4) hired a contractor to assist with developing the architecture. The bureau plans to issue the first version of the architecture by the end of September 2004. This version is to document the bureau's current IT environment. The bureau plans to issue the other key parts of the architecture—namely, the future IT operating environment and transition plan—in fiscal year 2005.

Also, the CIO is in the process of merging agencywide authority and responsibility for IT, including systems modernization planning, under the CIO in time to be reflected in the bureau's fiscal year 2006 budget and associated capital investment plans and business cases. Further, the CIO's office intends to hire a contractor to facilitate bureauwide integrated planning, including the formulation of integrated plans for systems modernization projects.

Until the FBI completes these and other efforts to introduce an integrated approach to IT project planning, there is increased risk that the bureau's IT systems will be unnecessarily duplicative, will later require expensive rework to be integrated, and will thus hamper organizational transformation efforts. According to the FBI, this risk has already become reality in the case of five key infrastructure projects (including Trilogy and the Integrated Data Warehouse) that were launched independently between May 2001 and June 2003 and later found to have significant areas of overlap. The FBI attributed the redundancy in part to the lack of integrated planning.

Policies and Procedures Governing Key Systems Modernization Management Capabilities Are Partially in Place and Further Improvements Are Planned

Establishing effective corporate policies and procedures for managing IT human capital, acquiring systems, and making investment decisions are examples of key best practices that leading organizations use to modernize their IT systems and facilitate organizational transformation. The FBI has such policies and procedures for managing IT human capital; however, it does not yet have a documented and consistent approach for acquisition and investment management. Specifically, adoption of best practices for acquisition management policies and procedures in such areas as configuration management and quality assurance varies among divisions, and bureau investment management policies and procedures, including selection and control processes, are still under development. The state of the FBI's acquisition and investment management policies and procedures is due to a number of factors, including diffused and decentralized IT management authority, past inattention to IT management, and lack of sustained IT leadership. The CIO has recently taken steps to strengthen policies and procedures in each of these areas. Until this is completed, the bureau will be challenged in its ability to effectively manage all of its systems modernization projects, and thus is at increased risk of acquiring systems that do not adequately satisfy mission needs on schedule and within budget, which could hamper the bureau's systems modernization and organizational transformation.

Strategic IT Human Capital Management Policies and Procedures Have Been Developed

As we have previously reported,[26] strategic human capital management includes viewing people as assets whose value to an organization can be enhanced by investing in them. As the value of people increases, so does the performance capacity of the organization. In March 2002, GAO, based on our experience with leading organizations, issued a model[27] with four cornerstones[28] encompassing strategic human capital management. One of the cornerstones, strategic workforce planning (also called 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. In December 2003, GAO issued a set of key principles, or practices, for effective strategic human capital planning.[29] These practices include

- involving top management, employees, and other stakeholders in developing, communicating, and implementing a strategic workforce plan;
- determining the critical skills and competencies that will be needed to achieve current and future programmatic results;
- developing strategies that are 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 made to achieving programmatic goals.

[26] 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); and *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[27] GAO-02-373SP.

[28] The four human capital cornerstones are leadership; strategic human capital planning; acquiring, developing, and retaining talent; and results-oriented organizational cultures.

[29] GAO-04-39.

These practices are generic and apply to any organization or organizational component, such as an agency's IT organization.

The bureau has developed IT human capital policies and procedures and incorporated them into the bureau's enterprisewide strategic human capital plan issued in March 2004.[30] These IT policies and procedures are in alignment with the key best practices discussed above. For example, they call for 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) to be involved with the development, communication, and implementation of these policies and procedures. Further, the policies and procedures provide for the development of a detailed data bank to store critical skills needed in the development and selection of personnel, including IT staff. They also define strategies to address workforce gaps, including recruiting programs that provide for tuition assistance and cooperative education. In addition, the policies and procedures call for establishing an IT center to support workforce strategies and train existing personnel for future competencies and skills that will be needed. Further, the policies and procedures require monitoring and evaluating the agency's progress by tracking implementation plans to ensure that results are achieved on schedule.

The FBI will face challenges as it implements its strategic IT human capital policies and procedures. As we have previously reported,[31] when implementing new human capital policies and procedures, how it is done, when it is done, and the basis on which it is done can make all the difference in whether such efforts are successful. With successful implementation, the bureau can better position itself to ensure it has the right people, in the right place, at the right time to effectively modernize IT and transform the organization.

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

[31] GAO-04-578T.

Use of Best Practices in Systems Acquisition Policies and Procedures Varies Widely among the Divisions

The Clinger-Cohen Act[32] requires, among other things, the establishment of effective IT management policies and procedures. The Software Engineering Institute's Capability Maturity Models™[33] provide for 30 best practice policies and procedures for five key systems acquisition management areas—configuration management, project management, quality assurance, requirements development and management, and risk management. Collectively, these management areas and associated best practices provide a foundation for

- acquiring systems that allow organizations to manage changes to the system configurations;
- tracking project cost, schedule, and performance;
- defining standards to ensure integrity in products;
- establishing clearly defined and managed requirements; and
- identifying and mitigating risks.

Each management area has five to seven best practices associated with it that, when properly defined and implemented, assist organizations in performing effectively in that area. A detailed list of the practices, by management area, is in appendix III.

The acquisition management policies and procedures currently in place at the FBI for these five areas vary widely by division. While each of the six divisions we examined has policies and procedures that incorporate many best practices, these divisions' policies and procedures also do not address important practices. For example, in project management, the divisions' policies and procedures generally addressed all of the best practices. Conversely, in requirements development and management, four of the six

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

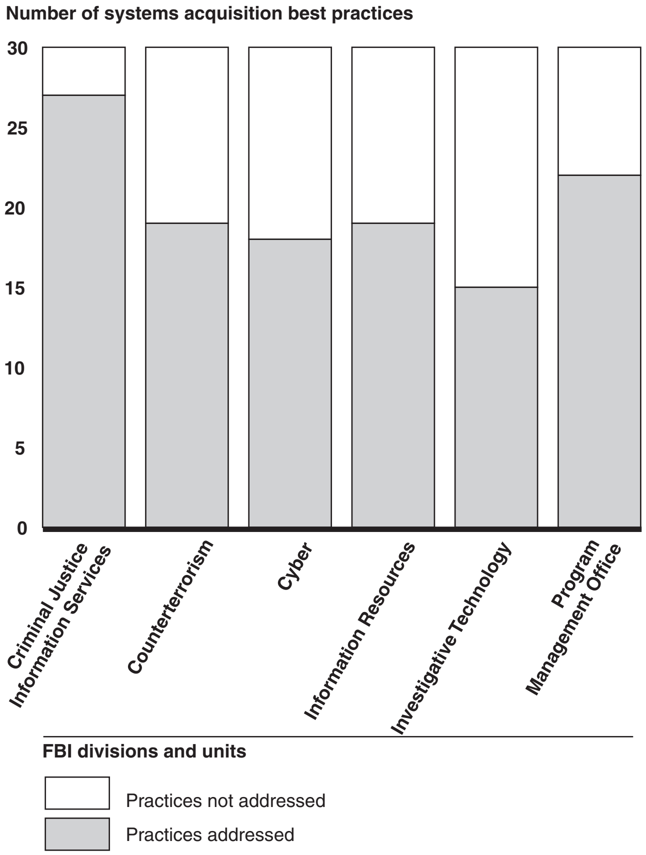
[33] Carnegie Mellon University's Software Engineering Institute has developed criteria, known as the *Software Acquisition Capability Maturity Model* (CMU/SEI-99-TR-002, April 1999) and *Key Practices of the Capability Maturity Model* (CMU/SEI-93-TR-25, February 1993) for determining organizations'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

divisions' policies and procedures addressed fewer than half of the best practices for that area. See figure 2 for a summary of our analysis.

The FBI attributed the variance among divisions and the lack of alignment with best practices to, among other things, the bureau's decentralized approach to managing IT and past inattention given to IT management. Until recently, authority for managing IT, along with budget control, was diffused and decentralized among the divisions. In addition, the FBI did not establish bureauwide policies and guidance for developing systems acquisition policies and procedures consistently and in accordance with best practices. As such, the divisions defined policies and procedures independently from one another, contributing to different sets of policies and procedures.

To strengthen the FBI's systems acquisition capabilities, the CIO has efforts planned and under way to define and implement bureauwide systems acquisition policies and procedures that are to incorporate best practices. Until this is accomplished, the bureau will be challenged in its ability to manage all of its systems modernization projects and thus is at increased risk that it will be unable to deliver promised capabilities on time and within budget.

Figure 2: Extent to Which Six FBI Divisions' Systems Acquisition Policies and Procedures Address Best Practices



Source: GAO analysis of FBI data.

The analyses in the following sections show the variance among divisions in their use of best practices for the five acquisition management areas: configuration management, project management, quality assurance, requirements development and management, and risk management. An analysis of each division is in appendix III.

Configuration Management

Configuration management involves identifying the configuration (i.e., descriptive characteristics of a system) at a given point in time, systematically controlling changes to that configuration, and maintaining the integrity of the configuration throughout the system's life cycle. Effective policies and procedures for configuration management[34] include the following practices:

1. defining roles and responsibilities, including identifying a person or group with authority for managing a system's baselines and approving changes to the baselines;

2. developing a plan that defines the activities to be performed, the schedule of the activities, and the resources required (e.g., staff);

3. establishing a repository (also called a library), using tools and procedures to store and retrieve the configuration and to maintain control over changes to it;

4. identifying, documenting, managing, and controlling configuration items and their associated baselines;

5. managing system change requests and problem reports by ensuring that configuration changes are initiated, recorded, reviewed, approved, and tracked;

6. periodically reporting status of the configuration; and

7. periodically auditing baselines, including assessing the integrity and correctness of baselines, reporting audit results, and tracking audit action items to closure.

The policies and procedures for three of the six divisions addressed these seven best practices, while policies and procedures for two divisions addressed all but one or two of the practices. The remaining division's policies and procedures addressed just one of the seven practices. See figure 3 for a summary of our analysis.

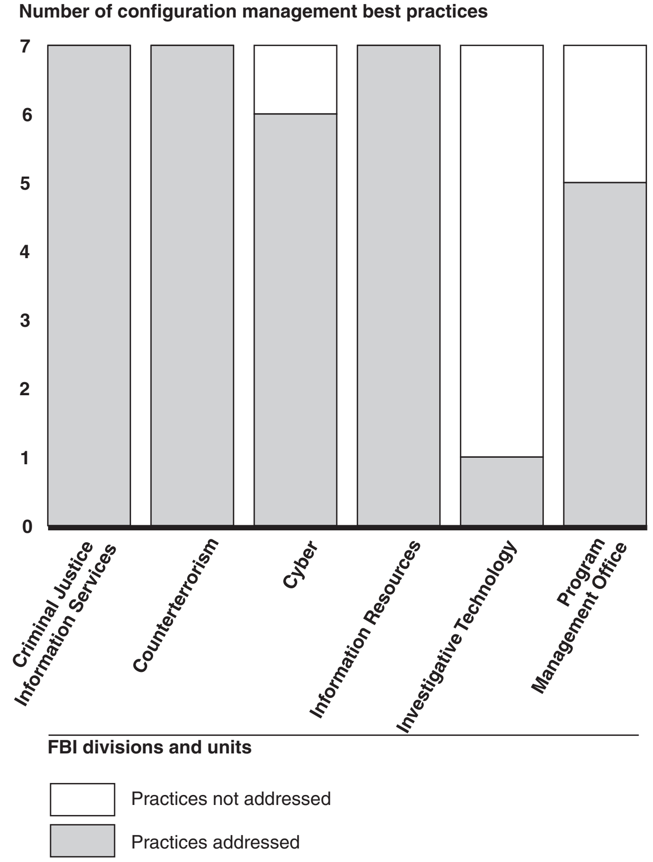
The key practices that are not addressed in division policies and procedures are important and their absence can negatively impact the

[34] See *Key Practices of the Capability Maturity Model* (CMU/SEI-93-TR-025, February 1993).

divisions' ability to effectively manage the configuration of their respective systems and thus their systems' ability to efficiently and effectively support division objectives. In particular, Investigative Technology's policies and procedures did not identify configuration management roles and responsibilities. This is important because project teams need to have a responsible party for approving and controlling changes. To do otherwise would allow anyone to make random changes to the configuration, potentially causing unnecessary rework and reconfiguration. As another example, this division's policies and procedures did not establish a library system. This is also critical to successful configuration management because the library system stores the initial configuration of the system as well as any subsequent changes. Without the library system, the project team would be unable to ensure the correctness of the current configuration.

In addition, the Program Management Office's policies and procedures did not provide for periodic baseline auditing and periodic management review of the status of configuration management activities. These practices are important because they verify that projects are in compliance with applicable configuration management standards and procedures, and they provide awareness of and insight into systems process activities at the appropriate level and in a timely manner.

Figure 3: Extent to Which Six FBI Divisions' Systems Acquisition Policies and Procedures Address Configuration Management Best Practices



Source: GAO analysis of FBI data.

Project Management

The purpose of project management is to manage the activities of the project office and supporting organization to ensure a timely, efficient, and effective acquisition. Effective policies and procedures for project management[35] include the following practices:

1. identifying project management roles and responsibilities;

2. developing a project management plan;

[35] See *Software Acquisition Capability Maturity Model* (CMU/SEI-99-TR-002, April 1999).

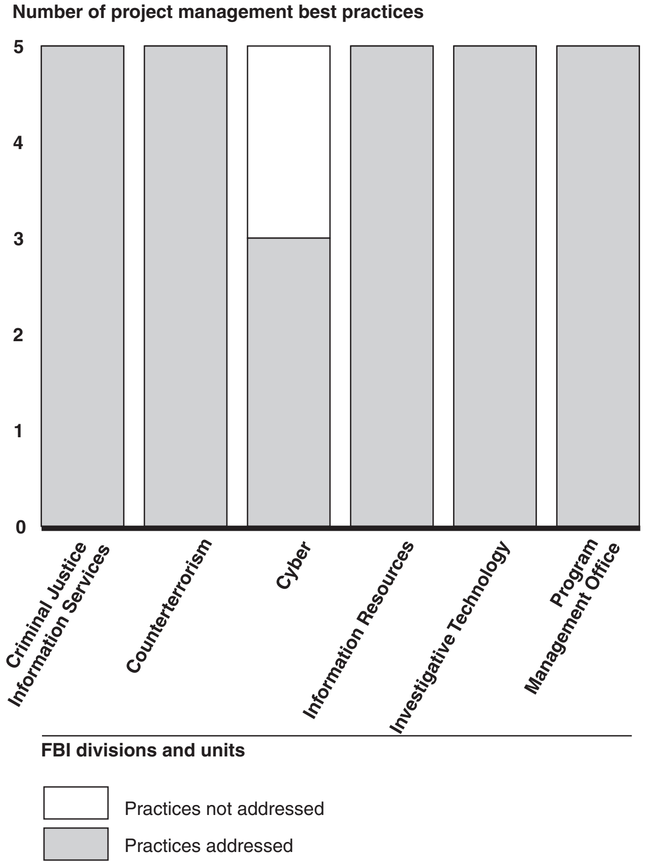
3. baselining and tracking the status of project cost, schedule, and performance, including associated risks;

4. establishing a process to identify, record, track, and correct problems discovered during the acquisition; and

5. periodically reviewing and communicating the status of project management activities and commitments with management and affected groups.

The policies and procedures for five of the six divisions addressed all five of these project management practices; one division did not address two practices. Specifically, Cyber's policies and procedures did not identify processes for baselining and tracking project cost, schedule, performance status, and associated risks. See figure 4 for a summary of our analysis. This practice is important because it provides measurable benchmarks against which to gauge progress, identify deviations from expectations, and permit timely corrective action to be taken. Without this practice, the chances of system projects costing more than budgeted, taking longer than envisioned, and not performing as intended are greatly increased. The division's policies and procedures also did not provide for a process to identify, record, track, and correct problems. This practice is important because it provides for systematically managing and controlling issues that impact cost, schedule, or performance.

Figure 4: Extent to Which Six FBI Divisions' Systems Acquisition Policies and Procedures Address Project Management Best Practices



Source: GAO analysis of FBI data.

Quality Assurance

Quality assurance describes processes for providing independent assessments of whether management process requirements are being followed and whether product standards and requirements are being satisfied. Effective quality assurance policies and procedures[36] include the following practices:

1. identifying quality assurance roles and responsibilities;

[36] See *Key Practices of the Capability Maturity Model* (CMU/SEI-93-TR-025, February 1993).

2. having a quality assurance plan;

3. participating in the development and review of plans, standards, and procedures;

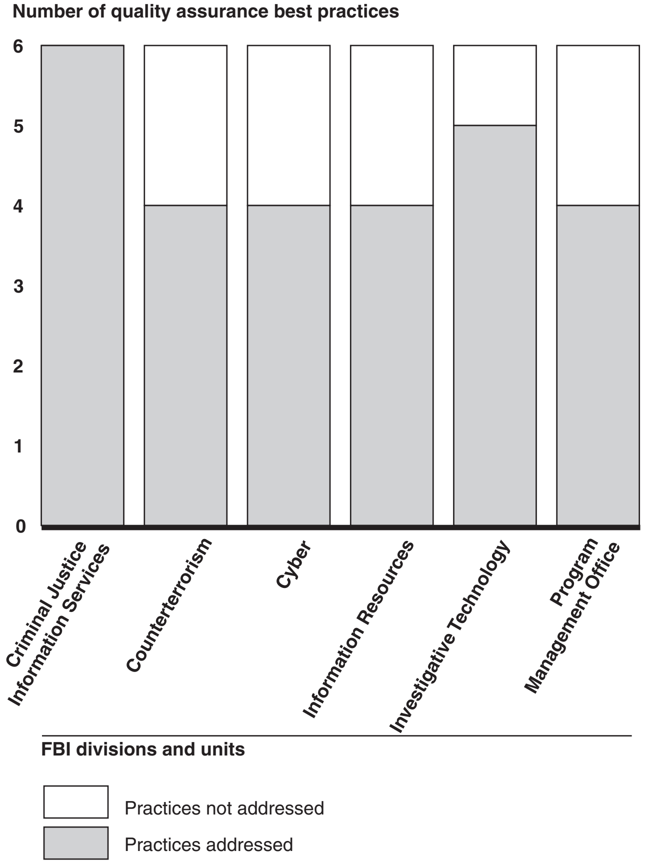
4. reviewing work activities and products;

5. documenting and handling deviations from standards and procedures that are found in activities and work products; and

6. periodically reporting and reviewing the results and findings of quality assurance activities with management.

One division has incorporated these six quality assurance practices in its policies and procedures; the remaining five divisions included all but one or two. See figure 5 for a summary of our analysis. For example, the policies and procedures for Counterterrorism and Information Resources do not address participating in the development and review of plans, standards, and procedures, which is key to ensuring that they are aligned with relevant systems acquisition policies, are appropriately tailored to meet project needs, and are usable for performing quality reviews and audits. In addition, the policies and procedures for Cyber, Investigative Technology, and the Program Management Office do not include periodic reporting and reviews of the results and findings of quality assurance activities. This practice is important to ensuring that issues and concerns that could impede quality outcomes are disclosed so that appropriate corrective action can be taken. If they are not disclosed, the chances of system cost, schedule, and performance shortfalls are increased.

Figure 5: Extent to Which Six FBI Divisions' Systems Acquisition Policies and Procedures Address Quality Assurance Best Practices



Source: GAO analysis of FBI data.

Requirements Development and Management

Requirements development and management involves establishing and maintaining agreement on what the system is to do (functionality), how well it is to do it (performance), and how it is to interact with other systems (interfaces). Effective policies and procedures for requirements development and management[37] include the following practices:

[37] See *Software Acquisition Capability Maturity Model* (CMU/SEI-99-TR-002, April 1999).

1. identifying requirements development and management roles and responsibilities;

2. involving end users in development of and changes to requirements;

3. having a requirements management plan;

4. developing and baselining requirements, and controlling changes to them;

5. appraising changes to requirements for their impact on the project or IT environment;

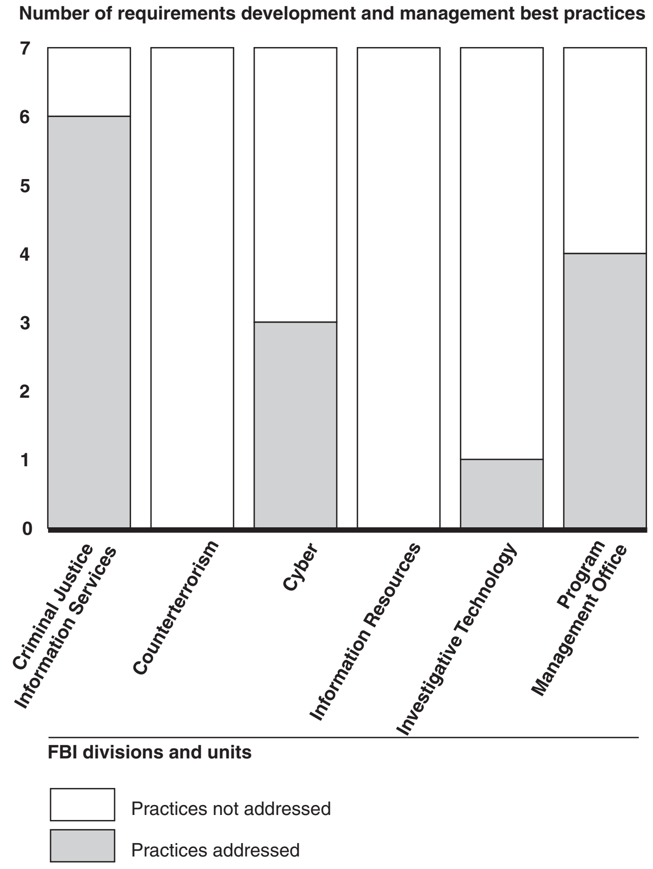
6. maintaining traceability among requirements and other project deliverables; and

7. periodically reviewing the status of requirements activities with management.

With one exception (CJIS), the policies and procedures for the divisions generally did not address the above practices. See figure 6 for a summary of our analysis. For instance, while the Program Management Office's policies and procedures met four of the seven practices, such as involving end users in development of and changes to the requirements and reviewing the status of project requirements activities with management, they did not address maintaining traceability among requirements and other project deliverables. This practice is important because it ensures that project deliverables used to acquire systems are consistent with end user needs, which is critical to delivering systems that perform as intended and thus meet mission needs.

Moreover, the policies and procedures of four divisions—namely Counterterrorism, Cyber, Information Resources, and Investigative Technology—satisfied three or fewer of the practices. For example, none of the four divisions' policies and procedures addressed appraising changes to requirements for their impact on the project or the IT environment. Appraising changes is important because it allows management and the project team to determine whether changes to the requirements, along with their associated effect on the existing IT environment as well as project cost and schedule estimates, would be worthwhile. Additionally, Investigative Technology was missing six of seven practices, including developing and baselining requirements and maintaining them under change control. These practices are essential to ensuring that requirements are completely and correctly defined and that uncontrolled changes, commonly referred to as “requirements creep,” are mitigated.

Figure 6: Extent to Which Six FBI Divisions’ Systems Acquisition Policies and Procedures Address Requirements Development and Management Practices



Source: GAO analysis of FBI data.

The actual consequences of not having effective requirements development and management policies and procedures can be seen in the performance of the bureau’s Trilogy project, which is to replace aging systems infrastructure and consolidate and modernize key investigative case management applications. The FBI reported that, as of August 2004, Trilogy has experienced a delay of at least 21 months and a cost increase of $201 million. According to the CIO, the project's added time and cost were due in large part to requirements development and management process weaknesses.

Risk Management

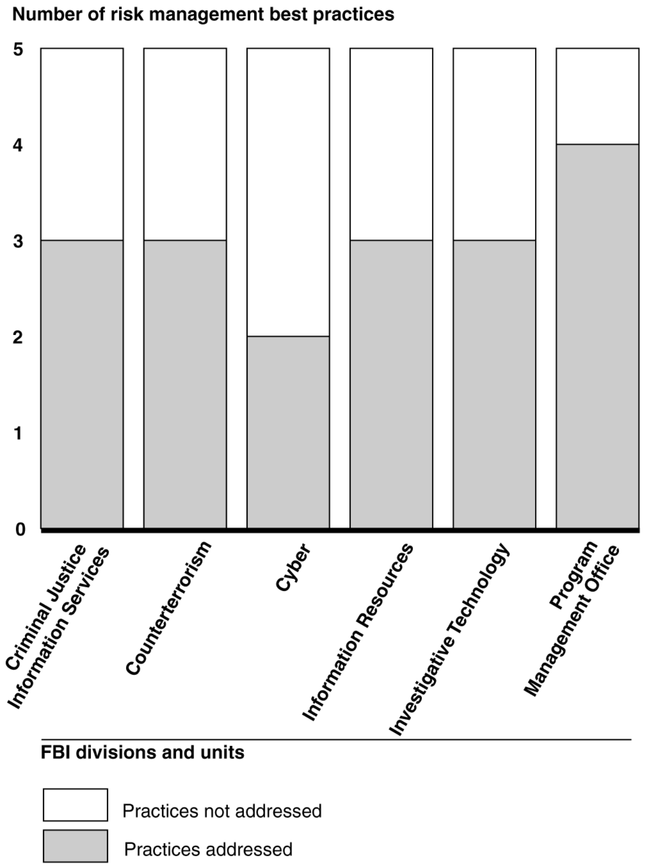
Managing risks means proactively identifying facts and circumstances that increase the probability of failing to meet system expectations and commitments and taking steps to prevent failures from occurring. Effective policies and procedures for risk management[38] include the following practices:

1. identifying risk management roles and responsibilities;
2. having a risk management plan;
3. integrating risk management with other management and planning functions;
4. identifying, analyzing, controlling, and mitigating project risks; and
5. periodically reviewing the status of project risks and risk mitigation activities with management.

The policies and procedures of all six divisions incorporate two or more of the five risk management best practices. See figure 7 for a summary of our analysis. However, key practices were not addressed. For example, all of the divisions' policies and procedures do not provide for integrating risk management with other planning and management functions. This practice is important because it ensures that possible risks and mitigation strategies are adequately provided for in project planning schedule estimates and identified risks are assessed for impact to the organization's IT environment. In addition, the policies and procedures of Counterterrorism, Cyber, and Information Resources do not provide for periodically reviewing the status of project risks and risk mitigation activities with management, a process that is key to ensuring that management is aware of risks to the project, plans to mitigate these risks, and the status and progress of mitigation activities.

[38] See *Software Acquisition Capability Maturity Model* (CMU/SEI-99-TR-002, April 1999).

Figure 7: Extent to Which Six FBI Divisions' Systems Acquisition Policies and Procedures Address Risk Management Best Practices



Source: GAO analysis of FBI data.

IT Investment Management Policies and Procedures Are Evolving Slowly toward Alignment with Best Practices

The Clinger-Cohen Act of 1996[39] provides an important framework for effective investment management. It requires federal agencies to focus on the results they achieve through IT investments while concurrently improving their acquisition processes. It also requires discipline and structure in how agencies select and control investments. In May 2000, we issued a framework[40] (which we updated in March 2004) that encompasses IT investment management best practices, including investment selection and control policies and procedures, and is based on our research at successful private and public sector organizations. This framework is consistent with the Clinger-Cohen Act and identifies, among other things, effective policies and procedures for developing an enterprisewide collection—or portfolio—of investments to enable an organization to determine priorities and make decisions across investment categories based on analyses of the relative organizational value and risks of all investments. These portfolios include three types of IT investments—planned (proposed systems or system enhancements), under way (systems under development), and completed (existing systems). The framework also calls for integrating and overseeing these investments to manage the complete portfolio of investments.

The bureau's efforts to define IT investment policies and procedures are evolving slowly toward alignment with best practices. Specifically, according to officials from the CIO's office, the bureau has had three separate and sequential efforts to develop its investment management process. The first effort started in December 2001, when the bureau developed an investment management and transition plan. This plan called for establishing and defining bureau policies and procedures for the select, control, and evaluate steps set forth in GAO's framework. In March 2002, the FBI completed the definition of select phase procedures and began pilot testing them in developing its fiscal year 2004 IT budget request for new investments and legacy (existing) system enhancements bureauwide. The bureau completed the pilot in May 2002, but efforts to further define policies and procedures for the control and evaluate phases stalled and were not fully completed.

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

[40] 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). In March 2004, GAO updated this version: *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

In early 2003, the bureau began its second effort—shifting focus on its investment management process by initiating development of a new process for investing in IT and other non-IT assets such as buildings and plant equipment. According to officials from the CIO's office, development of the process stalled at the end of 2003, before it could be fully implemented.

In early 2004, the bureau started its third and current effort. The FBI decided to have separate policies and procedures for IT due to the differences in IT and non-IT investments. According to the CIO, the bureau's current processes for IT investment management include one for investments that are planned and under way and another for maintenance of existing systems. The process for investments that are planned and under way is still being defined. The CIO has established a program office and has allocated staff, but the work is just beginning and is not planned to be completed until the second quarter of fiscal year 2005. For existing systems, the bureau developed a set of policies and procedures that define a process to allocate operations and maintenance resources against competing needs by assessing the performance of existing systems. The bureau is piloting the process on different types of systems (e.g., application, infrastructure) with the goal of enterprisewide implementation by April 2005. Between June and December 2003, the program office tested the procedures on Information Resources application systems. A second pilot was recently initiated in April 2004 on Information Resources infrastructure systems, with the goal of completing the test by November 2004. According to the CIO, the bureau has hired a contractor to assist with enterprisewide rollout, which began in June, and is also in the process of acquiring a tool to manage its IT investment portfolio.

According to bureau officials, including the current CIO, the slowly evolving state of investment management is due in part to the fact that the bureau CIO position, which is responsible for developing the requisite policies and procedures, has had a high rate of turnover. Specifically, the CIO has changed five times in the past 2 1/2 years. As a result, development of investment management policies and procedures has not benefited from sustained management attention and leadership, and thus has shifted focus repeatedly and lagged. Until planned and ongoing improvements are completed, the FBI will lack effective controls over its IT investments and thus will be unable to ensure that the mix of investments it is pursuing is the best to meet the bureau's goals for modernizing IT and transforming the organization.

Improvements Are Planned for Developing Systems Modernization Management Capabilities

The CIO has acknowledged the weaknesses in systems acquisition management and investment management and has improvements planned to strengthen them. For example, according to the CIO, the FBI is establishing a strategic planning process as part of a bureauwide IT management effort. The CIO also said that the results of the strategic planning process will be used to guide the enterprise architecture and IT investment management. In putting this process in place, the FBI has drafted an IT strategic plan (to be issued in September 2004) that outlines ongoing and planned efforts to strengthen both investment management and systems acquisition policies and procedures by standardizing them across the bureau and incorporating best practices such as GAO's investment management model and best practices in configuration management and quality assurance. In addition, the CIO has begun efforts to establish bureauwide requirements development and management policies and procedures by developing a process for requirements definition—the first step in developing requirements. The CIO has also drafted a life cycle management process that is to integrate systems acquisition management, investment management, and other key IT domain areas, such as IT strategic planning and enterprise architecture. According to the CIO, this integration is to be completed by the end of 2006.

These improvements, if properly defined and implemented, will increase the FBI's modernization management capabilities. However, we remain concerned about their completion for several reasons. First, the improvements have yet to be completely defined and implemented. In addition, other key ingredients to effective IT management—development of a modernization blueprint and the establishment of integrated project planning—are not yet in place. Further, as discussed earlier, the FBI has had problems sustaining leadership and management attention for similar IT improvements.

Conclusions

The FBI is beginning to lay the management foundation needed for comprehensive improvements in its systems modernization management approach and capabilities. The foundational steps are in appropriate areas, such as development of a modernization blueprint (enterprise architecture), initiation of integrated project planning, and establishment of IT management policies and procedures for human capital, systems acquisition, and investment selection and control. However, the steps still need to be fully defined and properly implemented across the bureau to produce the integrated systems environment needed to optimally support mission needs and produce system investments that deliver expected capabilities and mission benefits on time and within budget and thus support the organizational transformation. This will require senior executive leadership and commitment and provision of sufficient CIO authority to fully define and institutionalize effective IT management approaches and capabilities bureauwide. Such commitment includes vesting accountability and responsibility for managing IT under the CIO—including budget management control and oversight of IT programs and initiatives—and aligning modernization planning and management policies and procedures with the best practices of leading organizations. Until this occurs, the bureau will remain challenged in its ability to effectively and efficiently manage its systems modernization efforts, and thus its near-term investments in modernized systems will remain at risk.

Recommendations for Executive Action

Until the bureau's IT management foundation is completed and available to effectively guide and constrain the hundreds of millions of dollars it is spending on IT investments, we recommend that the Director direct the heads of the divisions to limit spending on their respective IT investments to cost-effective efforts that

- are congressionally directed;
- take advantage of near-term, relatively small, low-risk opportunities to leverage technology in satisfying a compelling bureau need;
- support operations and maintenance of existing systems critical to the FBI's mission; or
- support establishment of the FBI's IT management foundation, including the development of a modernization blueprint (enterprise architecture), initiation of integrated project planning, and development of IT management policies and procedures for systems acquisition and investment selection and control.

In establishing the management foundation, we recommend that the FBI Director provide the CIO with the responsibility and authority for managing IT bureauwide, including budget management control and oversight of IT programs and initiatives.

In addition, we recommend that the FBI Director, with assistance from the CIO, ensure that future and ongoing modernization plans and efforts are effectively integrated by taking five actions: (1) establishing a bureauwide requirement (policy) to develop an integrated plan (or set of plans) for modernization investments, (2) developing corresponding guidance on plan contents and scope, (3) ensuring the appropriate resources and training are available to implement policy and guidance, (4) assigning responsibility and accountability for developing the plans, and (5) assigning responsibility and accountability to the CIO for reviewing the plans to ensure adherence to the policy and guidance, including alignment with the bureau's enterprise architecture.

We also recommend that the FBI Director, with the CIO's assistance, take four actions to ensure that the bureau establishes effective policies and procedures for systems acquisition and investment management selection and control. With regard to systems acquisition, we recommend (1) correcting the weaknesses in configuration management, project management, quality assurance, requirements development and management, and risk management policies and procedures described in this report's body and detailed in appendix III and implementing the resulting changes accordingly; and (2) assessing the other divisions that manage IT investments to determine whether their policies and procedures align with best practices and, to the extent there are gaps, correcting them. With regard to IT investment management, we recommend (3) developing the bureau's investment management processes in accordance with key IT investment decision-making best practices, such as GAO's IT investment management framework; and (4) identifying, and acting on, options for speeding up their implementation.

Agency Comments and Our Evaluation

In its written comments on a draft of this report, which were signed by the CIO and are reprinted in appendix IV, the FBI agreed that the bureau is taking steps to lay the management foundation for improving IT operations. The FBI also agreed that, while progress is being made, much work remains to implement and institutionalize planned and ongoing IT management improvements. It stated that our recommendations are consistent with the FBI's internal reviews and with those of other oversight entities. In addition, the FBI described actions planned and under way to address our recommendations and provided technical comments, which we have incorporated, as appropriate, in the report.

We are sending copies of this report to the Chairman and Vice Chairman of the Senate Select Committee on Intelligence, and the Chairman and Vice Chairman of the House Permanent Select Committee on Intelligence. We are also sending copies to the Attorney General; the Director, FBI; the Director, Office of Management and Budget; and other interested parties. The report will also be available without charge on GAO's Web site at http://www.gao.gov.

Should you have any questions about matters discussed in this report, please contact me at (202) 512-3439 or by e-mail at hiter@gao.gov. Key contributors to this report are listed in appendix V.

Randolph C. Hite

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

Objectives, Scope, and Methodology

As agreed with your offices, our objectives were to examine whether the FBI has (1) an integrated plan for modernizing its IT systems, and (2) effective policies and procedures governing management of IT human capital, systems acquisition, and investment selection and control. For the first objective, we focused on the bureau's IT modernization plan and supporting documents. In light of the FBI's response that its divisions were responsible for modernization planning, we included six divisions in our scope of work—Criminal Justice Information Services (CJIS), Cyber, Information Resources, Investigative Technology, the Program Management Office, and Security—because they had the largest planned or ongoing IT modernization investments. For the second objective, we focused on the bureau's policies and procedures for IT human capital, systems acquisition, and investment selection and control. In response to this request, bureau officials told us that systems acquisition policies and procedures were developed within each division. To obtain a crosscutting sample, we analyzed the systems acquisition policies and procedures of at least one division with major IT modernization investments from each of the components,[1] based on funding for fiscal years 2003 through 2005; thus, the scope for systems acquisition included Counterterrorism, CJIS, Cyber, Information Resources, Investigative Technology, and the Program Management Office.

To address the first objective—determining whether the FBI had an integrated plan or set of plans for modernizing its IT systems—we reviewed program plans, IT capital asset plans and business cases (commonly called Exhibit 300s), and other supporting documentation from each of the six divisions, as well as the bureau's strategic plan, draft IT strategic plan, and information sharing strategy, and then compared this documentation with Office of Management and Budget (OMB) planning guidance[2] and our research and past experience on federal systems modernizations to determine the extent to which the plans exhibited an integrated approach to managing IT projects, including addressing project interdependencies. We also interviewed FBI officials from these organizations, as well as the Finance Division, Counterterrorism Division, Counterintelligence Division, Office of Intelligence, and the Office of the Chief Information Officer (CIO)

[1] There were no divisions from the Intelligence component included in our scope because it was recently formed in January 2003, and Intelligence officials stated that they were not yet managing any systems modernization initiatives and they had not established polices and procedures to do so.

[2] See OMB Circular Nos. A-11 and A-130.

to (1) verify and clarify our understanding of headquarters and division modernization planning roles, processes, and products; (2) determine why division plans did not fully satisfy the elements of effective modernization planning; and (3) identify the effects of not having a fully integrated modernization plan (or set of plans).

In addressing the second objective—determining whether the bureau has effective policies and procedures governing management of IT human capital, IT systems acquisition, and IT investment selection and control—we assessed whether bureau policies and procedures were fully consistent with the practices of successful private and public IT organizations and, where appropriate, those specified in relevant federal IT management laws and administrative guidance (e.g., OMB circulars and agency-specific rules and regulations) that embody such best practices. A detailed description of our methodology for each of these management controls and capabilities is provided below.

To evaluate the bureau's policies and procedures in IT human capital management, we analyzed the FBI's strategic human capital plan, specifically those parts addressing IT human capital management. We then compared the results of our analysis with best practices for strategic workforce planning.[3] We chose strategic workforce planning because it is central to strategic human capital management for organizations, like the FBI, that are in the early stages of transformation. In addition, these practices apply to any organization or organizational component, such as the bureau's IT organization. We also interviewed senior FBI officials, including the CIO and the assistant director responsible for the bureau's human capital effort, to verify and clarify our understanding of headquarters and division human capital policies and procedures.

To determine whether the FBI has effective policies and procedures governing management of IT systems acquisition, we compared division-level policies and procedures with best practices. In doing so, we focused on the following key areas: configuration management, project management, quality assurance, requirements development and management, and risk management. We evaluated these areas because they are used throughout the systems acquisition life cycle and are critical to the

[3] GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002) and *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

success of organizations, like the FBI, that are in the early stages of systems modernization. Best practices for these areas are provided in the Carnegie Mellon University Software Engineering Institute's Capability Maturity Models.[4] To document division policies and procedures, we reviewed division-level management plans and handbooks, standard operating procedures, common software processes, systems development life cycle guidance, management group charters, and management plan templates. We then compared the policies and procedures with best practices for the five key management areas. In addition, we interviewed the CIO and FBI division officials who were responsible for IT systems acquisition management to (1) verify and clarify our understanding of division-level policies and procedures in each of the five control areas; (2) identify planned and ongoing initiatives to, among other things, improve systems acquisition management across the bureau, including the definition and implementation of a bureauwide systems life cycle management process that is to include systems acquisition management policies and procedures consistent with best practices; (3) determine why divisions varied in their use of best practices; and (4) determine the effects of not having these practices in place on ongoing and planned systems modernization initiatives.

To evaluate the bureau's IT investment management, including selection and control, we reviewed the Inspector General's December 2002 report and audit follow-up memoranda[5] on the bureau's efforts to develop and implement effective investment management processes. We also reviewed bureau documents, including the draft IT strategic plan, on steps taken since the Inspector General's 2002 report. Further, we interviewed the CIO and officials from the CIO's office responsible for investment and portfolio management to understand improvements under way and planned, why progress has been slow, and the effect of not having effective policies and procedures in place and operating while the bureau continues to make large investments in modernized systems.

[4] See *Software Acquisition Capability Maturity Model* (CMU/SEI-99-TR-002, April 1999) and *Key Practices of the Capability Maturity Model* (CMU/SEI-93-TR-025, February 1993).

[5] U.S. Department of Justice Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report 03-09 (Washington, D.C., December 2002) and U.S. Department of Justice Office of the Inspector General, *Action Required on the Federal Bureau of Investigation's Management of Information Technology Investments*, *Audit Report Number 03-09*, (Washington, D.C., January 2004).

Finally, to verify our findings and validate our assessments, we met and discussed with the CIO and the affected division officials our analysis of the state of integration plans and IT management policies and procedures.

We performed our work at FBI headquarters in Washington, D.C., and at field locations in Clarksburg, West Virginia, and Quantico, Virginia, from November 2003 through July 2004, in accordance with generally accepted government auditing standards.

Brief Descriptions of Major IT Systems Modernization Initiatives

Initiative	Description of intended functions and services
Aurora	Provide system architectural, engineering, development, integration, and test services to complete the modernization of FBI information technology.
Collaborative Capabilities	Provide direct access to law enforcement and intelligence databases from a collection of personal computers connected through a common unclassified FBI local area network.
Combined DNA Index System	Enable federal, state, and local crime laboratories to exchange and compare DNA profiles electronically, including the capability to link serial violent crimes to each other and to convicted offenders.
Computer Analysis Response Team	Ensure the ability of the FBI to collect, preserve, examine, and present computer evidence in support of FBI investigative programs, including developing technical capabilities that provide timely and accurate forensic information and preserving evidence to be analyzed by counterintelligence and counterterrorism experts.
Digital Collection	Ensure the ability of the FBI to collect evidence and intelligence (for example, from telephone calls and modem transmissions) through the acquisition, deployment, and support of communications interception techniques and systems to facilitate and support national security, domestic counterterrorism, and criminal investigative efforts.
Electronic Surveillance Data Management System	Implement a system architecture that increases the FBI's ability to manage, analyze, and share electronic surveillance and other types of collected data, and integrates data analysis capabilities to improve the efficiency with which investigators can develop leads and intelligence.
Foreign Terrorism Tracking Task Force	Manage data for end-to-end decision making that contributes to the mission of keeping foreign terrorists and their supporters out of the United States or leads to their exclusion, denial of benefits, surveillance, or prosecution.
Integrated Automated Fingerprint Identification System	Provide the local, state, federal, and international law enforcement community and homeland security organizations with criminal history services and the capability to search the FBI fingerprint repository for matches to ten-print and latent fingerprints.
Investigative Data Warehousing and Virtual Knowledge Base	Provide the capability to easily and rapidly search and share counterterrorism and criminal investigative information—including text, photographs, video, and audio material—across the FBI and with federal, state, and local organizations.
IT Security/Information Assurance	Provide a foundation for safeguarding the FBI's information, including developing a comprehensive and proactive security program, improving security awareness, monitoring FBI systems, conducting vulnerability assessments, and establishing a critical incident response capability.
Joint Terrorism Task Force, Information Sharing Initiative	Provide the IT infrastructure required to support the task force's efforts to capture the cumulative knowledge of area law enforcement agencies and the federal government in a systematic and ongoing manner so as to produce regional counterterrorism and crime strategies and cooperative investigations.
Legat/International Infrastructure	Provide IT support and services to the FBI's foreign locations, including reducing vulnerabilities to accessing and sharing critical, time-sensitive information internationally.
National Crime Information Center 2000	Provide an online computerized index of crime information—including information about individuals, vehicles, and property—to local, state, federal, and international law enforcement and criminal justice agencies.
National Instant Criminal Background Check System	Conduct name searches and provide criminal history records on individuals purchasing firearms or transferring ownership of firearms.

(Continued From Previous Page)

Initiative	Description of intended functions and services
Security Management Information System	Support all activities and functions within the bureau's Security division, including replacing manual work processes with efficient streamlined automation, consolidating existing security applications, and enhancing electronic information sharing with other FBI divisions, the law enforcement community, and the intelligence community.
Sensitive Compartmented Information Operational Network	Provide a backup system for the top secret/sensitive compartmented information local area network and expand the user base of this network within FBI headquarters, field offices, and other facilities.
Special Technologies Applications Section	Provide IT resources and services for investigations of federal violations in which the Internet, computer systems, or networks are exploited as instruments or targets of terrorist organizations, foreign government-sponsored intelligence operations, or criminal activity.
Trilogy	Introduce new systems infrastructure and upgrade existing investigative and intelligence applications, including establishing an enterprise network to enable communications among hundreds of domestic and foreign FBI locations.

Source: GAO analysis of FBI data.

Summary of Systems Acquisition Analyses for Six FBI Divisions

Analyses for CJIS, Counterterrorism, and Cyber

Acquisition management control and best practice elements	Addressed by division policy? CJIS	Counterterrorism	Cyber
Configuration management			
Identifying roles and responsibilities	Yes	Yes	Yes
Developing a configuration management plan	Yes	Yes	Yes
Establishing a library system	Yes	Yes	Yes
Identifying, documenting, managing, and controlling configuration items and baselines	Yes	Yes	Yes
Managing change requests and problem reports	Yes	Yes	Yes
Periodically auditing baselines	Yes	Yes	Yes
Periodically having management review the status of configuration management activities	Yes	Yes	No
Project management			
Identifying roles and responsibilities	Yes	Yes	Yes
Developing a project management plan	Yes	Yes	Yes
Baselining and tracking project cost, schedule, and performance status and associated risks	Yes	Yes	No
Establishing a corrective action system to identify, record, track, and correct problems	Yes	Yes	No
Periodically reviewing and communicating the status of project management activities and commitments	Yes	Yes	Yes
Quality assurance			
Identifying roles and responsibilities	Yes	Yes	Yes
Developing a quality assurance plan	Yes	No	Yes
Participating in the development and review of integration plans, standards, and procedures	Yes	No	No
Reviewing activities and work products to verify compliance with applicable standards and procedures	Yes	Yes	Yes
Documenting and handling deviations in activities and work products	Yes	Yes	Yes
Periodically reporting and reviewing the results and findings of quality assurance activities	Yes	Yes	No

(Continued From Previous Page)

	Addressed by division policy?		
Acquisition management control and best practice elements	**CJIS**	**Counterterrorism**	**Cyber**
Requirements development and management			
Identifying roles and responsibilities	Yes	No	Yes
Involving end users in development of and changes to requirements	Yes	No	Yes
Developing a requirements management plan	Yes	No	No
Developing and baselining requirements, and maintaining them under change control	Yes	No	No
Appraising changes to requirements for their impact on the project or IT environment	No	No	No
Maintaining traceability among requirements and project deliverables	Yes	No	Yes
Periodically reviewing the status of requirements development and management activities with management	Yes	No	No
Risk management			
Identifying roles and responsibilities	No	Yes	No
Developing a risk management plan	Yes	Yes	Yes
Integrating risk management with other planning and management functions	No	No	No
Identifying, analyzing, controlling, and mitigating project risks	Yes	Yes	Yes
Periodically having management review the status of project risks and risk management activities	Yes	No	No

Source: GAO analysis of FBI data.

Analyses for Information Resources, Investigative Technology, and Program Management Office

Acquisition management control and best practice elements	Addressed by division policy?		
	Information Resources	Investigative Technology	Program Management Office
Configuration management			
Identifying roles and responsibilities	Yes	No	Yes
Developing a configuration management plan	Yes	Yes	Yes
Establishing a library system	Yes	No	Yes
Identifying, documenting, managing, and controlling configuration items and baselines	Yes	No	Yes
Managing change requests and problem reports	Yes	No	Yes
Periodically auditing baselines	Yes	No	No
Periodically having management review the status of configuration management activities	Yes	No	No
Project management			
Identifying roles and responsibilities	Yes	Yes	Yes
Developing a project management plan	Yes	Yes	Yes
Baselining and tracking project cost, schedule, and performance status and associated risks	Yes	Yes	Yes
Establishing a corrective action system to identify, record, track, and correct problems	Yes	Yes	Yes
Periodically reviewing and communicating the status of project management activities and commitments	Yes	Yes	Yes
Quality assurance			
Identifying roles and responsibilities	Yes	Yes	Yes
Developing a quality assurance plan	No	Yes	Yes
Participating in the development and review of integration plans, standards, and procedures	No	Yes	No
Reviewing activities and work products to verify compliance with applicable standards and procedures	Yes	Yes	Yes
Documenting and handling deviations in activities and work products	Yes	Yes	Yes
Periodically reporting and reviewing the results and findings of quality assurance activities	Yes	No	No

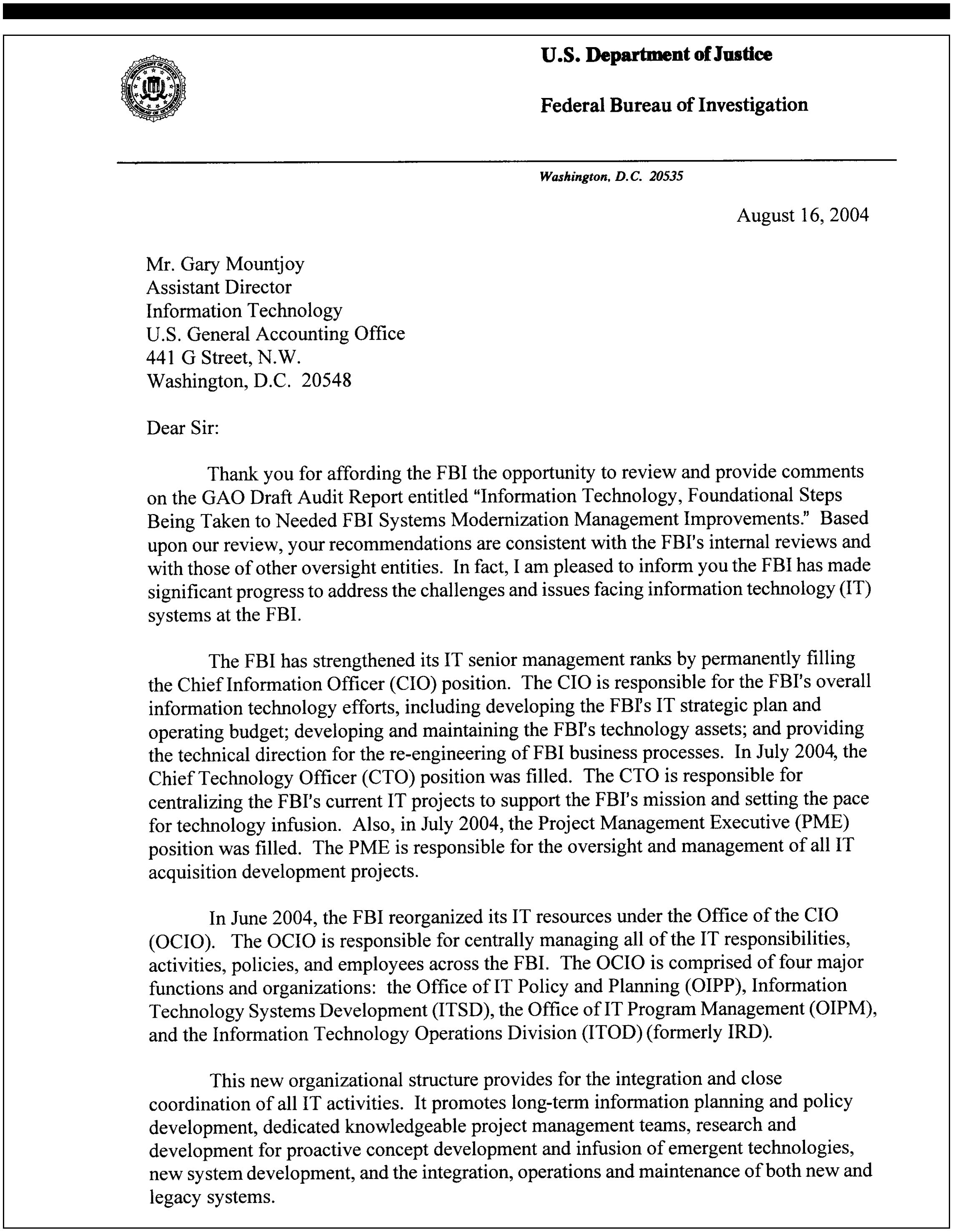
(Continued From Previous Page)

	Addressed by division policy?		
Acquisition management control and best practice elements	**Information Resources**	**Investigative Technology**	**Program Management Office**
Requirements development and management			
Identifying roles and responsibilities	No	No	Yes
Involving end users in development of and changes to requirements	No	No	Yes
Developing a requirements management plan	No	No	No
Developing and baselining requirements, and maintaining them under change control	No	No	Yes
Appraising changes to requirements for their impact on the project or IT environment	No	No	No
Maintaining traceability among requirements and project deliverables	No	Yes	No
Periodically reviewing the status of requirements development and management activities with management	No	No	Yes
Risk management			
Identifying roles and responsibilities	Yes	No	Yes
Developing a risk management plan	Yes	Yes	Yes
Integrating risk management with other planning and management functions	No	No	No
Identifying, analyzing, controlling, and mitigating project risks	Yes	Yes	Yes
Periodically having management review the status of project risks and risk management activities	No	Yes	Yes

Source: GAO analysis of FBI data.

Appendix IV

Comments from the Federal Bureau of Investigation



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

August 16, 2004

Mr. Gary Mountjoy
Assistant Director
Information Technology
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

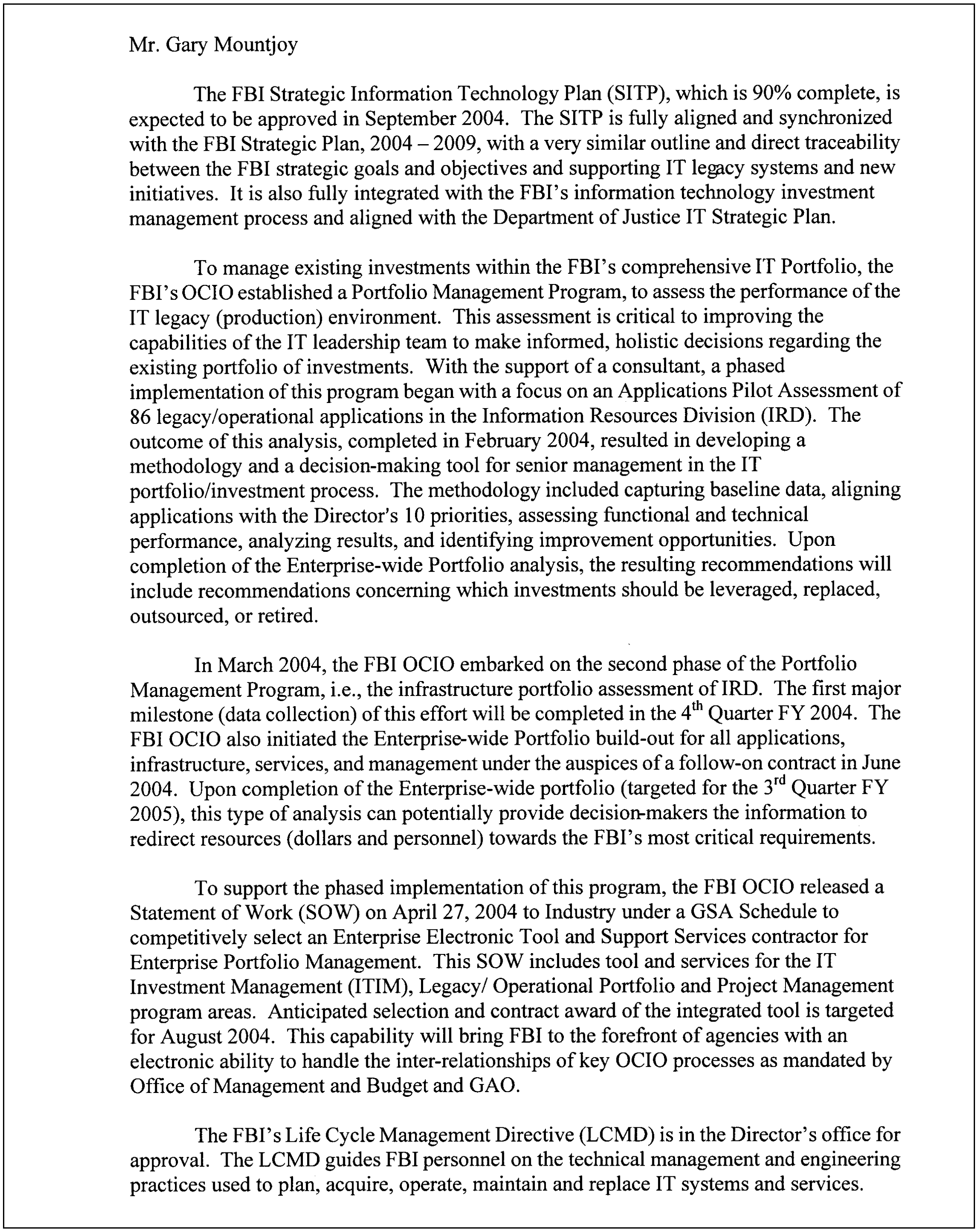
Dear Sir:

Thank you for affording the FBI the opportunity to review and provide comments on the GAO Draft Audit Report entitled "Information Technology, Foundational Steps Being Taken to Needed FBI Systems Modernization Management Improvements." Based upon our review, your recommendations are consistent with the FBI's internal reviews and with those of other oversight entities. In fact, I am pleased to inform you the FBI has made significant progress to address the challenges and issues facing information technology (IT) systems at the FBI.

The FBI has strengthened its IT senior management ranks by permanently filling the Chief Information Officer (CIO) position. The CIO is responsible for the FBI's overall information technology efforts, including developing the FBI's IT strategic plan and operating budget; developing and maintaining the FBI's technology assets; and providing the technical direction for the re-engineering of FBI business processes. In July 2004, the Chief Technology Officer (CTO) position was filled. The CTO is responsible for centralizing the FBI's current IT projects to support the FBI's mission and setting the pace for technology infusion. Also, in July 2004, the Project Management Executive (PME) position was filled. The PME is responsible for the oversight and management of all IT acquisition development projects.

In June 2004, the FBI reorganized its IT resources under the Office of the CIO (OCIO). The OCIO is responsible for centrally managing all of the IT responsibilities, activities, policies, and employees across the FBI. The OCIO is comprised of four major functions and organizations: the Office of IT Policy and Planning (OIPP), Information Technology Systems Development (ITSD), the Office of IT Program Management (OIPM), and the Information Technology Operations Division (ITOD) (formerly IRD).

This new organizational structure provides for the integration and close coordination of all IT activities. It promotes long-term information planning and policy development, dedicated knowledgeable project management teams, research and development for proactive concept development and infusion of emergent technologies, new system development, and the integration, operations and maintenance of both new and legacy systems.



Mr. Gary Mountjoy

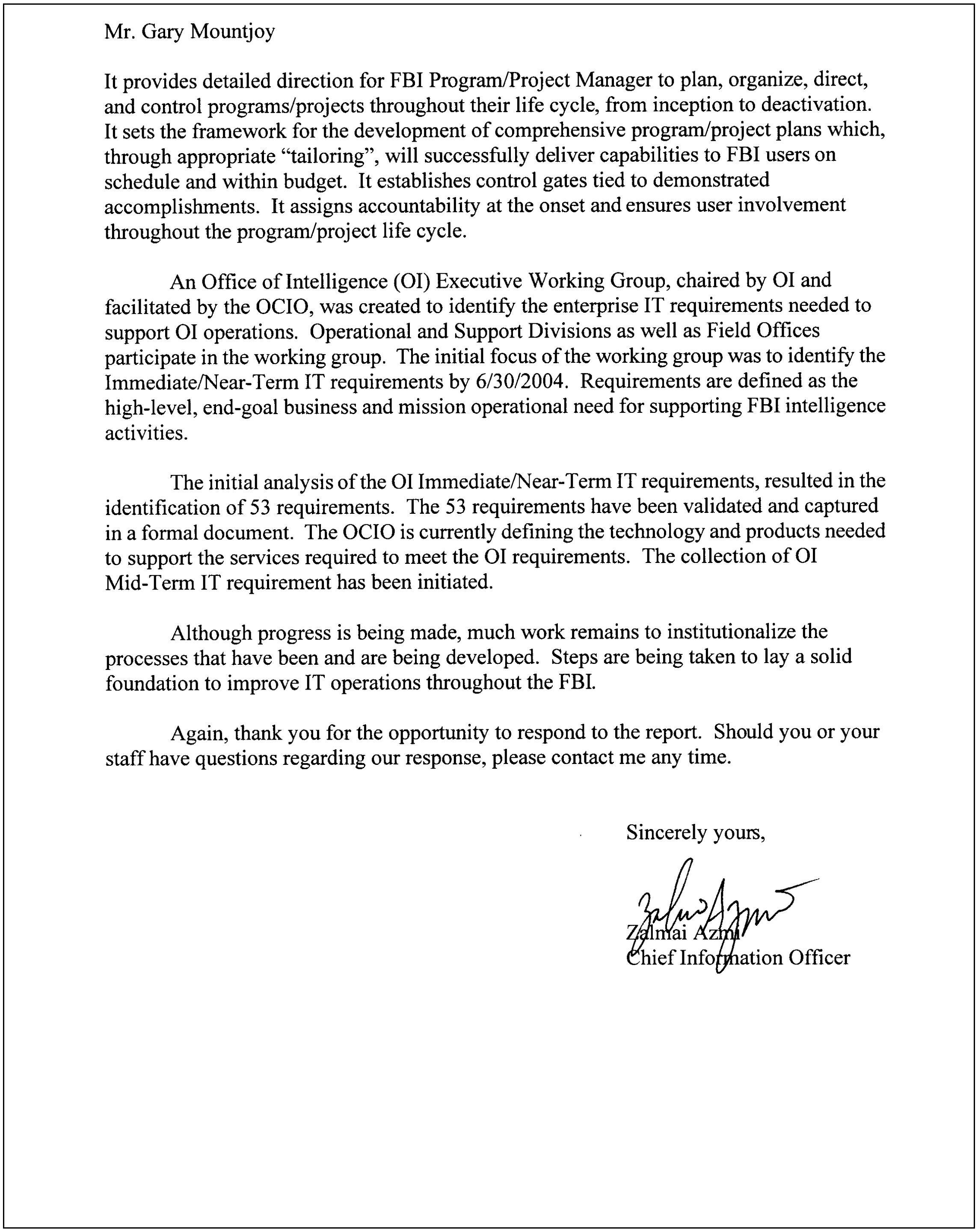
The FBI Strategic Information Technology Plan (SITP), which is 90% complete, is expected to be approved in September 2004. The SITP is fully aligned and synchronized with the FBI Strategic Plan, 2004 – 2009, with a very similar outline and direct traceability between the FBI strategic goals and objectives and supporting IT legacy systems and new initiatives. It is also fully integrated with the FBI's information technology investment management process and aligned with the Department of Justice IT Strategic Plan.

To manage existing investments within the FBI's comprehensive IT Portfolio, the FBI's OCIO established a Portfolio Management Program, to assess the performance of the IT legacy (production) environment. This assessment is critical to improving the capabilities of the IT leadership team to make informed, holistic decisions regarding the existing portfolio of investments. With the support of a consultant, a phased implementation of this program began with a focus on an Applications Pilot Assessment of 86 legacy/operational applications in the Information Resources Division (IRD). The outcome of this analysis, completed in February 2004, resulted in developing a methodology and a decision-making tool for senior management in the IT portfolio/investment process. The methodology included capturing baseline data, aligning applications with the Director's 10 priorities, assessing functional and technical performance, analyzing results, and identifying improvement opportunities. Upon completion of the Enterprise-wide Portfolio analysis, the resulting recommendations will include recommendations concerning which investments should be leveraged, replaced, outsourced, or retired.

In March 2004, the FBI OCIO embarked on the second phase of the Portfolio Management Program, i.e., the infrastructure portfolio assessment of IRD. The first major milestone (data collection) of this effort will be completed in the 4th Quarter FY 2004. The FBI OCIO also initiated the Enterprise-wide Portfolio build-out for all applications, infrastructure, services, and management under the auspices of a follow-on contract in June 2004. Upon completion of the Enterprise-wide portfolio (targeted for the 3rd Quarter FY 2005), this type of analysis can potentially provide decision-makers the information to redirect resources (dollars and personnel) towards the FBI's most critical requirements.

To support the phased implementation of this program, the FBI OCIO released a Statement of Work (SOW) on April 27, 2004 to Industry under a GSA Schedule to competitively select an Enterprise Electronic Tool and Support Services contractor for Enterprise Portfolio Management. This SOW includes tool and services for the IT Investment Management (ITIM), Legacy/ Operational Portfolio and Project Management program areas. Anticipated selection and contract award of the integrated tool is targeted for August 2004. This capability will bring FBI to the forefront of agencies with an electronic ability to handle the inter-relationships of key OCIO processes as mandated by Office of Management and Budget and GAO.

The FBI's Life Cycle Management Directive (LCMD) is in the Director's office for approval. The LCMD guides FBI personnel on the technical management and engineering practices used to plan, acquire, operate, maintain and replace IT systems and services.



Mr. Gary Mountjoy

It provides detailed direction for FBI Program/Project Manager to plan, organize, direct, and control programs/projects throughout their life cycle, from inception to deactivation. It sets the framework for the development of comprehensive program/project plans which, through appropriate "tailoring", will successfully deliver capabilities to FBI users on schedule and within budget. It establishes control gates tied to demonstrated accomplishments. It assigns accountability at the onset and ensures user involvement throughout the program/project life cycle.

An Office of Intelligence (OI) Executive Working Group, chaired by OI and facilitated by the OCIO, was created to identify the enterprise IT requirements needed to support OI operations. Operational and Support Divisions as well as Field Offices participate in the working group. The initial focus of the working group was to identify the Immediate/Near-Term IT requirements by 6/30/2004. Requirements are defined as the high-level, end-goal business and mission operational need for supporting FBI intelligence activities.

The initial analysis of the OI Immediate/Near-Term IT requirements, resulted in the identification of 53 requirements. The 53 requirements have been validated and captured in a formal document. The OCIO is currently defining the technology and products needed to support the services required to meet the OI requirements. The collection of OI Mid-Term IT requirement has been initiated.

Although progress is being made, much work remains to institutionalize the processes that have been and are being developed. Steps are being taken to lay a solid foundation to improve IT operations throughout the FBI.

Again, thank you for the opportunity to respond to the report. Should you or your staff have questions regarding our response, please contact me any time.

Sincerely yours,

Zalmai Azmi
Chief Information Officer

GAO Contact and Staff Acknowledgments

GAO Contact

Gary Mountjoy, (202) 512-6367

Staff Acknowledgments

In addition to the individual named above, key contributors to this report included Nabajyoti Barkakarti, Katherine Chu-Hickman, Lester Diamond, Elena Epps, Nancy Glover, Paula Moore, and Megan Secrest.

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

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

PRINTED ON ♻ RECYCLED PAPER

[redacted]