United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2008

INFORMATION TECHNOLOGY

FBI Is Implementing Key Acquisition Methods on Its New Case Management System, but Related Agencywide Guidance Needs to Be Improved

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-1014, a report to congressional requesters

September 2008

INFORMATION TECHNOLOGY

FBI Is Implementing Key Acquisition Methods on Its New Case Management System, but Related Agencywide Guidance Needs to Be Improved

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) is 3 years into its 6-year, $451 million program known as Sentinel, which is to replace its antiquated, paper-based, legacy systems for supporting mission-critical intelligence analysis and investigative case management activities. Because of the importance of Sentinel to the bureau's mission operations, GAO was asked to conduct a series of reviews on the FBI's management of the program. This review focuses on whether the FBI is employing effective methods in acquiring commercial solutions for Sentinel. To do so, GAO researched relevant best practices; reviewed FBI policies and procedures, program plans, and other program documents; and interviewed appropriate program officials.

What GAO Recommends

To increase the chances of successfully delivering commercial component-based systems like Sentinel, GAO is recommending that the FBI revise its corporate policies and guidance to fully incorporate the following acquisition methods:

- requirements/commercial product trade-off analysis,
- commercial product dependency analysis,
- commercial product modification, and
- legacy system integration management.

The FBI concurred with GAO's findings and recommendations and stated that actions are underway and planned to address them.

To view the full product, including the scope and methodology, click on GAO-08-1014. For more information, contact Randolph Hite (202) 512-3439 or hiter@gao.gov.

What GAO Found

The FBI's Sentinel program is implementing five key methods for acquiring commercial information technology solutions. In particular, it is managing Sentinel requirements by making sure that changes to established baselines are justified and approved on the basis of costs, benefits, and risks, and it is ensuring that different levels of requirements and related design specification and test cases are properly aligned with one another. In addition, the bureau is analyzing commercially available product alternatives in relation to requirements, costs, and other factors to ensure that the most cost-effective mix of products is being used to minimize requirement gaps. In doing so, it is taking steps to understand the dependencies among the commercial products, thus ensuring that they can interoperate effectively. Also, the bureau is not modifying the commercial products that it is selecting and using to develop Sentinel, which should allow it to minimize future maintenance costs by taking advantage of future product releases and other vendor product support. Last, it is taking steps to ensure that Sentinel integration with FBI legacy systems will occur when needed, for example, by establishing agreements with legacy system owners. Collectively, implementation of these acquisition methods should increase the chances of cost effectively delivering required Sentinel capabilities on time.

However, the implementation of most of these acquisition methods is generally not governed by bureauwide policies and guidance that address all relevant practices (see table). To the credit of program officials, this void in corporate policies and guidance has not affected Sentinel, as they are implementing all of the key practices either through reliance on their prime contractor's approaches or through Sentinel-specific plans. If policies and guidance relative to each of these methods for acquiring commercial component-based systems were incorporated into FBI-wide policies and guidance, the bureau could increase its chances of employing them on a repeatable basis across all applicable system investments.

Table: Extent to which FBI Has Defined and Sentinel Program Has Implemented Five Key Methods for Acquiring Commercial System Solutions

Key methods	Defined in FBI policy/guidance	Implemented for Sentinel
Requirements management	Yes	Yes
Requirements/commercial product trade-off analysis	Partial	Yes
Commercial product dependency analysis	No	Yes
Commercial product modification	Partial	Yes
Legacy system integration management	Partial	Yes

Source: GAO analysis of FBI data.

Contents

Letter 1

Results in Brief 2
Background 3
Sentinel Is Implementing Key Commercial Component-Based System Acquisition Methods, but Corporate Guidance Governing These Methods Is Not Fully Defined 13
Conclusions 23
Recommendations for Executive Action 23
Agency Comments 24

Appendix I **Objective, Scope, and Methodology** **25**

Appendix II **Comments from the Federal Bureau of Investigation** **28**

Appendix III **GAO Contact and Staff Acknowledgments** **31**

Figures

Figure 1: Simplified Representation of Sentinel Incremental Acquisition Approach 8
Figure 2: Conceptual View of FBI IT Life Cycle 10
Figure 3: Sentinel Requirements Change Control Process 15

Abbreviations

FBI	Federal Bureau of Investigation
IT	information technology
SEI	Software Engineering Institute
VCF	Virtual Case File

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 23, 2008

The Honorable Barbara Mikulski
Chair
The Honorable Richard Shelby
Ranking Member
Subcommittee on Commerce, Justice, Science,
and Related Agencies
Committee on Appropriations
United States Senate

The Honorable John Conyers, Jr.
Chairman
The Honorable Lamar Smith
Ranking Member
Committee on the Judiciary
House of Representatives

The Honorable F. James Sensenbrenner, Jr.
House of Representatives

The Federal Bureau of Investigation (FBI) is 3 years into its 6-year, $451 million system acquisition program to replace its antiquated, paper-based legacy systems for supporting mission-critical intelligence analysis and investigative case management activities. This program, known as Sentinel, is being executed through the integration of commercially available hardware and software components in a series of phases, with each phase consisting of segments that are to provide incremental capabilities. Because of the importance of Sentinel to the bureau's mission operations, you asked us to review the FBI's management of the program.

In response to your request, we have performed three incremental reviews of Sentinel that have addressed a range of system acquisition management practices. We issued reports on the results of the first two reviews in

October 2006[1] and July 2007.[2] This report provides the results of the third review. As agreed, the objective of our third review was to determine whether the FBI is employing effective methods in acquiring commercial solutions for Sentinel. To accomplish this, we focused on the following five key information technology (IT) management areas: (1) requirements management, (2) requirements/commercial product trade-off analysis, (3) commercial product dependency analysis, (4) commercial product modification, and (5) legacy system integration. For each of the areas, we researched relevant best practices; reviewed FBI policies, procedures, and guidance; analyzed program documentation; and interviewed program management and oversight officials to determine whether they have been addressed in bureauwide policies and guidance and implemented on Sentinel. In reviewing their implementation, we focused primarily on that segment of Sentinel capabilities that was being developed at the time we began our review.

We conducted this performance audit from October 2007 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details of our objective, scope, and methodology are included in appendix I.

Results in Brief

For its Sentinel program, the FBI is implementing five important methods for effectively acquiring commercial IT solutions. In particular, it is managing Sentinel requirements by making sure that changes to established baselines are justified and approved on the basis of costs, benefits, and risks, and it is ensuring that different levels of requirements, and related design specification and test cases, are properly aligned with one another. In addition, the bureau is analyzing commercially available product alternatives in relation to requirements, costs, and other factors to

[1] GAO, *Information Technology: FBI Has Largely Staffed Key Modernization Program, but Strategic Approach to Managing Program's Human Capital Is Needed*, GAO-07-19 (Washington, D.C.: Oct. 16, 2006).

[2] GAO, *Information Technology: FBI Following a Number of Key Acquisition Practices on New Case Management System, but Improvements Still Needed*, GAO-07-912 (Washington, D.C.: July 30, 2007).

ensure that the most cost-effective mix of products is used to minimize requirement gaps. In doing so, it is also taking steps to understand the dependencies among the commercial products to better ensure that they can interoperate effectively. Also, the bureau is not modifying the commercial products that it is selecting and using to develop Sentinel, which should allow it to minimize future maintenance costs by taking advantage of future product releases and other vendor product support. Finally, it is taking steps to ensure that Sentinel integration with FBI legacy systems will occur when needed by, for example, establishing agreements with legacy system owners. Collectively, implementation of these acquisition methods should increase the chances of cost effectively delivering required Sentinel capabilities on time.

However, with the exception of requirements management, implementation of all key practices associated with these methods is generally not governed by bureauwide policies or guidance. In the absence of such policies and guidance, Sentinel program officials have recognized the need to implement the acquisition methods and, in doing so, have either relied on their prime contractor's approaches and methodologies or have created Sentinel-specific plans to guide implementation efforts. To the extent that Sentinel's efforts are institutionalized and thus made repeatable across the FBI's other IT programs through improvements to corporate policies and guidance, the FBI can increase its ability to consistently deliver successful IT programs. Accordingly, we are recommending that the FBI revise its policies and guidance to fully address a number of key practices associated with (1) requirements/commercial product trade-off analysis, (2) commercial product dependency analysis, (3) commercial product modification, and (4) legacy system integration management.

In written comments on a draft of this report, signed by the FBI Chief Information Officer and reprinted in appendix II, the bureau agreed with our findings and recommendations, and described steps underway and planned to address them.

Background

The FBI serves as the primary investigative unit of the Department of Justice. Its mission includes investigating serious federal crimes, protecting the nation from foreign intelligence and terrorist threats, and assisting other law enforcement agencies. Approximately 12,000 special agents and 16,000 analysts and mission support personnel are located in the bureau's Washington, D.C., headquarters and about 70 offices in the United States and 50 offices in foreign countries. Mission responsibilities at the bureau are divided among a number of major organizational components, including:

National Security: integrates investigative and intelligence activities against current and emerging national security threats and provides information and analysis for the national security and law enforcement communities.

Criminal Investigations: investigates serious federal crimes and probes federal statutory violations involving exploitation of the Internet and computer systems.

Law Enforcement: provides law enforcement information and forensic services to federal, state, local, and international agencies.

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

Office of the Chief Information Officer: develops and implements the bureau's IT strategic plan and operating budget, which includes acquiring, operating, and maintaining IT assets.

IT Is Instrumental to FBI Mission Operations

To execute its mission, the FBI relies extensively on the use of IT. In particular, the bureau operates and maintains hundreds of computerized systems, databases, and applications, such as the

- Combined DNA Index System, which supports forensic examinations;
- National Crime Information Center and the Integrated Automated Fingerprint Identification System, which help state and local law enforcement agencies identify criminals;
- Automated Case Management System, which manages information collected on investigative cases;
- Investigative Data Warehouse, which aggregates data from disparate databases in a standard format to facilitate content management and data mining; and

- Terrorist Screening Database, which consolidates identification information about known or suspected international and domestic terrorists.

Prior FBI Attempt to Develop an Investigative Case Management System Was Not Successful

Following the terrorist attacks in the United States on September 11, 2001, the FBI shifted its mission focus to detecting and preventing future attacks, which led to the FBI's commitment to reorganize and transform. According to the bureau, the complexity of this mission shift, along with the changing law enforcement environment, strained its existing IT environment. As a result, the bureau accelerated the IT modernization program that it had begun in September 2000. This program, later named Trilogy, was the FBI's largest IT initiative to date and consisted of three parts: (1) the Information Presentation Component to upgrade FBI's computer hardware and system software, (2) the Transportation Network Component to upgrade the agency's communication network, and (3) the User Application Component to upgrade and consolidate the bureau's five key investigative software applications. The heart of this last component became the Virtual Case File (VCF) project, which was intended to replace the obsolete Automated Case Support system.

While the first two components of Trilogy are currently operating, the third component—VCF—never became operational because it was determined to be an infeasible and cost prohibitive solution. We have previously reported[3] on reasons for VCF's failure, which included limitations in system requirements, ineffective control over changes to the system, limited oversight of contractors, and lack of continuity in certain management positions and trained staff for key program positions.

Sentinel: A Brief Description

The Sentinel program began in 2005, and is intended to be both the successor to and an expansion of VCF. As we previously reported,[4] Sentinel is to meet a pressing need for a modern, automated capability for investigative case management and information sharing to help field agents and intelligence analysts perform their jobs more effectively and efficiently. More specifically, it is to (1) provide a single point of entry for

[3] GAO, *Information Technology: FBI Is Building Management Capabilities Essential to Successful System Deployment, but Challenges Remain*, GAO-05-1014T (Washington, D.C.: Sept. 14, 2005).

[4] GAO-07-912.

all investigative case management and paperless case management and workflow capabilities, (2) facilitate a bureauwide organizational change management program, and (3) provide intuitive interfaces that feature data relevant to individual users. Examples of specific Sentinel capabilities include leads management and evidence management; document and records management; indexed searching and electronic workflow; legacy system and external data source connectivity; training, statistical, and reporting tools; and security management.

After conducting a multistep evaluation of the different governmentwide acquisition contracts available to federal agencies,[5] the FBI issued a request for vendor proposals to more than 40 eligible companies under a National Institutes of Health contract in August 2005. In March 2006, the FBI awarded a task order to develop and integrate Sentinel to Lockheed Martin Corporation.

The FBI plans to deliver defined Sentinel capabilities in four phases using commercially available software and hardware components. The specific content of each phase is to be proposed by and negotiated with the prime contractor. The general capabilities for each phase are as follows:

- Phase 1: A Web-based user interface for accessing data from the Automated Case Management System and other legacy systems and a service-oriented architecture[6] to support delivery and sharing of common services across the bureau.

[5] Governmentwide acquisition contracts are authorized by the Clinger-Cohen Act to improve the acquisition of IT by federal agencies. These contracts are operated at the Department of Commerce, Department of Transportation, National Aeronautics and Space Administration, General Services Administration's Federal Technology Service, and National Institutes of Health. They are typically multiple-award contracts for IT that allow an indefinite quantity of goods or services (within specified limits) to be furnished during a fixed period, with deliveries scheduled through orders with the contractor. The providing agency awards the contract and other agencies issue task orders under it.

[6] A service-oriented architecture is an approach for sharing functions and applications across an organization by designing them as discrete, reusable, business-oriented services. These services need to be, among other things, (1) self-contained, meaning that they do not depend on any other functions or applications to execute a discrete unit of work; (2) published and exposed as self-describing business capabilities that can be accessed and used; and (3) subscribed to via well-defined and standardized interfaces instead of unique, tightly coupled connections. Such a service orientation is thus not only intended to promote the reduced redundancy and increased integration that any architectural approach is designed to achieve, but also to provide the flexibility needed to support a quicker response to changing and evolving business requirements and emerging conditions.

- Phase 2: An enterprise portal for accessing Sentinel case management capabilities, Web-application reengineering to provide faster response time, electronic authoring and approval of forms, and calendaring.

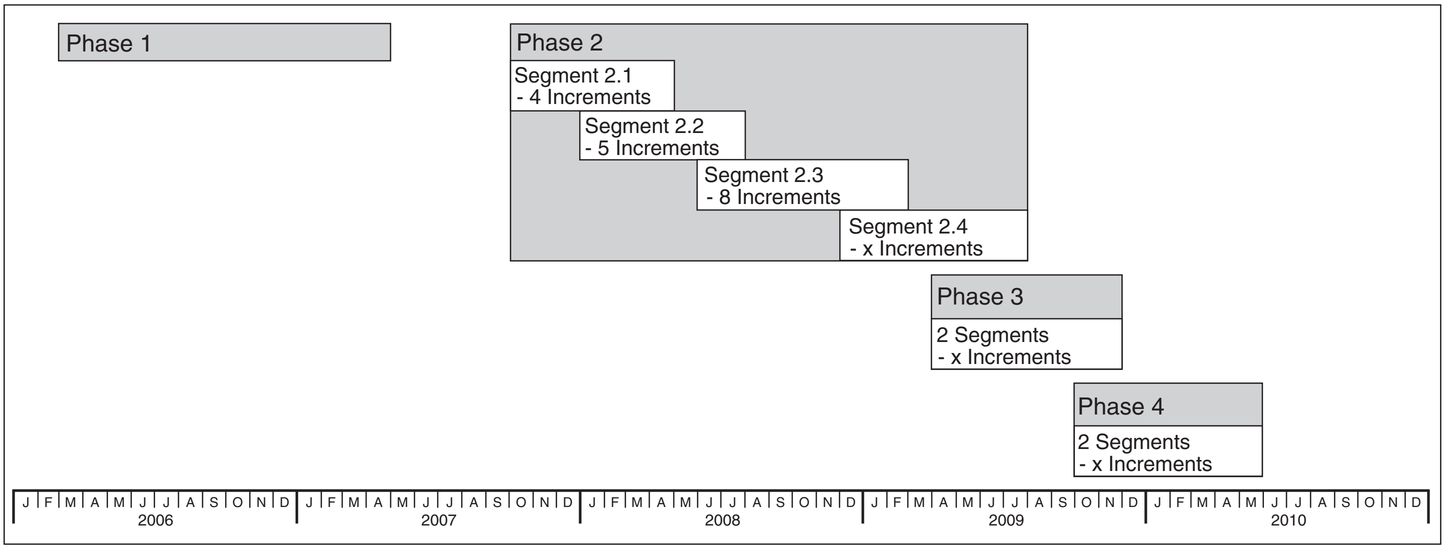
- Phase 3: Online searches, integration with FBI scanners, and template management.

- Phase 4: Enhanced case, evidence and crisis management, full search capability/information profile match, document authoring and workflow capabilities, fully certified FBI records management, and all case and ad hoc view capabilities.

Phase 1 capabilities were deployed in June 2007 and are currently operating. Following Phase 1, the FBI, in consultation with its prime contractor, adopted a more incremental design and development approach with more frequent deliveries of capabilities. In general, each phase is to consist of segments, which are to be logically grouped and sequenced bundles of system capabilities that are to be delivered in 3-6 month time frames. Each segment is to be further decomposed into a series of sequenced increments. Figure 1 provides a simplified representation of the relationship and timing of phases, segments, and increments.

Sentinel is currently in its second phase, which is to run from October 2007 to July 2009 (22 months) and is to consist of four segments. According to the Sentinel Program Office, Segment 1 was completed in April 2008; Segment 2 began in January 2008 and is largely complete, with deployment scheduled for July 2008. The FBI is currently developing Segment 3, with deployment planned for February 2009. The FBI estimates that the four phases will cost about $451 million through fiscal year 2012. The FBI has budgeted $183 million in funding for Phase 2 (excluding operations and maintenance) and, as of July 2008, had reportedly obligated $135 million.

Figure 1: Simplified Representation of Sentinel Incremental Acquisition Approach



Source: FBI data.

To manage Sentinel, the FBI established a program office within the Office of the Chief Information Officer. The program office is led by a program manager, a deputy program manager for systems development, and a deputy program manager for organizational change management.

Overview of FBI IT Acquisition Policies and Guidance

The FBI's policies and guidance governing the acquisition of IT programs such as Sentinel are contained in various documents, including its IT life-cycle management directive, which is dated August 2005 and was approved by the Chief Information Officer in January 2006.[7] The directive provides the bureau's framework for standardized, repeatable, and sustainable management of all of its IT programs and projects. According to the directive, the framework is to be tailored to the needs and priorities associated with each program/project.

The framework consists of, among other things, interrelated life-cycle phases, control gates, and reviews. The nine life-cycle phases are concept exploration, requirements development, acquisition planning, source selection, design, development and test, implementation and integration,

[7] FBI Information Technology Life Cycle Management Directive, Version 3.0 (Aug. 19, 2005).

operations and maintenance, and disposal. The life-cycle phases are associated with one or more control gates and/or program/project reviews. They are also linked to key stakeholder processes, including information security management, and recognized system development and acquisition best practice areas. The framework's elements are discussed in more detail below and depicted in figure 2.

- The seven control gates are mechanisms for executive-level control and direction, decision making, coordination, and confirmation of successful performance of activities to date. At these gates, a determination is made regarding the program/project's readiness to proceed to the next phase. Examples of control gates are system concept review, contract review board, enterprise architecture board, and technical review board.

- The 14 program/project reviews determine program/project satisfaction of the directive's requirements, completion of milestones, and system design satisfaction of FBI operational needs. The review results are used to inform control gate determinations and decisions. Examples of reviews are mission needs review, system specification review, preliminary design review, and product test readiness review.

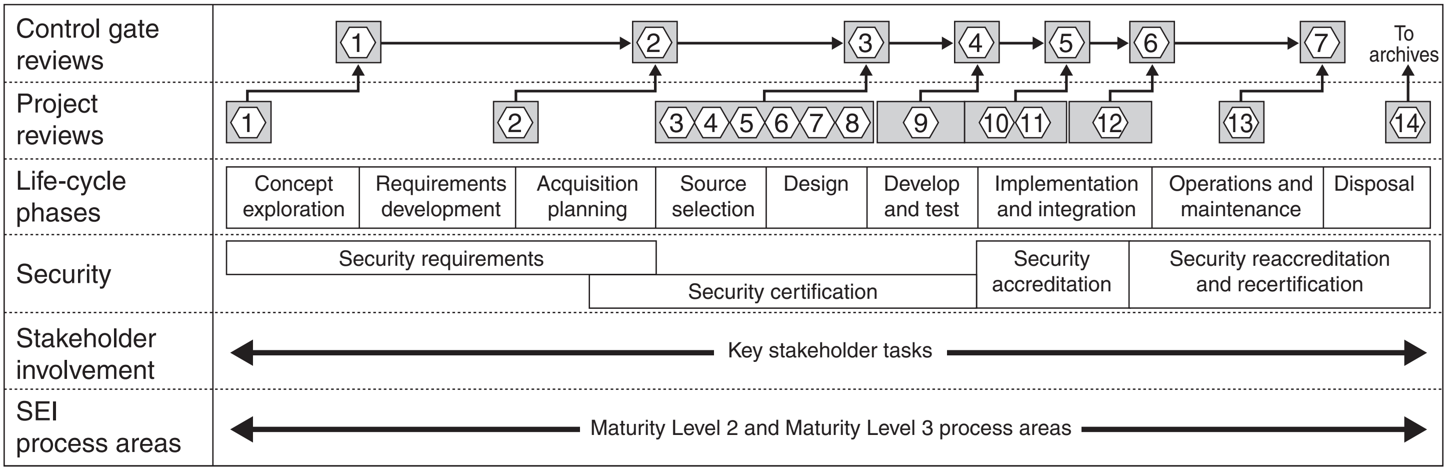
- The directive has seven key stakeholder processes that are not linked to any particular phase, gate, or review. These processes reflect such management functions as enterprise architecture alignment, investment management, budget execution, acquisition management, and information security management.

- The directive incorporates basic project management process areas and selected standardization process areas reflected in system development and acquisition best practices published by the Software Engineering Institute.[8] Among the process areas addressed are configuration management, process and product quality assurance, requirements development, and risk management.

According to Sentinel officials, they have tailored Version 3.0 of the directive for Sentinel, which is permitted by the guidance. However, a program official told us that a new version of the directive has been drafted.

[8] Software Engineering Institute (SEI) guidance includes maturity levels that provide a set of process areas that characterize different organizational behaviors.

Figure 2: Conceptual View of FBI IT Life Cycle



Source: FBI data.

In addition, the FBI's project manager's handbook,[9] dated September 2007, provides supporting guidance for implementing the IT life-cycle management directive. The handbook identifies and defines seven primary project management practices for effectively managing IT projects within the context of the management directive. These management practices include managing requirements, performance, and systems engineering, as well as the use of program controls.

Use of System Acquisition Management Best Practices Maximizes Chances for Program Success

Acquisition best practices are tried and proven methods that organizations capture in policies and guidance, define, and institutionally implement to minimize program risks and maximize the chances of program success. Using best practices can result in better outcomes—including cost savings, improved service and product quality, and ultimately, a better return on investment. For example, two software engineering analyses of nearly 200 systems acquisition projects indicated that teams using system acquisition best practices produced cost savings of at least 11 percent over similar projects conducted by teams that did not employ the kind of rigor and

[9] Office of IT Program Management, *Project Management for the FBI*, version 2 (September 2007).

discipline embedded in these practices.[10] In addition, our research shows that best practices are a significant factor in successful acquisition outcomes, including increasing the likelihood that programs and projects will be executed within cost and schedule estimates.[11] Examples of acquisition best practices or methods that are relevant to commercial component-based systems, like Sentinel, are managing system requirements, analyzing the trade-offs between system requirements and commercial products, analyzing dependencies among commercial products, limiting modification of commercial products, and integrating commercial component-based systems with legacy systems.

Prior GAO Reports Have Identified the Need for Improvements in FBI Corporate IT and Sentinel-Specific Management

Beginning in 2005, we have reported on shortfalls in the FBI's efforts to define and implement key IT management controls, such as centralizing IT responsibility and authority under the Chief Information Officer, defining and implementing an enterprise architecture, establishing IT investment management, defining and implementing systems development and acquisition practices, and strategically managing human capital, and have made recommendations to address these shortfalls that the FBI has largely agreed with. In September 2005,[12] we reported that the FBI had taken a range of steps to establish these institutional management controls. For example, it has centralized IT responsibility and authority under the Chief Information Officer, who has taken steps to define and implement an enterprise architecture, establish IT investment management, define and implement systems development and acquisition practices, and strategically manage human capital. In doing so, the FBI recognized the importance of IT to its organizational transformation efforts, and made it one of the bureau's top 10 priorities. Consistent with this, the FBI's strategic plan contains explicit IT-related strategic goals, objectives, and initiatives (both near term and long term) to support the collection, analysis, processing, and dissemination of information. The bureau also

[10] D.E. Harter, M.S. Krishnan, and S.A. Slaughter, "Effects of Process Maturity on Quality, Cycle Time, and Effort in Software Product Development," *Management Science*, vol. 46, no. 4, (2000); and B.K. Clark, "Quantifying the Effects of Process Improvement on Effort," *IEEE Software* (November/December 2000).

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

[12] GAO-05-1014T.

created its earlier described life-cycle management directive to govern all phases and aspects of IT projects, including Sentinel.

More recently, our reports have recognized the FBI's efforts to establish corporate management controls, and added that a key remaining challenge was to build on and further mature these capabilities and implement them effectively on each of its IT investments, including Sentinel. More specifically, we reported that the success of Sentinel will depend on how well the FBI defines and implements its new IT management approaches and capabilities. Among other things, we said that it will be crucial for the FBI to manage Sentinel requirements in the context of its architectural environment and the availability of commercial products, and to understand the capabilities and dependencies among the commercial products to minimize incompatibilities. We also said that it was crucial to prepare users for the business processes and individual role and responsibility impacts associated with implementing a commercial component-based system. As we stated at the time, not taking these steps would increase the risk of not delivering promised system capabilities and benefits on time and within budget.

We also reported in October 2006 on Sentinel's implementation of IT human capital,[13] noting that while the FBI had moved quickly to staff the Sentinel program office, it had yet to adopt a strategic approach to managing Sentinel human capital and was not treating human capital as a program risk. Accordingly, we recommended that it adopt such an approach. The FBI agreed with our recommendations.

In July 2007, we reported on Sentinel's implementation of a number of key system acquisition management controls that are grounded in best practices.[14] Specifically, we reported that the FBI was managing Sentinel according to a number of these best practices. However, we also reported, among other things, that the Sentinel cost and schedule estimates were not reliably derived, and that the bureau lacked corporate policies and guidance for cost and schedule estimating that reflected a number of best practices. Accordingly, we recommended that the FBI amend its IT handbook to incorporate these practices and that it ensure that they are implemented on all IT programs, including Sentinel. The FBI agreed with this recommendation.

[13] GAO-07-19.

[14] GAO-07-912.

Sentinel Is Implementing Key Commercial Component-Based System Acquisition Methods, but Corporate Guidance Governing These Methods Is Not Fully Defined

In acquiring Sentinel, the FBI is implementing leading practices associated with effectively acquiring commercial IT solutions. For each of the five acquisition methods that we examined, key acquisition practices are being satisfied. Moreover, this is occurring even though corporate policies and guidance do not address all of the methods. In implementing them, the bureau is relying on either its prime contractor's approaches or Sentinel-specific plans. The steps that Sentinel is taking in light of this void in FBI policies and guidance are notable. To the extent that these steps can be reflected in the FBI life-cycle management directive or other corporate policies and guidance that are used to plan and execute IT investments, they can become more repeatable across all programs and projects.

Key Aspects of Requirements Management Are Being Implemented

Effective requirements management is fundamental to successfully acquiring any IT system. Among other things, managing system requirements includes (1) controlling changes to requirements by establishing a baseline set of requirements and formally reviewing and approving changes to the baselines in light of expected costs, benefits, and associated risks; and (2) ensuring that the different levels of requirements (e.g., high-level operational or user requirements and detailed system and technical requirements) and their associated design specifications and test cases are aligned and consistent with one another (bidirectional traceability).[15]

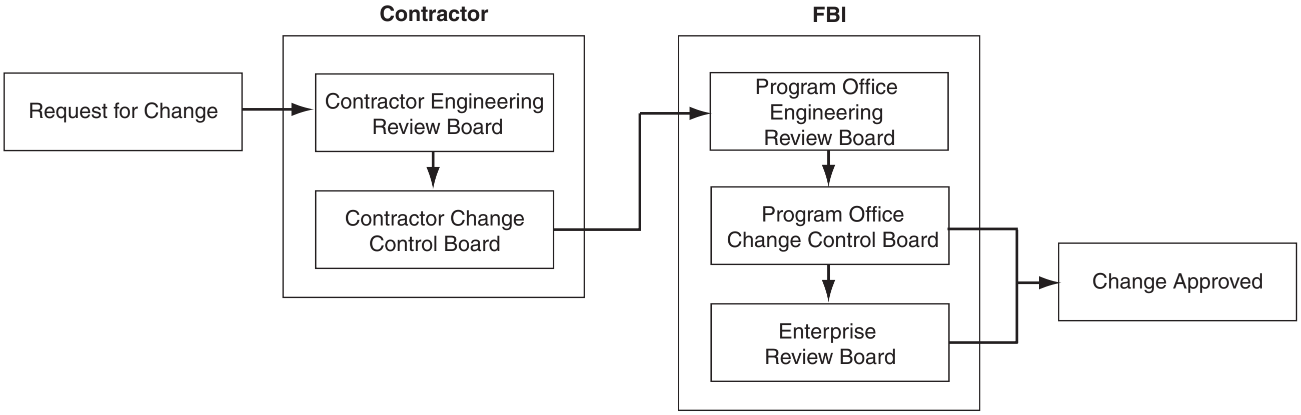
The Sentinel program office has defined plans and processes governing these two vital requirements management practices. Regarding the first practice, the program office has developed a configuration management plan that, among other things, establishes a process for submitting requirements change requests and for reviewing and approving these requests. As defined, this process provides for controlling changes to requirements baselines and associated documents. Further, it provides for only allowing changes to those baselines that have traversed a series of reviews and approvals by a hierarchy of contractor and program office review boards. More specifically, a proposed change request must be

[15] Carnegie Mellon University Software Engineering Institute, *Capability Maturity Model® Integration for Development*, version 1.2 (August 2006).

technically analyzed and approved by two levels of contractor review boards before it can be submitted to the FBI for program office review. Change requests submitted to the program office are first logged in by the configuration management team and analyzed for technical content. Once the content is validated, the team assesses the request's impact on program cost, schedule, and scope, and coordinates the reviews by the two program office review boards. The Engineering Review Board assesses the impact of the proposed change and makes recommendations to the Configuration and Change Management Board, which reviews the changes and, if within its authority, approves the request. Otherwise, the program office submits the request to the FBI's enterprise review board for approval. Under the process, each board's decisions are to be based on the proposed change's costs and benefits, as well as its risks to the program's ability to meet existing cost and schedule commitments. Once a change has been approved by the FBI, it is given to the contractor for incorporation into the baseline system configuration. (See fig. 3 for a summary of this process.)

To assist in implementing this process, the program office and the contractor are using a software tool that tracks and manages the change control process, ensuring that only approved changes are reflected in the baselines. We observed the operation of this tool and its capabilities, tracking one of the five actual change requests associated with Phase 2, Segment 1. In doing so, we witnessed the tool perform key functions and found that both the change control process and the tool were being implemented properly for the change request we observed.

Figure 3: Sentinel Requirements Change Control Process


Contractor
FBI
Request for Change
Contractor Engineering Review Board
Contractor Change Control Board
Program Office Engineering Review Board
Program Office Change Control Board
Enterprise Review Board
Change Approved

Source: GAO analysis of FBI data.

The program office's configuration management plan also describes a process for ensuring that requirements are traceable. To implement the configuration management plan and its requirements traceability process, the program office is using the above cited automated tool. This tool allows each requirement to be linked from its most conceptual, high-level definition to its most detailed, technical definition, as well as to design specifications and test cases. In effect, the tool maintains the linkages among the different levels of requirements, system design specifications, and test cases, even when the requirements change. To verify this traceability, we randomly selected 55 of the 241 Sentinel technical requirements for Sentinel Phase 2 Segment 1. We confirmed that all 55 were traceable both backwards to higher-level requirements and forward to design specifications and test results.[16]

As a result of its efforts, the program office has increased the chances that Sentinel will deliver capabilities that align with user and mission needs, and that it will not result in system capabilities that are unnecessary and not justified.

[16] Based on the results of our random sample, the 95 percent confidence interval for the Sentinel technical requirements that are not traceable is from 0 to 5 percentage points.

Important Aspects of Effective Requirements and Commercial Product Trade-Off Analysis Are Being Employed

Analyzing the trade-offs among defined system requirements and the capabilities offered by commercial products, including the products' conformance to the organization's architectural environment, is essential to successful delivery of commercial component-based IT programs such as Sentinel. By performing such analyses, an organization can understand which system requirements can and cannot be met by commercially available, architecturally compliant components and what cost-effective alternatives are available for meeting requirements that commercial products cannot meet. To accomplish this, best practices provide for (1) performing trade-off analyses early and continuously in a system's acquisition life cycle; (2) analyzing the gaps between defined requirements and commercial component capabilities to understand component feasibility; (3) ensuring that these analyses address the relative quality and cost trade-offs among such competing variables as system requirements, operational environment (current and future), cost and schedule constraints, and commercial product availability; and (4) involving relevant stakeholders in trade-off analyses and decision making.[17]

The program office is employing key practices for analyzing trade-offs between Sentinel requirements and available commercial products. For example, the Sentinel Systems Engineering Management Plan addresses the timing of trade-off analyses, stating that they are to be performed throughout the system's engineering life cycle. Thus far, the prime contractor has prepared two Sentinel trade-off analyses during Phase 2. While the first analysis, dated November 30, 2007, was performed late, according to a program office lessons learned document,[18] program officials told us that they have since taken steps to ensure that contractor-prepared analyses are done early and continuously. In this regard, we verified that the Phase 2 Integrated Master Schedule provides for a series of trade-off studies.

Further, Sentinel's engineering management plan also requires that the trade studies evaluate the advantages and disadvantages of candidate products using objective and relevant requirements-based criteria. Both

[17] See, for example, GAO, *Business Modernization: Some Progress Made toward Implementing GAO Recommendations Related to NASA's Integrated Financial Management Program*, GAO-05-799R (Washington, D.C.: Sept. 9, 2005); GAO-04-722; and GAO, *Business Modernization: Improvements Needed in Management of NASA's Integrated Financial Management Program*, GAO-03-507 (Washington, D.C.: Apr. 30, 2003).

[18] Sentinel Lessons Learned, version 2.6 (Feb. 15, 2008).

trade studies produced to date addressed this requirement by identifying gaps between relevant Sentinel requirements and the capabilities of the candidate commercial products. The first study, for example, found that only two of the evaluated products were able to satisfy a Sentinel requirement related to the versioning of reusable document templates.

Both of the trade studies also discuss relative quality/cost trade-offs among competing alternatives. In particular, both describe the extent to which the candidate products meet Sentinel requirements and their compatibility with the FBI's operational environment, and both use the relative costs and capabilities of product alternatives as a selection criterion. In addition, the second study takes into account the availability of the products. According to a contractor official, trade studies include only products that are immediately available in the commercial marketplace.

Further, while the above cited Sentinel lesson learned document states that the first study was performed without adequate stakeholder involvement, the second study addresses this lesson learned by involving the program office, including having the program office decide which product alternatives to pursue based on contractor recommendations. This involvement was evidenced by the fact that one version of this study reflects program office comments and input.

By ensuring that its second trade study is better aligned with relevant best practices, the program office is better positioned to make informed decisions in satisfying Sentinel requirements.

Key Aspects of Commercial Product Dependency Analysis Are Being Implemented

Dependency analysis is a key factor in verifying that acquisition decisions are based on deliberate and thorough research, analysis, and evaluation of commercial components' ability to interoperate effectively. The purpose of dependency analysis is to ensure that relationships between commercial products that need to interoperate as part of an integrated solution are fully understood before the products are purchased. As we have previously reported, analysis of component dependencies should be guided by a methodology that defines the activities that are to occur as part of system design. These activities include (1) allocating requirements among the various commercial components that constitute a given system design option, (2) defining the interactions among the various components to enable the successful interaction between them, and (3) using iterative prototyping to assess interactions among components.[19]

The Sentinel Program Office has relied on the prime contractor to perform these analyses using the contractor's approach and methods. Our analysis of available documentation shows that the contractor's approach and methods satisfy the key practices associated with effective commercial component dependency analysis. First, the prime contractor's requirements allocation approach calls for high-level system requirements to be allocated to program phases and segments, and for these requirements to be further decomposed into more detailed (technical) requirements and allocated to specific system components during design activities.

Second, Sentinel design documents define interactions that are to occur among the system components, including technical details required for the interactions, such as message/data formatting requirements, data transfer rates, transfer protocols, and security/privacy constraints.

Third, the second trade study states that selected vendors were asked to bring their software products into the prime contractor's software development facility in order to compare the products in a consistent manner. In doing so, the products were prototyped to determine how quickly and easily they could be integrated with the existing Sentinel system architecture. According to a prime contractor official, prototyping is also performed as part of product design to validate trade-off analysis decisions.

Implementing the full range of activities that allow for the relationships among commercial products to be fully understood before implementation activities begin will help the program office reduce the risk of integration problems, and thus avoid cost and schedule shortfalls.

Modification of Commercial Products Is Being Limited

Limiting changes to the commercial products that are used to create an IT system to only those changes that are justified on the basis of life-cycle costs and benefits is an important acquisition method. As we have previously reported,[20] this decreases the risk of a commercial product

[19] See, for example, GAO-05-799R.

[20] GAO-04-722.

being modified to the point that it becomes a one-of-a-kind, customized solution that is no longer supported by new releases of the vendor's product, thus becoming costly to maintain. Among other things, effectively controlling modifications to commercial components includes (1) having a defined policy or guidance governing modification of commercial products, (2) ensuring that any modification is justified on the basis of the life-cycle impact on system costs and benefits, and (3) working proactively with the product's vendor to incorporate planned modifications into the next release of the product.[21]

To the program office's credit, it has taken steps to employ each of these practices on Sentinel. First, the prime contractor's Systems Engineering Management Plan explicitly discourages the modification of commercial and government off-the-shelf IT components to the maximum extent possible. Further, senior officials, including the FBI Chief Information Officer and Sentinel Deputy Program Manager, told us that they are committed to avoiding such modifications.

Second, the Systems Engineering Management Plan states that the cost/benefit impacts of requirements changes that will involve modifying commercial products must be considered in approving any such change. This plan also provides for analyzing the total ownership costs (i.e., life-cycle costs) and schedule impact of any commercial, off-the-shelf product modifications necessary to meet Sentinel requirements, and it provides guidance for conducting these analyses.

Third, program officials and prime contractor representatives told us that they intend to request that commercial product vendors incorporate needed modifications to their products into future product releases. According to Sentinel officials, their efforts to limit commercial product modifications are aimed at avoiding the pitfalls that have befallen other commercial component-based systems. They further stated that they have not modified any of the components used to date in deploying Phase 1 and 2 capabilities, and they do not intend to modify any going forward. This is important because future Sentinel segments and increments call for continued use of commercial components, thus making these practices critical to the program's success.

[21] See, for example, GAO-04-722.

By establishing and implementing these component modification practices on Sentinel, the program office is increasing its ability to effectively use commercial products and minimizing its exposure to cost risks.

Steps Are Underway to Address Legacy System Integration

Successful delivery of a system like Sentinel requires integration with an organization's existing (i.e., legacy) systems. To effectively implement this acquisition method, it is important for a program office to ensure that the new system provides interfaces to the legacy systems and that legacy system owners are developing and testing required interfaces. According to leading practices, legacy system integration includes, among other things (1) identifying the systems to be integrated, (2) defining system interfaces, (3) working to establish the sequence and readiness of legacy systems integration, and (4) developing and testing the interfaces.[22]

The Sentinel program office has taken steps to implement these key practices, and in doing so has relied on its prime contractor to apply its own methodology for integrating legacy systems. Specifically, the Sentinel high-level system requirements identify the systems to be integrated with Sentinel. Moreover, design documents include high-level descriptions of Sentinel's intended interfaces to key FBI legacy systems, as well as interfaces to systems external to the FBI. According to program officials and prime contractor representatives, system integration planning will not occur until a specific program segment begins. Further, program officials stated that since the Phase 2 increments completed to date (i.e., Segment 1 increments) have required minimal integration with legacy or external systems, little interface definition and integration planning has yet been necessary.

Program officials told us that they intend to establish agreements, ranging from informal agreements to signed memoranda of understanding, with legacy system owners to ensure that their respective systems are ready in time for integration with Sentinel. According to these officials, the specific plans governing the sequence of these systems' readiness will be developed in accordance with Sentinel's incremental development approach. Further, an official said that the first increment to involve interfaces with legacy systems is underway.

[22] Carnegie Mellon University Software Engineering Institute, *Capability Maturity Model® Integration for Development*, version 1.2 (August 2006).

Further, the development and testing of Sentinel's legacy interfaces are to be detailed during segment planning. Since the increments that have been completed to date (i.e., Segment 1 increments) have required little integration with legacy or external systems, the development and testing of interfaces have not yet been necessary.

By taking steps to manage the integration of Sentinel with legacy systems, the program office will be better positioned to ensure that Sentinel is deployed on time and performs as intended.

FBI Policies and Guidance Do Not Address Most Key Acquisition Methods

With the exception of the practices that relate to effective requirements management, not all of the key practices that were earlier discussed in association with (1) requirements/commercial product trade-off analysis, (2) commercial product dependency analysis, (3) commercial product modification, and (4) legacy system integration management are fully reflected in any bureauwide policy or guidance. The extent to which the practices related to each of these five acquisition methods are addressed in FBI policies and guidance is discussed below:

- The FBI's life-cycle management directive addresses both requirements change control and requirements traceability. Specifically, the directive requires that projects manage and control requirements changes, including reviewing and controlling changes to baselined requirements and conducting and documenting impact analyses for any requirements change requests. The directive also speaks to the need for requirements to be traceable forward and backwards across the project life cycle, including the use of a requirements management tool that supports traceability across functions and interfaces as well as requirements tracking and reporting.

- For requirements/commercial product trade-off analysis, the FBI's life-cycle management directive partially addresses key practices. Specifically, the directive includes an appendix that provides a structural template outlining the content of a trade study or analysis to help choose among competing commercial component solutions for meeting a given mission need or problem. According to the template, analyses should be undertaken early in a system's life cycle (during the concept exploration phase) and should be updated and used throughout a system's life-cycle phases. Further, its content should include, among other things, a statement of the problem being addressed or the purpose of the study, the evaluation or selection criteria and related weighting factors being used, the alternative solutions being evaluated and their characteristics, a comparative analysis of the solutions to include weighted scoring of each, and a recommended course of action. However, the directive does not explicitly address, for example, (1) analyzing the gaps between defined requirements and the capabilities of commercial component alternatives to understand each component's feasibility, (2) ensuring that the analyses' selection criteria include the relative quality and costs of competing alternatives relative to system requirements and the organization's operational environment (current and future), and (3) involving relevant stakeholders in the analysis and decision-making process.

- For commercial product dependency analysis, neither the FBI's life-cycle management directive nor the related handbook addresses the key practices associated with this acquisition method. While FBI officials stated that they rely on contractors to perform the practices associated with this method because the practices are engineering oriented, it is important for the bureau to provide its program managers with policy and guidance relative to the method so that they can be positioned to effectively manage and oversee the contractors' efforts.

- For commercial product modification, the FBI's Business Process Reengineering Executive Playbook[23] partially addresses the method's associated practices. Specifically, it states that the FBI is to limit the modification of commercial component systems, adding that modifying a commercial product negates the advantages of using such systems and introduces major problems in maintaining the system's software. However, neither the FBI's life-cycle management directive nor the reengineering playbook explicitly addresses two other key practices: (1) ensuring that any modification is justified on the basis of the life-cycle impact on system costs and benefits and (2) working proactively with the product's vendor to incorporate planned modifications into the next release of the product.

- For legacy system integration management, the FBI's Transition and Sequencing Plan partially addresses two key practices. Specifically, this plan recognizes the importance of identifying the legacy systems that will need to be integrated, and in particular, identifies those systems relative to Sentinel. In addition, the plan also recognizes the need to understand the dependencies among systems as a means to determining their sequencing, and, in this regard, provides time frames of when systems that are to be impacted by Sentinel will be, among other things, interfaced to it. However, the FBI's policy and guidance documents do not address the

[23] Office of Chief Information Officer, *Business Process Reengineering Executive Playbook*, Business Process Management Office, Federal Bureau of Investigation.

other two key practices associated with this method: (1) defining system interfaces and (2) developing and testing the interfaces.

By not defining these practices in FBI corporatewide policies and guidance, the chances that they will be implemented on a repeatable basis across all bureau IT programs and projects are reduced.

Conclusions

Successfully implementing large-scale IT programs depends in large part on the rigorous implementation of acquisition management best practices. For systems like Sentinel, which are to minimize the development and use of customized software, relevant best practices extend to those that are unique to commercial component-based systems. Following such practices minimizes a program's exposure to risk and helps deliver promised capabilities and benefits on time and within budget. This is especially important for the Sentinel system, which is to provide long-overdue, mission-critical intelligence and investigative services across the FBI.

Employing such practices in a repeatable fashion across all programs requires that these practices be institutionally defined and that their use be enforced and measured. The FBI has, for the most part, not institutionalized defined key practices associated with requirements/commercial product trade-off analysis, commercial product dependency analysis, commercial product modification, and legacy system integration. To the credit of Sentinel program officials, this void in corporate policies and guidance is being effectively overcome, as the program is implementing these key practices either through reliance on its prime contractor's approaches or through Sentinel-specific plans. If these Sentinel practices are successfully incorporated into FBI-wide policies and guidance, then their chances of being employed on a repeatable basis across all applicable FBI system investments will be increased.

Recommendations for Executive Action

To leverage key commercial component-based acquisition methods being implemented on Sentinel, and increase the chances of these practices being implemented on all FBI IT programs, we are making four recommendations. We recommend that the FBI Director instruct the Chief Information Officer to incorporate into FBI policy or guidance each of the practices that we identified in this report as not being addressed relative to (1) requirements/commercial product trade-off analysis, (2) commercial product dependency analysis, (3) commercial product modification, and (4) legacy system integration management.

Agency Comments

In written comments on a draft of this report, signed by the FBI Chief Information Officer and reprinted in appendix II, the bureau agreed with our findings and recommendations, adding that our review of Sentinel was thorough. The bureau also stated that it is committed to creating policies, procedures, and processes that are standardized, repeatable, and reflective of industry best practices, and it described steps that are either planned or underway to address our recommendations. For example, the FBI stated that it will examine or is examining its processes and procedures for analyzing and understanding gaps between defined requirements and the capabilities of commercial products, and ensuring that product selection decisions are based on the relative quality and costs of competing alternatives.

We are sending copies of this report to the Chairman and Vice Chairman of the Senate Select Committee on Intelligence and the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence, as well as to the Chairman and Ranking Member of the Senate Committee on the Judiciary, and the Chairman and Ranking Member of the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies. We are also sending copies to the Attorney General; the Director, FBI; the Director, Office of Management and Budget; and other interested parties. In addition, 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. Contact points for our Office of Congressional Relations and Public Affairs Office may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Randolph C. Hite

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

Appendix I: Objective, Scope, and Methodology

Our objective was to determine whether the Federal Bureau of Investigation (FBI) is employing effective methods in acquiring commercial solutions for Sentinel. To accomplish this, we focused on the following five key information technology (IT) management areas: (1) requirements management, (2) requirements/commercial product trade-off analysis, (3) commercial product dependency analysis, (4) commercial product modification, and (5) legacy system integration.

To address our objective, we researched relevant best practices, including published guidance from the Software Engineering Institute and GAO-issued reports associated with each of these five areas.[1] To identify the FBI's efforts, we obtained and reviewed FBI IT management policies and guidance, including its Information Technology Life Cycle Management Directive (Version 3.0),[2] Project Manager's Handbook, and Business Process Reengineering Executive Playbook, and compared them to the practices in each of the five IT management areas to determine the extent to which they were included in FBI guidance.

We also reviewed program office and prime contractor planning and program management documentation, including the Sentinel Systems Engineering Management Plan (Version 3) and Sentinel Configuration Management Plan (Version 3). In addition, we interviewed Sentinel program officials as well as prime contractor representatives, as appropriate, to determine how the FBI had defined its approach to managing each of these five areas and how it had actually implemented them on Sentinel. In reviewing the FBI's implementation on Sentinel, we focused primarily on Phase 2, Segment 1, which was the segment being developed at the time we began our review. We also performed the following additional audit work:

[1] Carnegie Mellon University Software Engineering Institute, *Capability Maturity Model® Integration for Development*, version 1.2 (August 2006); Carnegie Mellon University Software Engineering Institute, *Interpreting Capability Maturity Model® Integration (CMMI®) for COTS-Based Systems* (October 2003); GAO, *Business Modernization: Some Progress Made toward Implementing GAO Recommendations Related to NASA's Integrated Financial Management Program*, GAO-05-799R (Washington, D.C.: Sept. 9, 2005); GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722, (Washington, D.C.: July 30, 2004), and GAO, *Business Modernization: Improvements Needed in Management of NASA's Integrated Financial Management Program*, GAO-03-507 (Washington, D.C.: Apr. 30, 2003).

[2] According to a program office official, a new version of this directive has been drafted.

- For requirements management, we reviewed: (1) the Sentinel Configuration Management Plan, (2) the contractor's Requirements Satisfaction Report, and (3) the contractor's System Design Document. In addition, to determine the extent to which the requirements were traceable, we randomly selected 55 requirements from the program office's Requirement's Traceability Matrix and traced them backwards to the Sentinel System Requirements Specification and forward to design specifications and test cases. This sample was designed with a 5 percent tolerable error rate at the 95 percent level of confidence, so that if we found 0 problems in our sample we could conclude statistically that the error rate was less than 5 percent. Based upon the weight of all other factors included in our evaluation, our verification of 55 out of 55 requirements was sufficient to demonstrate traceability. Further, we tracked one of the five change requests associated with Phase 2, Segment 1 to determine whether the change had been reviewed and approved consistent with the established requirements change control process. In addition, we interviewed program officials involved in the requirements management process to discuss their roles and responsibilities for managing requirements.

- For trade-off analysis, we reviewed: (1) the Sentinel Lessons Learned document, (2) the Forms Tool Capability Trade Study, (3) the Search Tool Capability Trade Study, and (4) the Design Concept Description and Architecture. In addition, we interviewed the prime contractor's Chief Architect for Sentinel to discuss trade studies.

- For commercial product dependency analysis, we reviewed: (1) two Sentinel Interface Control Documents and (2) the Interface Design Document. We also reviewed the above cited trade studies with respect to efforts to prototype the interaction among commercial products that were being studied. In addition, we interviewed the prime contractor's Chief Architect for Sentinel to discuss how trade studies took commercial product dependencies into account.

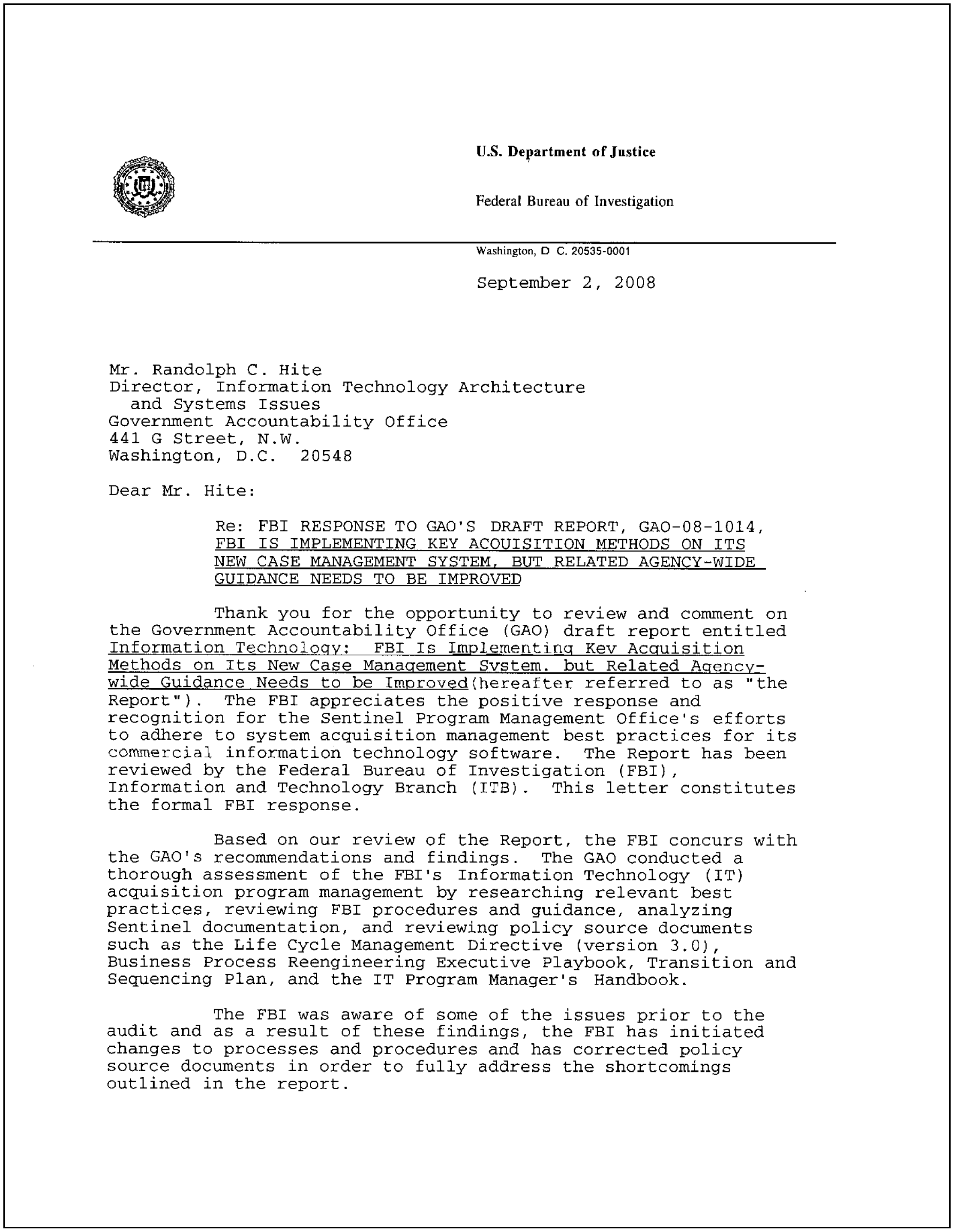
- For commercial product modification, we reviewed the Systems Engineering Management Plan and interviewed the FBI Chief Information Officer and Sentinel Deputy Program Manager about their commercial product modification policies.

- For legacy system integration, we reviewed the Sentinel (1) Design Concept Description and Architecture, (2) Interface Design Document, (3) Software Design Document, and (4) Test and Evaluation Master Plan. In addition, we interviewed the Sentinel System Analysis Section Lead to discuss Sentinel's integration of legacy systems.

To assess data reliability, we reviewed quality and access controls of the program office systems and tools used to generate the data. We also reviewed related program documentation to substantiate data provided by program officials during interviews. Further, we have also made appropriate attribution in the report to indicate the data's sources.

We conducted our work from our Washington, D.C., headquarters, and at FBI headquarters and facilities in the greater Washington, D.C., metropolitan area between October 2007 and September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Federal Bureau of Investigation



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D C. 20535-0001

September 2, 2008

Mr. Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

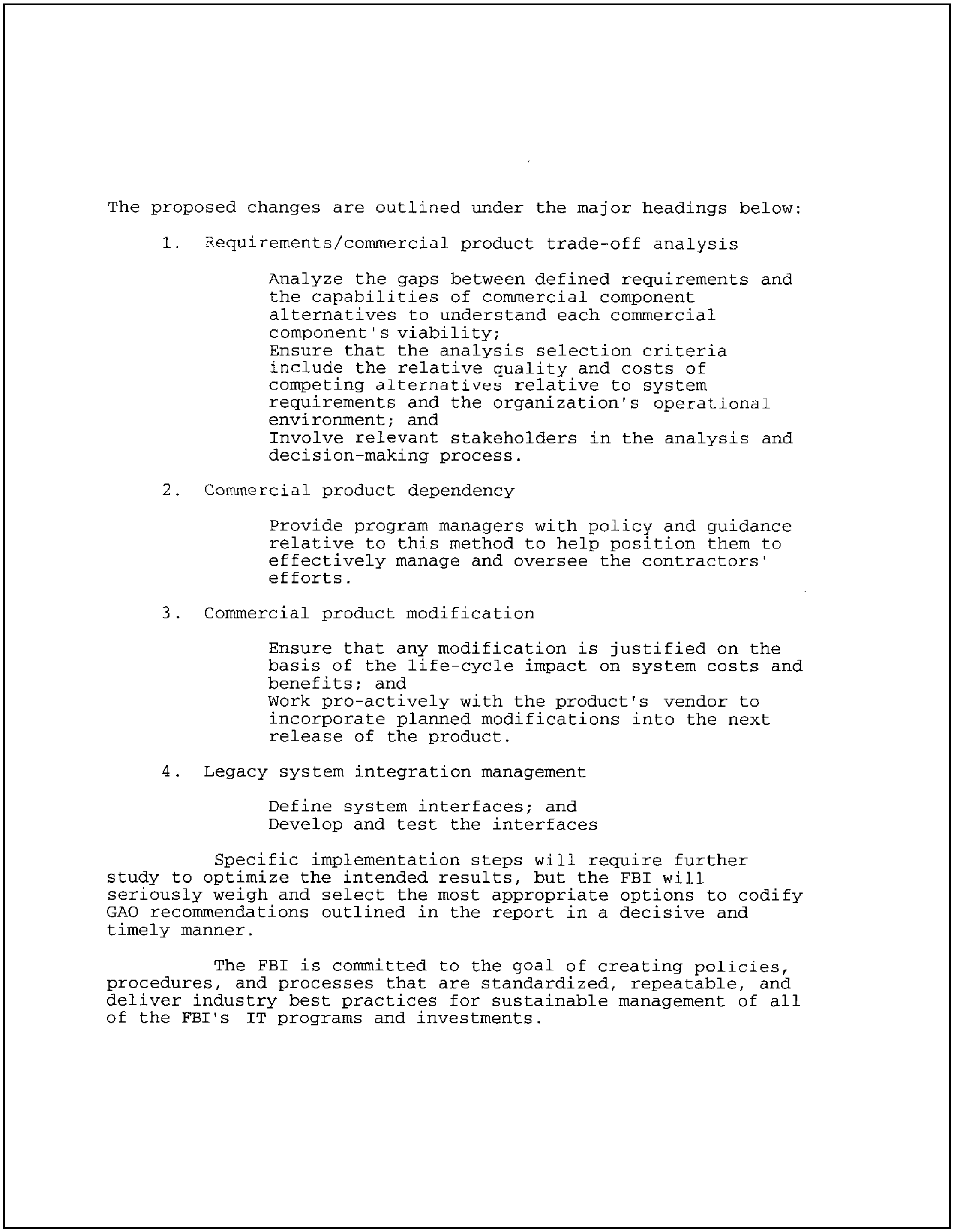
Dear Mr. Hite:

Re: FBI RESPONSE TO GAO'S DRAFT REPORT, GAO-08-1014, FBI IS IMPLEMENTING KEY ACQUISITION METHODS ON ITS NEW CASE MANAGEMENT SYSTEM, BUT RELATED AGENCY-WIDE GUIDANCE NEEDS TO BE IMPROVED

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled Information Technology: FBI Is Implementing Key Acquisition Methods on Its New Case Management System, but Related Agency-wide Guidance Needs to be Improved(hereafter referred to as "the Report"). The FBI appreciates the positive response and recognition for the Sentinel Program Management Office's efforts to adhere to system acquisition management best practices for its commercial information technology software. The Report has been reviewed by the Federal Bureau of Investigation (FBI), Information and Technology Branch (ITB). This letter constitutes the formal FBI response.

Based on our review of the Report, the FBI concurs with the GAO's recommendations and findings. The GAO conducted a thorough assessment of the FBI's Information Technology (IT) acquisition program management by researching relevant best practices, reviewing FBI procedures and guidance, analyzing Sentinel documentation, and reviewing policy source documents such as the Life Cycle Management Directive (version 3.0), Business Process Reengineering Executive Playbook, Transition and Sequencing Plan, and the IT Program Manager's Handbook.

The FBI was aware of some of the issues prior to the audit and as a result of these findings, the FBI has initiated changes to processes and procedures and has corrected policy source documents in order to fully address the shortcomings outlined in the report.



The proposed changes are outlined under the major headings below:

1. Requirements/commercial product trade-off analysis

   Analyze the gaps between defined requirements and the capabilities of commercial component alternatives to understand each commercial component's viability;

   Ensure that the analysis selection criteria include the relative quality and costs of competing alternatives relative to system requirements and the organization's operational environment; and

   Involve relevant stakeholders in the analysis and decision-making process.

2. Commercial product dependency

   Provide program managers with policy and guidance relative to this method to help position them to effectively manage and oversee the contractors' efforts.

3. Commercial product modification

   Ensure that any modification is justified on the basis of the life-cycle impact on system costs and benefits; and

   Work pro-actively with the product's vendor to incorporate planned modifications into the next release of the product.

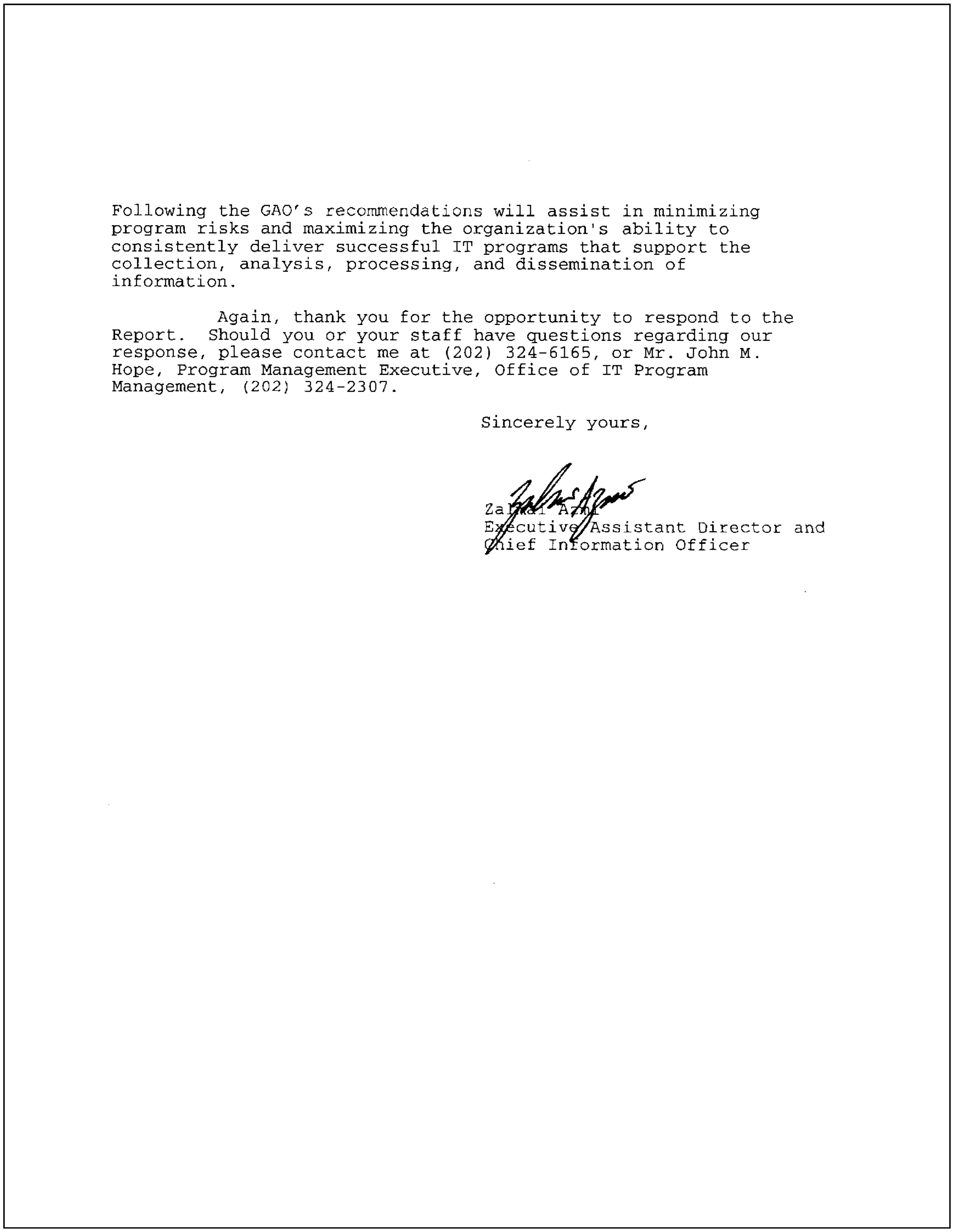
4. Legacy system integration management

   Define system interfaces; and

   Develop and test the interfaces

Specific implementation steps will require further study to optimize the intended results, but the FBI will seriously weigh and select the most appropriate options to codify GAO recommendations outlined in the report in a decisive and timely manner.

The FBI is committed to the goal of creating policies, procedures, and processes that are standardized, repeatable, and deliver industry best practices for sustainable management of all of the FBI's IT programs and investments.



Following the GAO's recommendations will assist in minimizing program risks and maximizing the organization's ability to consistently deliver successful IT programs that support the collection, analysis, processing, and dissemination of information.

Again, thank you for the opportunity to respond to the Report. Should you or your staff have questions regarding our response, please contact me at (202) 324-6165, or Mr. John M. Hope, Program Management Executive, Office of IT Program Management, (202) 324-2307.

Sincerely yours,

Zalmai Azmi
Executive Assistant Director and
Chief Information Officer

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite at (202) 512-3439 or hiter@gao.gov

Staff Acknowledgments

Major contributors to this report were Deborah Davis (Assistant Director), Paula Moore (Assistant Director), Carl Barden, Sharhonda Deloach, Neil Doherty, Nancy Glover, Daniel W. Gordon, Lee McCracken, Teresa Smith, Eric Trout, and Kevin Walsh.

(310656)

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 "E-mail 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, DC 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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON RECYCLED PAPER