United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2007

INFORMATION TECHNOLOGY

FBI Following a Number of Key Acquisition Practices on New Case Management System, but Improvements Still Needed

GAO-07-912

July 2007

INFORMATION TECHNOLOGY

FBI Following a Number of Key Acquisition Practices on New Case Management System, but Improvements Still Needed

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-912, a report to congressional requesters

Why GAO Did This Study

The Sentinel program is intended to replace and expand on the Federal Bureau of Investigation's (FBI) failed Virtual Case File (VCF) project and thereby meet the bureau's pressing need for a modern, automated capability to support its field agents and intelligence analysts' investigative case management and information sharing requirements. Because of the FBI's experience with VCF and 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 Sentinel. This review focuses on the FBI's (1) use of effective practices for acquiring Sentinel and (2) basis for reliably estimating Sentinel's schedule and costs. To address its objectives, 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 Sentinel's success, GAO is recommending that the FBI (1) strengthen support contractor tracking and oversight and (2) establish and implement policies, procedures, and tools needed to develop reliable schedule and cost estimates for IT programs, including Sentinel. The FBI concurred with GAO's second recommendation, but not the first. GAO does not agree with FBI's position.

www.gao.gov/cgi-bin/getrpt?GAO-07-912.

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

The FBI is managing its Sentinel program according to a number of key systems acquisition best practices. For example, the FBI has followed best practices when soliciting offers from contractors to lead the development of Sentinel; it has also followed the practices in evaluating the offers and making a contract award decision. In addition, it has established and is following effective processes to proactively identify and mitigate program risks before they have a chance to become actual cost, schedule, or performance problems. Further, it has taken a range of steps to effectively define expectations for its prime contractor and to measure performance against these expectations and related incentives and hold the contractor accountable for results. However, the bureau has not done the same for one key aspect of tracking and overseeing its program management support contractors. In particular, it has not established performance and product quality standards for these support contractors. According to FBI officials, such standards are not necessary because they monitor their support contractors on a daily basis, including the review and approval of all work products. By not implementing this practice, GAO believes that the FBI's monitoring does not adequately ensure that Sentinel support contractors are performing important program management functions effectively and efficiently.

The FBI's policies, procedures, and supporting tools that form the basis for Sentinel's schedule and cost estimates do not adequately reflect key best practices. While the FBI has issued an IT program management handbook, related guidance, and tools that define how IT program schedules and costs are to be estimated, this handbook and related material do not, for example, address such key practices as having a historical database of program schedule and cost estimates to inform future estimates. As a result, the reliability of Sentinel's schedule and cost estimates is questionable. GAO's analyses of the Sentinel cost estimates and program officials' statements confirm this. For example, the analyses show that the estimates do not include all relevant costs, such as a technology refresh, and are not grounded in fully documented methodologies or a corporate history of experiences on other IT programs. FBI officials agreed that they need to update their IT program management handbook and related materials to incorporate schedule and cost estimating best practices and to establish a historical database of its estimating experiences on IT programs. Until FBI takes these steps, IT programs, such as Sentinel, are unlikely to have reliable schedule and cost estimates to support informed investment decision making, and their actual progress is unlikely to track closely to estimates.

Contents

Figures

Abbreviations

CIO-SP2i	Chief Information Officer-Solutions and Partners 2
COTS	commercial off-the-shelf
GEMPC	government estimate of most probable cost
GWAC	governmentwide acquisition contract
IGCE	independent government cost estimate
NIH	National Institutes of Health
VCF	Virtual Case File

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 30, 2007

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

In early 2005, the Federal Bureau of Investigation (FBI) began its Sentinel program, estimated to be a 6-year, $425 million program to replace and expand both its failed Virtual Case File (VCF) project and its antiquated, paper-based, legacy system for supporting mission-critical intelligence analysis and investigative case management activities. One of the reasons we and others have cited for VCF's failure was limited use of acquisition management best practices. Because of the FBI's experience with VCF and the importance of Sentinel to the bureau's mission operations, you requested us to review the FBI's management of Sentinel.

In response to your request, we agreed to perform a series of incremental reviews to address a broad range of objectives. We initiated our work on these reviews in August 2005 and released the first of our reports on Sentinel in October 2006.[1] This report provides the results of our second

[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.: October 2006).

review. As agreed, the two specific objectives for this report are to determine the FBI's (1) use of effective practices for acquiring Sentinel and (2) basis for reliably estimating Sentinel's schedule and costs. For the first objective, we focused on contract solicitation and award, risk management, organizational change management, configuration management, and contractor tracking and oversight. In addressing both objectives, we researched relevant best practices, reviewed FBI policies and procedures, program plans and other program documents, and interviewed appropriate program officials to ascertain whether the practices had been defined and implemented. 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 September 2005 and May 2007 in accordance with generally accepted government auditing standards. Details on our objectives, scope, and methodology are included in appendix I.

Results in Brief

The FBI is managing various aspects of Sentinel according to a number of effective system acquisition best practices. According to FBI officials, they have made these practices an area of focus in order to minimize Sentinel's exposure to risk. Our research shows that use of these and other practices increase the chances of program success. For Sentinel, the FBI has

- taken appropriate steps when soliciting proposals from contractors to lead the development of Sentinel and when evaluating the offers and awarding contracts;
- established and is following effective processes to proactively identify and mitigate program risks before they have a chance to become actual cost, schedule, or performance problems;
- begun to plan and position itself for the human capital and business process changes that are embedded in the commercial software products that are to be used for Sentinel, such as changes to staff roles and responsibilities and the procedures governing the execution of them;
- established and is implementing controls and tools for systematically identifying Sentinel's component parts (software, hardware, and documentation) and controlling this configuration of parts in a way that reasonably ensures the integrity of each; and

- undertaken a range of activities to effectively define expectations for the prime contractor and to measure performance against and to hold the contractor accountable for meeting these expectations.

However, the bureau is not effectively performing a key tracking and oversight practice for its many support contractors that are performing program management functions. Specifically, it has not defined metrics-based performance standards for these contractors' services and products. FBI officials stated that this practice is not necessary because they monitor these support contractors on a daily basis, including review and approval of all work products. Given the bureau's extensive reliance on support contractors to augment its own program management staff, taking a more proactive, standards-based approach to maximize the performance of support contractors is important to Sentinel's overall success. By not establishing standards in statements of work governing the quality of these contractors' products and services, the FBI cannot adequately ensure that its support contractors are performing important program management functions efficiently.

The FBI's policies and procedures that form the basis for Sentinel's schedule and cost estimates are not fully consistent with reliable estimating practices. While the FBI has issued an IT program management handbook, related guidance, and tools that define how IT program schedules and costs are to be estimated, this handbook and related material do not, for example, address having a historical database of program schedule and cost estimates to inform future estimates. As a result, the reliability of Sentinel schedule and cost estimates is questionable. In this regard, our analysis of the Sentinel cost estimates shows that they do not include all relevant costs, such as a technology refresh and government labor and inflationary costs, and are not adequately grounded in fully documented methodologies or a corporate history of experiences on other IT programs. These limitations are in part because of the absence of key practices in the FBI's handbook and related materials and in part because the FBI did not follow its own handbook in estimating Sentinel's costs. Without reliable estimates, FBI leadership and Congress will not have an adequate basis for informed program decision making, and program execution is unlikely to track closely to estimates.

To ensure that the FBI maximizes the performance of its support contractors and produces and uses reliable cost and schedule estimates on programs like Sentinel, we are recommending that the bureau strengthen one key aspect of support contractor tracking and oversight and establish and implement the policies, procedures, and tools needed to reliably

develop schedule and cost estimates for all its IT programs, including Sentinel.

In written comments on a draft of this report, signed by the FBI Chief Information Officer, the bureau stated that it agreed with our second recommendation. However, the bureau disagreed with the first recommendation, stating that its existing efforts to track and oversee each Sentinel support contractor are sufficient. However, the FBI's comments did not fully address the underlying basis for our recommendation, which was that the absence of defined quality and timeliness standards for support contractor products and services limits the bureau's ability to clearly direct and measure contractor performance, in turn limiting how effectively and efficiently key program management functions could be performed. As a result, we disagree with the FBI's position on this recommendation. The FBI also provided technical comments, which we have incorporated as appropriate into the report.

Background

The FBI serves as the primary investigative unit of the Department of Justice. The FBI's 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 in more than 70 offices in the United States and in more than 50 offices in foreign countries. Mission responsibilities at the bureau are divided among a number of major organizational components, including:

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

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.

Office of the Chief Information Officer: develops the bureau's IT strategic plan and operating budget and develops and maintains technology assets.

Information Technology Is Instrumental to FBI Mission Operations

To execute its mission responsibilities, the FBI relies extensively on the use of information systems. 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;
- the National Crime Information Center and the Integrated Automated Fingerprint Identification System, which help state and local law enforcement agencies identify criminals;
- the Automated Case Management System, which manages information collected on investigative cases;
- the Investigative Data Warehouse, which aggregates data from disparate databases in a standard format to facilitate content management and data mining; and
- the Terrorist Screening Database, which consolidates identification information about known or suspected international and domestic terrorists.

Following the terrorist attacks in the United States on September 11, 2001, the FBI shifted its mission focus to detecting and preventing future attacks and began 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, FBI's primary case management application.

While the first two components of Trilogy experienced cost overruns and schedule delays, in part because of fundamental changes to requirements, both are currently operating. However, we recently reported[2] that certain information security controls over the Trilogy-related network were ineffective in protecting the confidentiality, integrity, and availability of information and information resources. For instance, we found that FBI did not consistently (1) configure network devices and services securely to prevent unauthorized insider access; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Taken collectively, we concluded that these weaknesses place sensitive information transmitted on the network at increased risk of unauthorized disclosure or modification and could result in a disruption of service. Accordingly, we recommended that the FBI Director take several steps to fully implement key activities of the bureau's information security program for the network. These activities include updating assessments and plans to reflect the bureau's current operating environment, providing more comprehensive coverage of system tests, and correcting security weaknesses in a timely manner.

In commenting on this report, the FBI's Chief Information Officer (CIO) concurred with many of our recommendations, but did not believe that the bureau had placed sensitive information at an unacceptable risk for unauthorized disclosure, modification, or insider threat exploitation. The CIO cited significant strides in reducing risk since the Robert Hanssen espionage investigation. In response, we stated that until weaknesses identified in network devices and services, identification and authentication, authorization, cryptography, audit and monitoring, physical security, and patch management are addressed, increased risk to FBI's critical network remains. Further, until the bureau fully and effectively implements certain information security program activities for the network, security controls will likely remain inadequate or inconsistently applied.

[2]GAO, *Information Security: FBI Needs to Address Weaknesses in Critical Network*, GAO-07-368 (Washington, D.C.: April 2007).

The third component of Trilogy—VCF— never became fully operational. In fact, the FBI terminated the project after Trilogy's overall costs grew from $380 million to $537 million. VCF fell behind schedule and pilot testing showed that completing it was infeasible and cost prohibitive. Among reasons we and others have cited for VCF's failure were poorly defined system requirements, ineffective requirements change control, limited contractor oversight, and human capital shortfalls because of, for example, no continuity in certain management positions and a lack of 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. In brief, Sentinel is to meet FBI's 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. The program's key objectives are to (1) successfully implement a system that acts as a single point of entry for all investigative case management and that provides paperless case management and workflow capabilities, (2) facilitate a bureau-wide organizational change management program, and (3) provide intuitive interfaces that feature data relevant to individual users. Using commercially available software and hardware components, Sentinel is to provide a range of investigative case management and workflow capabilities, including

- leads management and evidence management;
- document and records management, indexed searching, and electronic workflow;
- links to legacy FBI systems and external data sources;
- training, statistical, and reporting tools; and
- security management.

The FBI chose to use a governmentwide acquisition contract[3] (GWAC) for Sentinel after conducting a multi-step evaluation of the different GWACs available to federal agencies. In August 2005, the FBI issued a request for vendor proposals to more than 40 eligible companies under a National Institutes of Health (NIH)[4] contracting vehicle. According to the CIO, the request was also provided to more than 500 eligible subcontractors. For the next 8 months, FBI's Sentinel Source Selection Evaluation Team reviewed and evaluated vendors' responses to the task order request for proposal to determine which proposal represented the best value. The evaluation team recommended—and FBI ultimately chose—Lockheed Martin as the primary Sentinel contractor. In March 2006, the FBI awarded the task order to develop and integrate Sentinel to Lockheed Martin.

The FBI has structured the acquisition of Sentinel into four phases; the completion of each is expected to span about 12 to 18 months. According to FBI officials, the FBI is conducting end user training for Phase 1 and expects to roll out the Phase 1 production in June 2007. The specific content of each phase is to be proposed by and negotiated with the prime contractor. The general content of each phase has these and other capabilities include

Phase 1: A Web-based portal that will provide a data access tool for the Automated Case Management System and other legacy systems; a service-

[3]GWACs are governmentwide contracts authorized by the Clinger-Cohen Act to improve the acquisition of IT by federal agencies. GWACs are operated at the departments of Commerce and Transportation, the National Aeronautics and Space Administration, GSA's Federal Technology Service, and NIH. GWACs 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 order from it.

[4]NIH's CIO—Solutions and Partners 2 Innovations (CIO-SP2i) contract vehicle was created in 1996 to streamline federal agencies' purchasing of IT products and services. The contract has a spending cap of $19.5 billion and encompasses all aspects of support for federal CIOs, from direct technology purchases to consulting services for management activities. There are 45 prime contractors currently associated with the CIO-SP2i vehicle and, unlike other GWACs, prime contractors on this NIH vehicle may act as subcontractors for other primes.

oriented architecture[5] definition to support delivery and sharing of common services across the bureau.

Phase 2: Case document and records management capabilities, document repositories, improved information assurance, application workflow, and improved data labeling to enhance information sharing.

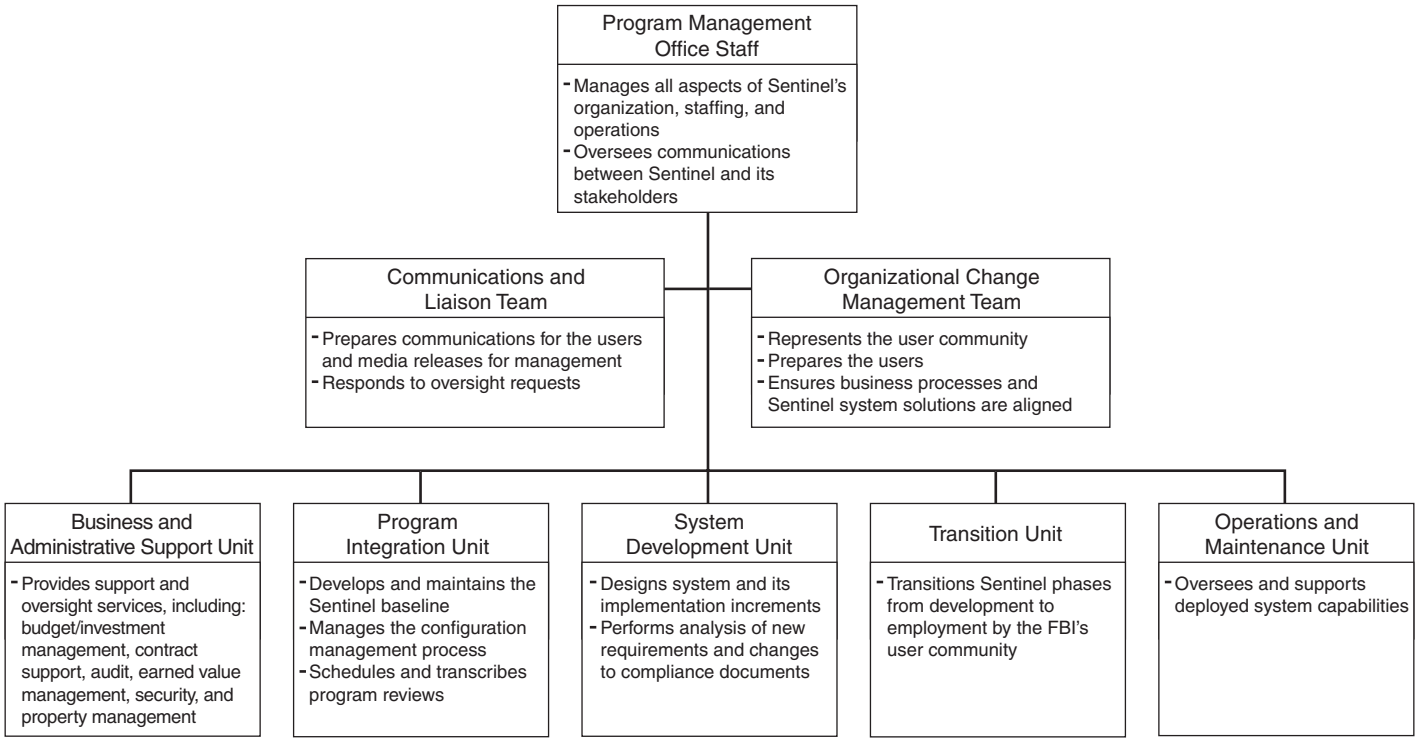
Phase 3: Updated and enhanced system storage and search capabilities.

Phase 4: Implementing the remaining components of the new case management system to replace ACS.

To manage the acquisition and deployment of Sentinel, the FBI established a program management office within the CIO's office. The program office is led by a program manager and consists of the eight primary FBI units (see fig. 1). Overall, the FBI estimates that the four phases will cost about $425 million through fiscal year 2011. For fiscal year 2005, the FBI reprogrammed $97 million in appropriated funds from various sources to fund Sentinel work. For fiscal years 2006 and 2007, the FBI said it budgeted about $85 million and $138 million respectively, for Sentinel, of which it reports having obligated about $95 million. For fiscal year 2008, the FBI reports that it has budgeted about $50 million for Sentinel.

[5]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 kind of flexibility needed to support a quicker response to changing and evolving business requirements and emerging conditions.

Figure 1: Sentinel Program Office Structure



Source: GAO analysis of FBI data.

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

Acquisition best practices are tried and proven methods, processes, techniques, and activities that organizations define and use 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 acquisitions projects indicated that teams using systems 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 discipline embedded in these practices. 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.[6]

We and others have identified and promoted the use of a number of best practices associated with acquiring IT systems. In 2004, we reported[7] on 18 relevant best practices and grouped them into two categories: (1) ten practices for acquiring any type of business system and (2) eight complementary practices that relate specifically to acquiring commercial component-based business systems. Examples of these practices relevant to any business systems acquisition include ensuring that (1) reasonable planning for all parts of the acquisition occurs, (2) a clear understanding of system requirements exists, and (3) risks are proactively identified and systematically mitigated. Examples of best practices relevant to commercial component-based systems acquisitions include ensuring that (1) commercial product modification is effectively controlled, (2) relationships among commercial products are understood before acquisition decisions are made, and (3) the organizational impact of using new system functionality is proactively managed. Each of these practices is composed of from one to eight activities and is summarized in table 1 and described in greater detail in appendix II.

Table 1: Summary of Business Systems Acquisition Best Practices

Best practices	Activity
Best practices relevant to any business systems acquisition	
Acquisition planning To ensure that reasonable planning for all parts of the acquisition is conducted.	• Plans are prepared during acquisition planning and maintained throughout the acquisition. • Planning addresses the entire acquisition process, as well as life cycle support of the products being acquired. • The acquisition organization has a written policy for planning the acquisition. • Responsibility for acquisition planning activities is designated.
Architectural alignment To ensure that the acquisition is consistent with the organization's enterprise architecture.	• The system being acquired is assessed for alignment with the enterprise architecture at key life cycle decision points, and any deviations from the architecture are explicitly understood and justified by an explicit waiver to the architecture. • Product line requirements——rather than just the requirements for the system being acquired——are an explicit consideration in each acquisition.

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

[7]GAO-04-722.

Best practices	Activity
Contract tracking and oversight To ensure that contract activities are performed in accordance with contractual requirements.	• The acquiring organization has sufficient insight into the contractor's activities to manage and control the contractor and ensure that contract requirements are met. • The acquiring organization and contractor maintain ongoing communication; commitments are agreed to and implemented by both parties. • All contract changes are managed throughout the life of the contract. • The acquisition organization has a written policy for contract tracking and oversight. • Responsibility for contract tracking and oversight activities is designated. • The acquiring organization involves contracting specialists in the execution of the contract. • A quantitative set of software and system metrics is used to define and measure product quality and contractor performance. • In addition to incentives for meeting cost and schedule estimates, measurable, metrics-based product quality incentives are explicitly cited in the contract.
Economic justification To ensure that system investments have an adequate economic justification.	• System investment decisions are made on the basis of reliable analyses of estimated costs, expected benefits, and anticipated risks. • Large systems acquisitions are (to the maximum extent practical) divided into a series of smaller, incremental acquisition efforts, and investment decisions on these smaller efforts are made on the basis of reliable analyses of estimated costs, expected benefits, and anticipated risks.
Evaluation To ensure that evidence showing that the contract products satisfy the defined requirements are provided prior to accepting contractor products.	• Evaluation requirements are developed in conjunction with the contractual requirements and are maintained over the life of the acquisition. • Evaluations are planned and conducted throughout the total acquisition period to provide an integrated approach that satisfies evaluation requirements and takes advantage of all evaluation results. • Evaluations provide an objective basis to support the product acceptance decision. • The acquiring organization has a written policy for managing the evaluation of the acquired products. • Responsibility for evaluation activities is designated.
Project management To ensure that the project office and its supporting organizations function efficiently and effectively.	• Project management activities are planned, organized, controlled, and communicated. • The performance, cost, and schedule of the acquisition are continually measured, compared with planned objectives, and controlled. • Problems discovered during the acquisition are managed and controlled. • The acquisition organization has a written policy for project management. • Responsibility for project management is designated.
Requirements development and management To ensure that contractual requirements are clearly defined and understood by the acquisition stakeholders.	• Contractual requirements are developed, managed, and maintained. • The end user and other affected groups have input into the contractual requirements over the life of the acquisition. • Contractual requirements are traceable and verifiable. • The contractual requirements baseline is established prior to release of the solicitation package. • The acquisition organization has a written policy for establishing and managing the contractual requirements. • Responsibility for requirements development and management is designated. • Requirements that are mandatory versus optional are clearly delineated and used in deciding what requirements can be eliminated or postponed to meet other project goals, such as cost and schedule constraints.

Best practices	Activity
Risk management To ensure that risks are proactively identified and systematically mitigated.	• Projectwide participation in the identification and mitigation of risks is encouraged. • The defined acquisition process provides for the identification, analysis, and mitigation of risks. • Milestone reviews include the status of identified risks. • The acquisition organization has a written policy for managing acquisition risk. • Responsibility for acquisition risk management activities is designated.
Solicitation To ensure that a quality solicitation is produced and a best-qualified contractor is selected.	• The solicitation package includes the contractual requirements and the proposal evaluation criteria. • The technical and management elements of proposals are evaluated to ensure that the requirements of the contract will be satisfied. • The selection official selects a supplier who is qualified to satisfy the contract's requirements. • The acquiring organization has a written policy for conducting the solicitation. • Responsibility for the solicitation is designated. • A selection official has been designated to be responsible for the selection process and decision. • The acquiring team includes contracting specialists to support contract administration.
Transition to support To ensure proper transfer of the system from the acquiring organization to the support organization.	• The acquiring organization ensures that the support organization has the capacity and capability to provide the required support. • There is no loss in continuity of support to the products during transition from the supplier to the support organization. • Configuration management of the products is maintained throughout the transition. • The acquiring organization has a written policy for transitioning the products to the support organization. • The acquiring organization ensures that the support organization is involved in planning for transition to support. • Responsibility for transition to support activities is designated.
Complementary best practices relevant to commercial component-based business systems acquisitions	
Component modification To ensure that commercial product modification is effectively controlled.	• Modification of commercial components is discouraged and allowed only if justified by a thorough analysis of life cycle costs and benefits.
Configuration management To ensure the integrity and consistency of system commercial components.	• Project plans explicitly provide for evaluation, acquisition, and implementation of new, often frequent, product releases. • Modification or upgrades to deployed versions of system components are centrally controlled and unilateral user release changes are precluded.
Dependency analysis To ensure that relationships among commercial products are understood before acquisition decisions are made.	• Decisions about acquisition of commercial components are based on deliberate and thorough research, analysis, and evaluation of the components' interdependencies.
Legacy systems integration planning To ensure reasonable planning for integration of commercial products with existing systems.	• Project plans explicitly provide for the necessary time and resources for integrating commercial components with legacy systems.

Best practices	Activity
Organization change management To ensure that the organizational impact of using new system functionality is proactively managed.	• Project plans explicitly provide for preparing users for the impact that the business processes embedded in the commercial components will have on users respective roles and responsibilities. • The introduction and adoption of changes to how users will be expected to execute their jobs is actively managed.
Solicitation To ensure that a quality solicitation is produced and a best-qualified contractor is selected.	• Systems integration contractors are explicitly evaluated on their ability to implement commercial components.
Tradeoff analysis To ensure that system requirements alone do not drive the system's solution.	• Investment decisions throughout a system's life cycle are based on tradeoffs among the availability of commercial products (current and future), the architectural environment in which the system is to operate (current and future), defined system requirements, and acquisition cost/schedule constraints.
Vendor and product research and evaluation To ensure that vendor and product characteristics are understood before acquisition decisions are made.	• Commercial component and vendor options are researched, evaluated/tested, and understood, both early and continuously. • A set of evaluation criteria for selecting among commercial component options is established that includes both defined system requirements and vendor/commercial product characteristics (e.g., customer satisfaction with company and product line).

Sources: See sources listed in appendix I of this report.

FBI Is Establishing Institutional IT Management Controls, but Success of IT Programs Depends on Implementation of Controls

The FBI has recognized the importance of IT to transformation, making it one of the bureau's top ten priorities. Consistent with this, the FBI's strategic plan contains explicit IT-related strategic goals, objectives, and initiatives (near-term and long-term) to support the collection, analysis, processing, and dissemination of information. This recognition is important because, as we previously reported,[8] the bureau's longstanding approach to managing IT has not always been fully consistent with leading practices. The effects of this can be seen in, for example, the failure of projects such as VCF. To address these issues, the FBI has, as we reported in 2004, centralized IT responsibility and authority under the CIO and the CIO has taken steps to define and implement management capabilities in the areas of enterprise architecture, IT investment management, systems development and acquisition, and IT human capital.

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

Since 2004, the FBI has continued to make progress in establishing key IT management capabilities. As we previously reported,[9] the FBI has created a life cycle management directive that governs all phases and aspects of the bureau's IT projects, including Sentinel. The directive includes guidance, planned reviews, and control gates for each project milestone, including planning, acquisition, development, testing, and operational management of implemented systems.

However, we have also reported that the challenge now for the FBI is to build on these foundational capabilities and implement them effectively on the program and project investments it has under way and planned, including Sentinel. More specifically, we stated 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 understand and control Sentinel requirements in the context of (1) its enterprise architecture, (2) the capabilities and interoperability of commercially available products, and (3) the bureau's human capital and financial resource constraints, and to prepare users for the impact of the new system on how they do their jobs. We concluded that not taking these steps will introduce program risks that could lead to problems similar to those that contributed to the failure of the VCF.

In this regard, we recently reported on Sentinel's implementation of IT human capital best practices.[10] We determined that the FBI had moved quickly to staff the Sentinel program office, had created a staffing plan that defined program positions needed for the program, and had filled most of them, primarily with contract staff. However, we also determined that the Sentinel staffing plan addressed only the program office's immediate staffing needs. It did not provide for the kind of strategic human capital management focus that is essential to success. Exacerbating this situation was that the FBI was not proactively managing Sentinel human capital availability as a program risk. We concluded that, unless the FBI adopted a more strategic approach to managing human capital for the Sentinel

[9]GAO, *Information Technology, FBI Is Building Management Capabilities Essential to Successful System Deployments, but Challenges Remain*, GAO-05-1014T (Washington, D.C.: September 2006).

[10]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.: October 2006).

program and treated human capital as a program risk, the chances of delivering required intelligence and investigative support capabilities in a timely and cost-effective manner were reduced. Accordingly, we recommended that the FBI adopt such an approach, and the FBI agreed with our recommendations. According to the FBI's CIO, Sentinel human capital management improvements are being accomplished as part of ongoing Office of the CIO's human capital management initiatives, which are being pursued in close coordination with ongoing FBI-wide human capital management improvements.

FBI Is Largely Following Several Best Practices in Managing Key Aspects of Sentinel

The FBI is managing various aspects of Sentinel in accordance with a number of key system acquisition best practices because the FBI CIO and Sentinel program manager have made doing so an area of focus, which reduces Sentinel acquisition risks. At the same time, however, acquisition risks are being increased because support contractors that are performing program management functions are not subject to metrics-based, performance standards. Without such standards, the FBI cannot adequately ensure that support contractors are performing important program management functions effectively and efficiently.

Important Steps in Soliciting Sentinel Contractor Proposals and Awarding the Prime Contract Were Conducted

The FBI took a number of important steps when soliciting offers from contractors to lead the development of Sentinel and in evaluating the offers and making a contract award decision.[11]

We and others[12] have reported on contract solicitation and award best practices used to solicit commercial, component-based IT systems. These practices provide for establishing an organizational framework to conduct a solicitation, including things such as establishing a solicitation policy, defining roles and responsibilities, hiring a qualified solicitation team (including designating responsibility for the selection of a vendor and including contract specialists on the solicitation team). These practices also include guidance on how to evaluate proposals, including things such

[11]We did not determine whether the FBI had complied with the Federal Acquisition Regulation or other contracting or ordering requirements in soliciting and evaluating proposals and in issuing the task order.

[12]See GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 2004) and SEI's Software Acquisition Capability Maturity Model.

as: (1) explicitly evaluating systems integration contractors on their ability to implement commercial IT components; (2) specifying the contractual requirements and the proposal's evaluation criteria in the solicitation package; (3) evaluating the technical and management elements of proposals on the basis of how they satisfy the requirements of the contract; and (4) selecting a contractor that is qualified to satisfy the contract's requirements.

The FBI followed all of these best practices for Sentinel. For instance, the FBI developed a policy for conducting the solicitation—the Sentinel Source Selection Plan—that addressed, among other things, the qualifications for members of the source selection organization. The source selection plan also identified the individual ultimately responsible for conducting the solicitation and making the award decision.

With regard to evaluating proposals, the Sentinel solicitation package contained the contractual requirements and evaluation criteria the bureau would use. Those criteria were designed to explicitly evaluate vendors on their ability to integrate commercial IT products and components like those to be used in Sentinel. In addition, FBI evaluated vendor proposals based on both the technical and management elements of their respective proposals, including elements like past performance, proposed technical approach, proposed management approach, plans for mitigating organizational conflict of interest, proposed security approach, and demonstrated prior success in meeting schedule requirements, controlling costs, and program planning. In addition, the FBI used a GWAC, in which vendors' technical competence had already been already established, thus helping to ensure that the FBI's selected vendor was qualified. For a summary of the FBI's implementation of these best practices, see table 2.

Table 2: FBI's Implementation of Contract Solicitation and Award Best Practices for Sentinel

Contract solicitation and award best practices	Implemented for Sentinel?
The solicitation package includes the contractual requirements and the proposal evaluation criteria.	yes
The technical and management elements of proposals are evaluated to ensure that the requirements of the contract will be satisfied.	yes
The selection official selects a supplier qualified to satisfy the contract's requirements.	yes
The acquiring organization has a written policy for conducting the solicitation.	yes

Contract solicitation and award best practices	Implemented for Sentinel?
Responsibility for the solicitation is designated.	yes
A selection official has been designated to be responsible for the selections process and decision.	yes
The acquiring team includes contracting specialists to support contract administration.	yes
Systems integration contractors are explicitly evaluated on their ability to implement commercial components.	yes

Source: GAO analysis of FBI data.

An Effective Risk Management Process Has Been Defined and Is Being Followed for Sentinel

The FBI has established and is following effective processes for proactively identifying and mitigating program risks before they have a chance to become actual cost, schedule, or performance problems.

We and others view risk management as a core acquisition management practice. In brief, risk management is a process for identifying potential acquisition problems and taking appropriate steps to avoid them. It includes identifying risks and categorizing them based on estimated impact, developing and executing risk mitigation strategies, and reporting on progress in doing so. Risk management practices include, among other things: (1) encouraging project-wide participation in the identification and mitigation of risks; (2) defining and implementing a process for the identification, analysis, and mitigation of acquisition risks; (3) examining the status of identified risks in program milestone reviews; (4) establishing a written policy for managing acquisition risk; and (5) designating responsibility for acquisition risk management activities.

FBI's approach for managing Sentinel's risks employs best practices. (See table 3.) For instance, the Sentinel Risk Management Plan encourages all project team members to identify and mitigate risks, and program officials told us that an e-mail notification system has been implemented in which team members use an e-mail template to forward perceived or newly identified risks to program management. Furthermore, the Risk Management Plan and the prime contractor's Risk and Opportunity Management Plan establish mechanisms for analyzing and mitigating identified risks. Under these plans, risk review boards (1) solicit input on risks from employees, (2) approve specified risk mitigation plans for these risks and assign the risks to their respective risk registers, and (3) periodically review each risk within the register to monitor the implementation of the mitigation plans. Further, these plans (as well as the bureau's Life Cycle Management Directive) call for program control gate

and milestone reviews that include the status of identified risks, which our analysis of gate and milestone documentation shows includes consideration of risks. This is important because it gives FBI management the opportunity to be apprised of the risks facing the program and what program staff is doing to prevent these risks from occurring when milestone decisions are made.

Table 3: FBI's Implementation of Risk Management Best Practices for Sentinel

Risk management best practices	Implemented for Sentinel?
Projectwide participation in the identification and mitigation of risks is encouraged.	yes
The defined acquisition process provides for the identification, analysis, and mitigation of risks.	yes
Milestone reviews include the status of identified risks.	yes
The acquisition organization has a written policy for managing acquisition risk.	yes
Responsibility for acquisition risk management activities is designated.	yes

Source: GAO analysis of FBI data.

FBI Is Beginning to Address Organizational Change and Impacts of Sentinel

The FBI is beginning to plan for and position itself for the human capital and business process changes that are embedded in the commercial off-the-shelf (COTS) software products that are to be used for Sentinel. Given that the first phase of Sentinel involves minimal new COTS software products and later phases are to be heavily COTS-based, the timing of this planning and positioning is appropriate.

As we have previously reported, acquiring software-intensive systems that leverage commercial components involves acquisition management best practices beyond those associated with custom, one-of-a-kind software development efforts. One category of best practices related to COTS acquisitions is proactively planning for and positioning the organization for the people and process changes that will occur as a result of adopting the functionality embedded in commercial products. In short, such change occurs because COTS products are created based on a set of requirements that will have marketability to a broad customer base, rather than to a single customer, which in this case is the FBI. While such products are configurable to align with the customer's architectural needs, such as business rules and date standards, the standard core functionality in the products will require the implementing organization to adopt the product's

embedded business processes, which in turn will require changes to the roles and responsibilities of the organization's workforce and the policies and procedures that they follow.

To ensure that the organizational impact of implementing a COTS-based system is effectively managed, best practices advocate that (1) project plans explicitly provide for preparing users for the impact that the business processes embedded in the commercial components will have on their roles and responsibilities and (2) the organization actively manages the introduction and adoption of changes to how users will be expected to execute their jobs.

As noted earlier, Phase I of Sentinel does not involve extensive use of COTS. Rather, Phase I largely involves development of a customized Web-based portal to the FBI's legacy case management system. Thus, the need for the FBI to have already planned for and be positioned to introduce significant Sentinel-induced organizational change is not expected to be as critical as in later phases. According to the Sentinel program manager, the impact on users in Phase 1 will be minimal due to the small scope of changes that users will need to deal with. Phase 2, in comparison, will introduce changes to individual users' roles, responsibilities, and business practices resulting from re-engineered business processes and a range of COTS-based system capabilities. This means that most of the organizational change management activities for Sentinel are planned for such later phases.

Recognizing the relevance of organizational change management to post-Phase 1 efforts, the FBI has taken steps consistent with both of these previously-cited best practices. (See table 4.) With respect to planning, the Sentinel Program Management Plan identifies the need to work closely with users to ensure that they understand Sentinel capabilities, and the Sentinel Communication Plan outlines a strategy to assist FBI personnel in understanding the purpose and scope of Sentinel and its implications. Among other things, this plan provides for tracking user acceptance, including metrics to continually gauge acceptance and the effectiveness of the strategy. In addition, the Sentinel Training and Strategy Plan provides for analyzing workforce impacts and addressing changes to individuals' roles and responsibilities.

Regarding actively managing the introduction of changes to how individuals execute their jobs, the FBI has set in motion five areas of activity that are embodied in the previously-mentioned plans. These activities are stakeholder management, organizational impact assessment

and understanding, communication, training, and performance support. More specifically, the prime contractor has conducted a Sentinel Stakeholder and Organizational Risk Assessment based in part on visiting several FBI field offices and conducting focus groups with prospective Sentinel users to assess risks to users' acceptance of Sentinel. The results of this analysis have been incorporated into their communication and training plans and are to be addressed through things such as user manuals and program documentation. For instance, the risk and impact analysis showed that on-screen navigation through Sentinel was an area of user concern, so the training plan has treated this as an area of emphasis. According to program officials, such areas of focus are intended to proactively engage and manage stakeholders through the change process, with the ultimate goal of having Sentinel become "business as usual." The challenge that the FBI faces as it proceeds with future Sentinel phases is to ensure that the five areas of activity, particularly the communication and training plans, are effectively implemented.

Table 4: FBI's Implementation of Organizational Change Management Best Practices for Sentinel

Organizational change management best practices	Implemented for Sentinel?
Project plans explicitly provide for preparing users for the impact that the business processes embedded in the commercial components will have on their roles and responsibilities.	yes
The organization actively manages the introduction and adoption of changes to how users will be expected to execute their jobs.	yes

Source: GAO analysis of FBI data.

Sentinel Configuration Management Process Defined and Largely Implemented

The FBI has put in place controls and tools for systematically identifying Sentinel's component parts (software, hardware, and documentation) and controlling the configuration of these parts in a way that reasonably ensures the integrity of each and it has effectively implemented most of those controls. However, FBI has not fully implemented one of the key practices. As a result, it is unclear whether the support contractor that is responsible for this practice is in fact executing it in an effective and efficient manner.

Configuration management is an essential ingredient in successful IT systems programs such as Sentinel. The purpose of configuration management is to maintain integrity and traceability and to control modifications or changes to program assets like technology products and

program documentation throughout their life cycles. Effective configuration management, among other things, enables integration and alignment among related program assets. As we have previously reported,[13] an effective configuration management program comprises four primary elements, each of which should be described in a configuration management plan and implemented according to the plan.

The four elements of an effective configuration management program are:

- **Configuration identification:** Identifying, documenting, and assigning unique identifiers (e.g., serial number and name) to program assets, generally referred to as configuration items.

- **Configuration control:** Evaluating and deciding whether to approve changes to a product's baseline configuration, generally accomplished through configuration control boards, which evaluate proposed changes on the basis of costs, benefits, and risks, and decide whether to permit a change.

- **Configuration status accounting:** Documenting and reporting on the status of configuration items as a product evolves. Documentation, such as historical change lists, are generated and kept in a library, thereby allowing organizations to be continuously aware of the state of a product's configuration and thus to be in a position to make informed decisions about changing the configuration.

- **Configuration auditing:** Determining alignment between the actual product and the documentation describing it, thereby ensuring that the documentation used to support the configuration control board's decision making is consistent with the actual system products that reflect these decisions. Configuration audits, both functional and physical, are performed when a significant product change is introduced and they help to ensure that only authorized changes are being made.

The FBI developed the Sentinel Configuration Management Plan to govern the assets that both the FBI and prime contractor develop. This plan reflects the bureau's Life Cycle Management Directive and each of the

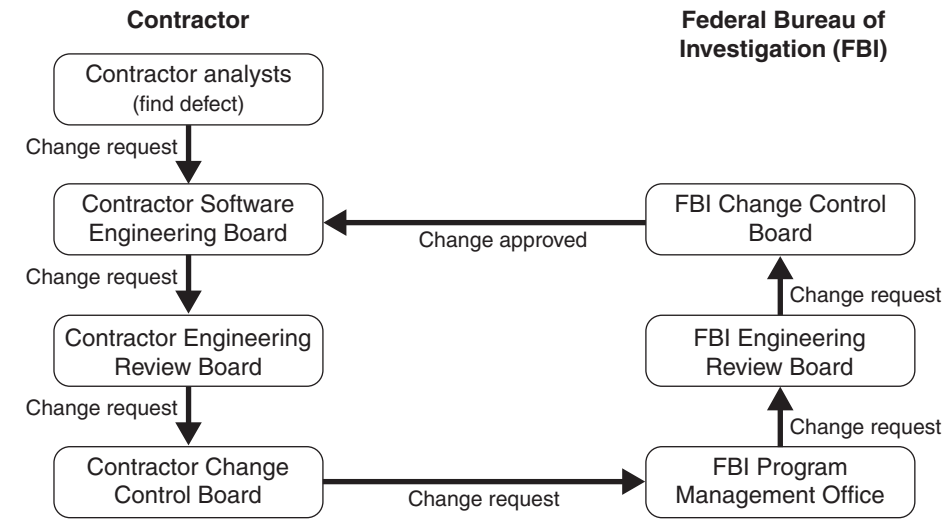
[13]GAO, *DOD Business Systems Modernization: Long-standing Weaknesses in Enterprise Architecture Development Need to Be Addressed*, GAO-05-702 (Washington, D.C.: July 2005).

previously-cited best practices. Moreover, the FBI has largely implemented its plan, as described here and summarized in table 5.

- With respect to configuration identification, the plan defines which classes of program assets are under configuration control and specifies how program staff is to (a) determine the program's configuration items and (b) assign each a unique identifier. In this regard, we observed the naming conventions the program office created for identifying and uniquely naming program assets and then verified that the FBI had inventoried items in accordance with these conventions. In addition, we observed that the FBI had placed under configuration control all of its relevant program documentation, as well as all the data item deliverables from the prime contractor, including multiple software components.

- Regarding configuration control, the FBI's plan calls for, and its prime contractor has implemented, a commercially available software tool to store and manage the program's configuration items, including such things as baselined planning documents and hardware and software assets. Among other things, we observed that the tool features a series of access controls that permit only authorized changes to program assets. For example, the tool did not allow unauthorized changes to configuration items. The FBI and the prime contractor have established configuration control boards, engineering review boards, and software change control boards as specified in the plan to establish a baselined configuration for Sentinel's assets and to authorize changes to them. These boards work together (see fig. 2) to review suggested changes to configuration items on the basis of potential impacts on the rest of the system, including risk, cost, and schedule implications. If these boards approve a change, it is executed by the contractor and recorded in the tool. If a change is rejected by one of the review boards, it is dropped and that decision is also recorded along with the board's rationale.

Figure 2: Configuration Control Process for Sentinel



Source: GAO analysis of contractor and FBI configuration management plans.

- Concerning configuration status accounting, the FBI's plan outlines procedures that are consistent with best practices and FBI's Life Cycle Management Directive. These procedures include keeping historical change lists and producing monthly configuration status accounting reports. However, according to FBI officials, the FBI is not producing regular reports as called for in its plan because the configuration management tool that the FBI is using has the ability to produce the same kinds of reports on demand. Such "real time" reporting satisfies the intent of this best practice.

- With respect to configuration auditing, the FBI's plan calls for audits of the status of program assets. However, the bureau is not following its plans because, according to program officials, the configuration management tool's embedded controls and processes reduce the need for such audits. One such control that we observed includes the automatic recording of who made a change to the software or hardware asset and when the change was made. Nevertheless, the FBI has tasked one of its support contractors with checking the status of configuration items on a daily basis to augment the tool controls. According to the contractor's representative performing this check, the boards' configuration-related decisions are compared with the configuration status reflected in the tool; deviations are to be reported to program management. This approach, according to bureau officials, constitutes "real time" auditing and is better than the periodic audits

cited in the Configuration Management Plan. However, this contractor's activities are not documented or otherwise governed by explicit performance criteria. As a result, the results of configuration audits were not available to assess possible configuration management and security impacts, as provided for in the Sentinel Configuration Management Plan. Thus, we could not verify the FBI's implementation of configuration auditing activities. This lack of performance criteria and measures for support contractors are described further in the next section. FBI officials stated that they intended to perform configuration audits called for in their plan in early June.

Table 5: Sentinel's Implementation of Configuration Management Best Practices

Configuration management best practices	Implemented for Sentinel?
1. Configuration identification	yes
2. Configuration control	yes
3. Configuration status accounting	yes
4. Configuration auditing	partially implemented

Source: GAO analysis of FBI data.

Most Key Tracking and Oversight Activities Being Performed for Sentinel Contractors

The FBI is performing a range of activities to effectively define expectations for its prime contractor and to measure performance against and hold the contractor accountable for meeting these expectations. The bureau is also performing a number of key practices that are relevant to tracking and overseeing the many support contractors that are performing program management functions. However, it is not performing one key practice—establishing and employing product and service performance standards. As a result, the FBI cannot adequately ensure that these support contractors are performing required program management functions effectively and efficiently.

Contract tracking and oversight is the process by which contractual agreements are established and contractor efforts to satisfy those agreements are monitored. This process involves information sharing between the acquirer and contractor to ensure that contractual requirements are understood, that there are measurements to disclose overall project status and problems, and that there are appropriate incentives for ensuring that cost and schedule commitments are met and that quality products are delivered. Contract tracking and oversight begins with the award of a contract and ends at the conclusion of the contract's period of performance.

Contract tracking and oversight best practices include ensuring that (1) the acquiring organization has sufficient insight into the contractor's activities to manage and control the contractor and ensure that the contract's requirements are met; (2) the acquiring organization and contractor maintain ongoing communication and both parties implement agreed-to commitments; (3) all contract changes are managed throughout the life of the contract; (4) the acquisition organization has a written policy for contract tracking and oversight; (5) responsibility for contract tracking and oversight activities is designated; (6) the acquiring organization involves contracting specialists in the execution of the contract; (7) a quantitative set of software and system metrics is used to define and measure product quality and contractor performance; and (8) incentives for meeting cost and schedule estimates and measurable, metric-based product quality incentives are explicitly cited in the contract.

The FBI has taken a number of actions to satisfy these best practices with respect to the Sentinel prime contractor; however, the bureau has not done the same in tracking and overseeing the many support contractors that are performing program management functions. Three examples of best practices implemented in relation to the prime contractor are described here. (See app. III for information on the implementation of all eight practices.)

- To ensure sufficient insight into the contractor's activities, the bureau has instituted integrated product teams for Sentinel, whereby members of the program management office work side by side with the prime contractor. As a result, the Sentinel program office has had daily insight into the direction of the contractor's work, thereby giving the FBI management regular opportunities to manage and control the contractor's activities. Moreover, the FBI requires that the prime contractor provide a monthly report detailing the contractor's activities during the previous month, as well as its anticipated activities for the next month, to permit further insight into the contractor's activities. In addition, the bureau has also established weekly meetings with its contractors to review accomplishments, ongoing issues, and program risks.

- Concerning managing changes to the contract throughout its lifetime, the program office has implemented a change control process consisting of several review boards to manage changes to program assets. According to program officials, board decisions that significantly change requirements (e.g., deliverables) are handled through contract letters. These letters serve as an official record of the

FBI's direction to the contractor, including changes to deliverables called for in the statement of work.

- Regarding having a written policy for contract tracking and oversight, the FBI's Life Cycle Management Directive established the bureau's policy for tracking and overseeing contractors on all IT programs, including Sentinel. In addition, the Sentinel Program Management Plan provides additional procedures, including conducting reviews such as the Requirements Clarification review, the Design Concept Review, and the Preliminary Design Review. Further, the Sentinel statement of work contains requirements for the contractor's earned value management system, earned value baseline, and the contractor's monthly earned value status reports.

With respect to support contractor tracking and oversight, the bureau is at least partially satisfying all but one of these relevant best practices. (See app. III for information on implementation of all eight practices.) However, it has not, for example, established and applied measurable performance standards in its support contractors' statements of work. Specifically, while these statements of work identify specific tasks to be accomplished and assign responsibility for overseeing their execution, they do not cite associated quality and timeliness standards for contract deliverables or other such performance measures. As noted earlier, for example, the activities performed by the configuration management support contractor (see prior section) are not governed by written procedures and are not subject to explicit performance standards. Program officials stated that they manage support contractors daily through face-to-face interaction, and that all work products provided by support contractors are reviewed and approved by government supervisors.[14] Thus, they added, explicit performance standards are not needed. Given the bureau's reliance on support contractors, however, maximizing their performance is important to Sentinel's overall success. By not ensuring that statements of work spell out measures governing product and service quality and timeliness, the FBI cannot adequately ensure that these contractors are performing important program management functions effectively and efficiently.

[14]We did not assess whether these arrangements amount to personal services contracts for which statutory authority is required. A personal services contract is characterized by the employer-employee relationship it creates between the government and the contractor's personnel. See Federal Acquisition Regulation 37.104.

Table 6: Sentinel's Implementation of Contract Tracking and Oversight Best Practices

Best practices for contract tracking and oversight	Implemented for prime contractor?	Implemented for support contractors?
The acquiring organization has sufficient insight into the contractor's activities to manage and control the contractor and ensure contract requirements are met.	yes	yes
The acquiring organization and contractor maintain ongoing communication; commitments are agreed to and implemented by both parties.	yes	yes
All contract changes are managed throughout the life of the contract.	yes	not applicable[a]
Responsibility for contract tracking and oversight activities is designated.	yes	yes
The acquisition organization has a written policy for contract tracking and oversight.	yes	yes
The acquiring organization involves contracting specialists in the execution of the contract.	yes	yes
A quantitative set of software and system metrics is used to define and measure product quality and contractor performance.	yes	no
In addition to incentives for meeting cost and schedule estimates, measurable, metrics-based product quality incentives are cited in contract.	yes	not applicable[b]

Source: GAO analysis of FBI data.

[a]FBI officials stated that program support contractor staff is largely acquired through existing government contracts that are managed outside of the FBI. As a result, changes to these contracts are beyond the control and authority of the FBI.

[b]According to program officials, none of the support contracts allow for incentives.

FBI Policies and Procedures Governing Sentinel Schedule and Cost Estimates Do Not Reflect Important Best Practices

The FBI's policies and procedures that form the basis for Sentinel's schedule and cost estimates are not fully consistent with reliable estimating practices. While the FBI has issued an IT program management handbook, related guidance, and tools that define how IT program schedules and costs are to be estimated, this handbook and related material do not, for example, address having a historical database of program schedule and cost estimates to inform future estimates. In addition, this handbook and related material do not adequately address such schedule estimating practices as providing float time between key activities and reserve time for high risk activities, and they do not adequately address such cost estimating best practices as documentation of source information. The cost estimates that the FBI has developed for

Sentinel reflect these limitations in policies, procedures, and tools. In particular, the estimates to date did not include all relevant costs and could not be verified by supporting documentation. Without well-defined policies, procedures, and supporting tools for estimating IT programs' schedules and costs, the reliability of these programs' respective estimates is questionable and, in the case of Sentinel, a key basis of informed investment management is missing.

FBI Policies and Procedures for Estimating Program Schedules Address Some, but Not All, Best Practices

The success of any program depends in part on having a reliable schedule of when the program's set of work activities will occur, how long they will take, and how they are related to one another. As such, the schedule not only provides a road map for systematic execution of a program, but also provides the means by which to gauge progress, identify and address potential problems, and promote accountability. Among other things, best practices and related federal guidance call for a program schedule to be program-wide in scope, meaning that it should include the integrated breakdown of the work to be performed by both the government and its contractors over the expected life of the program. Best practices also call for the schedule to expressly identify and define the relationships and dependencies among work elements and the constraints affecting the start and completion of work elements. A well-defined schedule helps to identify the amount of human capital and fiscal resources that are needed to execute the program, and thus is an important contribution to a reliable cost estimate.

Our research has identified a range of best practices associated with effective schedule estimating.[15] These practices include

- *Capturing key activities:* The schedule should reflect all key activities (steps, events, outcomes, etc.) as defined in the program's work breakdown structure, to include activities to be performed by both the government and its contractors.

- *Sequencing key activities:* The schedule should line up key activities in the order that they are to be carried out. In particular, activities that must finish prior to the start of other activities (i.e., predecessor activities) as well as activities that cannot begin until other activities are completed (i.e., successor activities) should be identified. By doing

[15]GAO, *Cost Assessment Guide: "Best Practices for Estimating and Managing Program Costs,"* 2007 exposure draft.

so, dependencies among activities that collectively lead to the accomplishment of events or milestones can be established and used as a basis for guiding work and measuring progress.

- *Establishing the duration of key activities:* The schedule should reflect how long each activity will take to execute. In determining the duration of each activity, the same rationale, data, and assumptions used for cost estimating should be used for schedule estimating. Further, these durations should be as short as possible and they should have specific start and end dates. Excessively long periods needed to execute an activity should prompt further decomposition of the activity so that shorter execution durations will result.

- *Assigning resources to key activities:* The schedule should reflect who will do the work activities, whether all required resources will be available when they are needed, and whether any funding or time constraints exist.

- *Establishing the critical path for key activities:* The schedule should identify the longest duration path through the sequenced list of key activities, which is known as the schedule's critical path. If any activity slips along this path, the entire program will be delayed. Therefore, potential problems that might occur along or near the critical path should be identified and reflected in the scheduling of the time for high risk activities (see next).

- *Identifying "float time" between key activities:* The schedule should identify the time that a predecessor activity can slip before the delay affects successor activities, which is known as "float time" and is an indicator of schedule flexibility. As a general rule, activities along the critical path typically have the least amount of float time.

- *Distributing reserves to high risk activities:* The baseline schedule should include a buffer or a reserve of extra time. Typically, the schedule reserve is calculated by taking the difference in time between the planned completion date and the contractual completion date for either the program as a whole or for a part of the program. As a general rule, the reserve should be applied to high risk activities, which are typically found along the critical path.

- *Integrating key activities horizontally and vertically:* The schedule should be horizontally integrated, meaning that it should link the products and outcomes associated with already sequenced activities (see previous section). These links are commonly referred to as "hand

offs" and serve to verify that activities are arranged in the right order to achieve aggregated products or outcomes. The schedule should also be vertically integrated, meaning that traceability exists among varying levels of activities and supporting tasks and sub-tasks. Such mapping or alignment among levels enables different groups to work to the same master schedule.

The FBI's policies and procedures that govern IT program schedule estimating are defined in the bureau's IT Program Management Handbook and its IT Investment Management Process. To the bureau's credit, these documents reflect several of the previously cited best practices for schedule estimating. For example, the handbook requires program managers to define and sequence the key activities required to complete a given project, to determine the durations of each activity, and to identify the resources needed to complete tasks. Further, the handbook calls for the identification of the project's critical path and "float time." However, the handbook and associated worksheets do not specifically call for the distribution of schedule reserve to high risk activities or for the integration of tasks horizontally and vertically. Moreover, FBI policies and procedures only partially provide for assigning resources to key activities because the FBI's guidance does not address consideration of whether funding or time constraints exist. (See table 7 for a summary of the extent to which FBI policies and procedures address each of the best practices.)

FBI Office of the CIO officials agreed that these best practices are not addressed in current bureau policies for estimating schedules and that they need to be. Until they are, schedule estimates for FBI IT programs, like Sentinel, will be of questionable reliability, and thus the risk of Sentinel's actual performance not tracking closely to plans is increased.

The delays that the FBI has recently experienced on Phase I of Sentinel illustrate how this risk may have been realized. Specifically, the original milestone for completing deployment of Sentinel Phase I to all headquarters and field offices was May 2007. However, according to bureau officials, this milestone slipped to June 2007. According to program officials, the delay is due to a number of factors, including early miscommunication with the prime contractor on when work on the program was to begin, a number of changes within the prime contractor's staff, and problems integrating commercial products that were not discovered until system acceptance testing. However, the limitations in the FBI's policies and procedures that are the basis for the Sentinel schedule could have led to development of a Phase I schedule that was not sufficiently reliable, and thus was a contributor to this schedule slip.

Table 7: FBI's Implementation of Best Practices for Schedule Estimation

Schedule estimation best practices	Implemented for Sentinel?
Capture of key activities	yes
Sequencing of key activities	yes
Duration of key activities	yes
Resources for key activities	partially
Identification of critical path	yes
Identification of "float time" between key activities	yes
Distribution of reserve to high risk activities	no
Horizontal and vertical integration within key activities	no

Source: GAO analysis of FBI data.

FBI Policies and Procedures for Estimating Program's Costs Address Some, but Not All, Best Practices

A reliable cost estimate is critical to the success of any IT program. Such an estimate provides the basis for informed investment decision making, realistic budget formulation and program resourcing, meaningful progress measurement, proactive course correction when warranted, and accountability for results. According to OMB,[16] programs must maintain current and well-documented estimates of program costs, and these estimates must encompass the full life cycle of the program. Among other things, OMB states that generating reliable program cost estimates is a critical function necessary to support OMB's capital programming process. Without this capability, agencies are at risk of experiencing program cost overruns, missed deadlines, and performance shortfalls.

Our research has identified a number of best practices that are the basis of effective program cost estimating. We have grouped these practices into four characteristics of a high-quality and reliable cost estimate.[17] They are

- *Comprehensive:* The cost estimates should include both government and contractor costs of the program over its full life cycle, from

[16]Office of Management and Budget, *Circular No. A-11, Preparation, Submission, and Execution of the Budget* (Washington, D.C.: Executive Office of the President, June 2006); *Circular No. A-130 Revised, Management of Federal Information Resources* (Washington, D.C.: Executive Office of the President, Nov. 28, 2000); and *Capital Programming Guide: Supplement to Circular A-11, Part 7, Preparation, Submission, and Execution of the Budget* (Washington, D.C.: Executive Office of the President, June 2006).

[17]GAO, *Cost Assessment Guide: "Best Practices for Estimating and Managing Program Costs,"* 2007 exposure draft.

inception of the program through design, development, deployment, and operation and maintenance to retirement of the program. They should also provide a level of detail appropriate to ensure that cost elements are neither omitted nor double counted, and they should document all cost-influencing ground rules and assumptions.

- *Well-documented:* The cost estimates should capture in writing such things as the source data used and their significance, the calculations performed and their results, and the rationale for choosing a particular estimating method or reference. Moreover, this information should be captured in such a way that the data used to derive the estimate can be traced back to, and verified against their sources.

- *Accurate:* The cost estimates should provide for results that are unbiased, and they should not be overly conservative or optimistic (i.e., should represent most likely costs). In addition, the estimates should be updated regularly to reflect material changes in the program, and steps should be taken to minimize mathematical mistakes and their significance. Among other things, the estimate should be grounded in documented assumptions and a historical record of cost and schedule estimating and actual experiences on other comparable programs.

- *Credible:* The cost estimates should discuss any limitations in the analysis performed due to uncertainty or biases surrounding data or assumptions, and their derivation should provide for varying major assumptions and recalculating outcomes based on sensitivity analyses, and the associated risk and uncertainty inherent in estimates should be disclosed. Further, the estimates should be verified based on cross-checks using other methods and by comparing the results with independent cost estimates.

The FBI's policies and procedures that govern estimating program costs are defined in the bureau's IT Program Management Handbook, Cost-Benefit Analysis Guide, and IT Investment Management Process. To the bureau's credit, these documents reflect some of the previously cited best practices. For example, the handbook calls for cost estimates to be comprehensive and to be life cycle in scope, including total costs (e.g., research, development, production, training, operations and maintenance, software licensing, and labor) over its full life cycle (from initiation to system retirement). Moreover, FBI guidance partially provides for documenting these estimates and ensuring their accuracy by, for example, stating that estimating assumptions should be documented and that the estimates are to be updated on a regular basis.

However, these policies and procedures do not reflect all of the cost estimating best practices associated with well-documented, accurate, and credible estimates. With respect to being well-documented, they do not require that the sources of historical data used in the estimate be documented and, with respect to accuracy, they do not provide for the establishment and use of a historical database of estimating and actual experiences on comparable programs. Without documenting estimated data sources, the basis for the estimates, including the circumstances surrounding the data used to derive and whether these data have been properly normalized, cannot be understood. This means that the reliability of the estimate for either current use in managing a program or for inclusion in a historical database for use in future program estimates, cannot be assured. Further, without provision for establishing and using a historical database, one will not be available to inform future estimates, as is the case for the FBI. With respect to credibility, the FBI's policies and procedures do not address the need to consider and reflect any limitations in the analyses on which the estimates are based, or to document any uncertainty or biases surrounding the data used. As a result, the associated uncertainty in the estimate itself cannot be determined, thus limiting the estimate's integrity and utility. Further, the FBI's policies and procedures do not provide for the conduct of risk/sensitivity analyses[18] and disclosure of the associated risk and uncertainty of the estimates. Thus, estimates will not include important information to inform program decision making, such as the range of potential costs surrounding the point estimate and the reasons behind this range.

FBI Office of the CIO officials agreed that these practices are not included in the bureau's policies and procedures that form the basis for IT program cost estimates and that they need to be. Until an effective basis for cost estimating is in place and employed, FBI IT programs, like Sentinel, will likely not have reliable cost estimates to properly inform investment decision making and the risk of actual program cost performance not tracking closely to estimates will be increased.

[18]A risk/uncertainty analysis quantifies the risk inherent in a cost estimate by using probability distributions and ranges of cost to assess the aggregate variability in the point estimate. The result is a set of estimated probabilities of achieving alternative outcomes given the uncertainty in the underlying parameters.

Table 8: Summary of FBI Policies' and Procedures' Reflection of Best Practices Characteristics for Cost Estimating

Cost estimation best practice characteristics	Addressed in policies and procedures?
Comprehensive	yes
Well documented	partial
Accurate	partial
Credible	no

Source: GAO analysis of FBI data.

Our analysis of Sentinel cost estimates[19] revealed reliability issues. In particular, none of the estimates are comprehensive in that they each omit relevant costs. For example, one estimate does not include government or support contractor costs and, according to program officials, another estimate does not include technology refresh, certain government labor costs, or inflationary costs. In addition, these estimates cannot be considered fully accurate or well documented. For example, according to program officials, none of the estimates was derived using a historical database reflecting actual and estimated costs on similar programs. Further, none of the estimates had a fully documented estimating methodology, although some parts of one cost estimate were documented. Also, none of the estimates could be traced to the source of the data that were used in developing them. These reliability concerns with the Sentinel cost estimates are due in part to the FBI's not following its own cost estimating policies and procedures and in part to the previously

[19]The FBI has developed three different types of Sentinel cost estimates. The first estimate was developed in April 2005 and is referred to as the Independent Government Cost Estimate (IGCE). In short, an IGCE is performed to check the reasonableness of contractors' cost proposals and to make sure that the proposals offered are within a feasible budget range so that funds will be available to execute the program. An IGCE is submitted by the program manager as part of a request for contract funding. It provides the government's assessment of the program's most probable cost. The second estimate, which is referred to as the Government Estimate of Most Probable Cost (GEMPC), was prepared in March 2006, and is actually an independent assessment of what the contractor estimates it will cost to execute the terms of the contract. The GEMPC determines the realism of the contractor's estimate, including identifying potential areas of risk that require further negotiation between the government and the contractor. The third estimate is what is presented in the OMB 300 budget exhibit, which is intended to be an estimate of a program's cost over its life cycle. This estimate includes annual funding requirements for future budget years.

mentioned limitations in the FBI's cost estimating policies, procedures, and supporting tools. As a result, the Sentinel cost estimates do not provide a sufficient basis for informed investment decision making and do not facilitate meaningful tracking of progress against estimates, both of which are fundamental to effectively managing an IT program.

Conclusions

The success of large-scale IT programs, such as Sentinel, is to a large part determined by the extent to which they are executed according to rigorous and disciplined system acquisition management best practices. While implementing such practices does not guarantee program success, doing so will minimize the program's exposure to risk and thus the extent to which the program falls short of expectations. In the case of Sentinel, living up to expectations is critical because not only are the capabilities that Sentinel is to provide mission critical, they are long overdue and thus time is of the essence.

To the FBI's credit, it has implemented a number of best practices for Sentinel and by doing so has placed itself on a path to both avoid the kind of missteps that led to the failure of VCF and increase the chances of putting needed mission capabilities in the hands of bureau agents and analysts as soon as possible. Nevertheless, the FBI is still not where it needs to be in managing its program office support contracts and in having reliable estimates of Sentinel schedules and costs to manage and disclose progress and to inform bureau, Department of Justice, and congressional investment decision making. As a result, there is a risk that contractor-provided program management support will not be performed effectively and efficiently. Given that Sentinel's program office relies extensively on such contractor support to execute its many program management functions, less than high quality support contractor performance could adversely affect Sentinel's success. Risks also exist relative to having a reliable basis for informed decisions about Sentinel's investment options because bureau policies, procedures, and tools that form the basis for Sentinel schedule and cost estimates do not reflect important best practices. Moreover, the cost estimates that the FBI has developed to date for Sentinel reflect these limitations. This means that bureau and Justice leadership and Congress lack reasonable assurance that they have a reliable cost basis on which to decide among competing investment options and measure Sentinel's progress.

Both effective support contractor tracking and oversight and reliable schedule and cost estimating are critical management functions that should be implemented for programs like Sentinel according to

organizational policies and procedures that are grounded in relevant best practices. The FBI's current policies and procedures in this area do not address several key best practices, and hence the bureau has not implemented such practices for Sentinel. It is important that the FBI correct this void in its policies and procedures and that all its IT programs implement these practices.

Recommendations

To strengthen the FBI's management of its Sentinel program, we are recommending that the FBI Director instruct the bureau's CIO to

- work with Sentinel support contractors, where feasible, to establish and implement performance standards in statements of work relative to the quality and timeliness of products and the performance of services and
- revise the IT handbook and related guidance to address schedule and cost estimating best practices that are identified in this report as not being addressed in FBI policies and procedures and ensure that these best practices are fully employed on all major IT programs, including Sentinel.

Agency Comments and Our Evaluation

In written comments on a draft of this report signed by the FBI CIO and reprinted in appendix IV, the bureau stated that it agreed with our recommendation to revise and implement its guidance for IT program schedule and cost estimation. The FBI CIO stated that the bureau plans to do so by September 30, 2007.

However, the FBI disagreed with our recommendation to establish and implement metrics-based performance standards for its Sentinel program office support contractors, stating that the program office already provides sufficient oversight of these contractors. To support this position, the FBI commented that Sentinel's staffing plan contains support contractor position descriptions that include identifying the skills required to execute each position's functions. Further, it commented that all support contractor's products are reviewed and approved by government supervisors, and that the support contractors submit reports on accomplishments that are used by the FBI in reviewing and approving invoices. While we do not take issue with any of these comments, we also do not believe that these actions fully address our recommendation. As a result, we disagree with the bureau's position. Specifically, our point is not whether the functions that support contractors perform, or the skills

needed to perform them, are identified or whether support contractors' work is reviewed before invoice payment is approved; rather, our point is that standards governing the quality and timeliness of the functions and work performed are not defined; this lack of standards, in turn, increases the chances of support contractors producing products or providing services that fall short of expectations and thus do not support effective and efficient program management. As we state in our report, this is particularly important for the Sentinel program because the bureau is relying extensively on support contractors to augment its own program management staff.

The FBI also provided technical comments, which we have incorporated throughout the report as appropriate.

We are sending copies of this report to the Chairman and Vice Chairman of the Senate Select Committee on Intelligence and the 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; the Chairman and Ranking Member of the House Committee on Appropriations, Subcommittee on Science; the departments of State, Justice, and Commerce, 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 V.

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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the FBI's (1) use of effective practices for acquiring Sentinel and (2) basis for reliably estimating Sentinel's schedule and costs.

To address the first objective, we focused on five key areas associated with acquiring commercial component-based IT systems, as agreed with our requestors: solicitation,[1] risk management, organizational change management, configuration management, and contract tracking and oversight. We researched relevant best practices, including published guidance from the Software Engineering Institute (SEI) and GAO-issued reports associated with each of these five areas. We also obtained and reviewed relevant FBI policies, procedures, guidance, and Sentinel program documentation (see below), and interviewed pertinent Sentinel program and Office of the CIO officials as well as prime contractor (Lockheed Martin) and support contractor representatives where 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. We then compared this body of evidence to best practices and related guidance that we researched, identified variances, and discussed the reasons for and impact of any variances with FBI officials.

The key, governing FBI documents that we obtained and reviewed relative to each of the five areas included (1) FBI Information Technology Life Cycle Management Directive version 3.0; (2) Project Management Handbook, version 1; and (3) Sentinel Program Management Plan, version 1.2. In addition, we obtained and reviewed the following documents that were specific to each of the five areas:

- For solicitation, these documents include: (1) the Sentinel Source Selection Plan; (2) the Sentinel Source Selection Decision document; and (3) the Sentinel Source Selection Evaluation Team Final Report.

- For risk management, these documents include: (1) the Sentinel Risk Management Plan; (2) the Sentinel Risk Register; and (3) the Lockheed Martin Risk and Opportunity Management Plan for Sentinel.[2]

[1]We did not determine whether the FBI complied with the Federal Acquisition Regulation or other contracting or ordering requirements in soliciting and evaluating proposals and in issuing the task order.

[2]We did not verify whether the individuals assigned responsibility for a given risk had actually executed the risk mitigation strategy.

- For organizational change management, these documents include: (1) the Sentinel Workforce Transformation Strategy and Plan; (2) the Sentinel Stakeholder and Organizational Risk Assessment; (3) the Sentinel Organizational Impact Assessment; (4) the Sentinel Communications Plan; and (5) the Sentinel Training Strategy and Plan.

- For configuration management, these documents include: (1) the Sentinel Configuration Management Plan; and (2) the Lockheed Martin Configuration Management Plan for Sentinel.

- For contract tracking and oversight these documents include (1) the statements of work for Sentinel support contractors; (2) the Sentinel Measurement Plan; (3) selected Sentinel Measurement reports; (4) the Sentinel Statement of Work; and (5) select monthly EVM reports.[3]

To address our second objective, we used GAO's draft guide on estimating program schedules and costs, which is based on extensive research of best practices, and federal schedule and cost estimating guidance found in the OMB Capital Programming Guide. In addition, we obtained and reviewed FBI policies and procedures governing schedule and cost estimating, including the FBI Program Management Handbook, FBI Information Technology Life Cycle Management Directive, and the FBI Information Technology Management Guide. We then compared the bureau's policies and procedures to the practices in GAO's guide and to federal guidance, identified variances, and discussed reasons for variances with officials from the Office of the CIO. We also interviewed program officials, and/or obtained and reviewed Sentinel cost estimates relative to the analysis, data, and calculations supporting each estimate.

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 September 2005 and May 2007 in accordance with generally accepted government auditing standards.

[3]We did not examine specific contractor invoices or the controls surrounding review and approval of invoices because these financial management activities are being addressed as part of an ongoing GAO review.

Appendix II: Key IT System Acquisition Best Practices

We and others have identified and promoted the use of a number of best practices associated with acquiring IT systems. In 2004, we reported[1] on 18 relevant best practices and grouped them into two categories: (1) ten practices for acquiring any type of business system and (2) eight complementary practices that relate specifically to acquiring commercial component-based business systems. Each is described here.

Best Practices Relevant to Any IT Business Systems Acquisition

1. Acquisition Planning

Purpose: To ensure that reasonable planning for all parts of the acquisition is conducted.

Description: Acquisition planning is the process for conducting and documenting acquisition planning activities beginning early and covering all parts of the project. This planning extends to all acquisition areas, such as budgeting, scheduling, resource estimating, risk identification, and requirements definition as well as the overall acquisition strategy.

Acquisition planning begins with the earliest identification of a requirement that is to be satisfied through an acquisition.

Activities: (1) Plans are prepared during acquisition planning and maintained throughout the acquisition. (2) Planning addresses the entire acquisition process, including life cycle support of the products being acquired. (3) The acquisition organization has a written policy for planning the acquisition. (4) Responsibility for acquisition planning activities is designated.

2. Architectural Alignment

Purpose: To ensure that the acquisition is consistent with the organization's enterprise architecture.

Description: Architectural alignment is the process for analyzing and verifying that the proposed architecture of the system being acquired is

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

consistent with the enterprise architecture for the organization acquiring the system. Such alignment is needed to ensure that acquired systems can interoperate and are not unnecessarily duplicative of one another. Exceptions to this alignment requirement are permitted, but only when justified and only when granted an explicit waiver from the architecture. A particular architectural consideration is whether requirements that extend beyond the specific system being acquired should be considered when selecting system components. Such "product line" (i.e., systems that are developed from a common set of assets and share a common and managed set of features) considerations can provide substantial production economies over acquiring systems from scratch.

Activities: (1) The system being acquired is assessed for alignment with the enterprise architecture at key life cycle decision points and any deviations from the architecture are explicitly understood and justified by an explicit waiver to the architecture. (2) Product line requirements—rather than just the requirements for the system being acquired—are an explicit consideration in each acquisition.

3. Contract Tracking and Oversight

Purpose: To ensure that contract activities are performed in accordance with contractual requirements.

Description: Contract tracking and oversight is the process by which contractual agreements are established and contractor efforts to satisfy those agreements are monitored. It involves information sharing between the acquirer and contractor to ensure that contractual requirements are understood, that there are regular measurements to disclose overall project status and whether problems exist, and that there are appropriate incentives for ensuring that cost and schedule commitments are met and that quality products are delivered. Contract tracking and oversight begins with the award of the contract and ends at the conclusion of the contract's period of performance.

Activities: (1) The acquiring organization has sufficient insight into the contractor's activities to manage and control the contractor and ensure that contract requirements are met. (2) The acquiring organization and contractor maintain ongoing communication; commitments are agreed to and implemented by both parties. (3) All contract changes are managed throughout the life of the contract. (4) The acquiring organization has a written policy for contract tracking and oversight. (5) Responsibility for contract tracking and oversight activities is designated. (6) The acquiring organization involves contracting specialists in the execution of the contract. (7) A quantitative set of software and system metrics is used to

define and measure product quality and contractor performance.[2] (8) In addition to incentives for meeting cost and schedule estimates, measurable, metrics-based product quality incentives are explicitly cited in the contract.

4. Economic Justification

Purpose: To ensure that system investments have an adequate economic justification.

Description: Economic justification is the process for ensuring that acquisition decisions are based on reliable analyses of the proposed investment's likely costs versus benefits over its useful life as well as an analysis of the risks associated with actually realizing the acquisition's forecasted benefits for its estimated costs. Moreover, it entails minimizing the risk and uncertainty of large acquisitions that require spending large sums of money over many years by breaking the acquisition into smaller, incremental acquisitions. Economic justification is not a one-time event, but rather is performed throughout an acquisition's life cycle in order to permit informed investment decision making.

Activities: (1) System investment decisions are made on the basis of reliable analyses of estimated system life cycle costs, expected benefits, and anticipated risks. (2) Large systems acquisitions are (to the maximum extent practical) divided into a series of smaller, incremental acquisition efforts, and investment decisions on these smaller efforts are made on the basis of reliable analyses of estimated costs, expected benefits, and anticipated risks.

5. Evaluation

Purpose: To ensure that evidence showing that the contract products satisfy the defined requirements are provided prior to accepting contractor products.

Description: Evaluation is the process by which contract deliverables are analyzed to determine whether they meet contract requirements. It includes developing criteria such as product acceptance criteria to be included into both the solicitation package and the contract. It should be conducted continuously throughout the contract period as products are

[2]Richard J. Adams, Suellen Eslinger, Karen L. Owens, and Mary A. Rich, *Reducing Risk in the Acquisition of Software-Intensive Systems: Best Practices from the Space System Domain* (Los Angeles, Calif: 2003).

delivered. It begins with development of the products' requirements and ends when the acquisition is completed.

Activities: (1) Evaluation requirements are developed in conjunction with the contractual requirements and are maintained over the life of the acquisition. (2) Evaluations are planned and conducted throughout the total acquisition period to provide an integrated approach that satisfies evaluation requirements and takes advantage of all evaluation results. (3) Evaluations provide an objective basis to support the product acceptance decision. (4) The acquisition organization has a written policy for managing the evaluation of the acquired products. (5) Responsibility for evaluation activities is designated.

6. Project Management

Purpose: To ensure that the project office and its supporting organizations function efficiently and effectively.

Description: Project management is the process for planning, organizing, staffing, directing, and managing all project-office-related activities, such as defining project tasks, estimating and securing resources, scheduling activities and tasks, training, and accepting products. Project management begins when the project office is formed and ends when the acquisition is completed.

Activities: (1) Project management activities are planned, organized, controlled, and communicated. (2) The performance, cost, and schedule of the acquisition are continually measured, compared with planned objectives, and controlled. (3) Problems discovered during the acquisition are managed and controlled. (4) The acquisition organization has a written policy for project management. (5) Responsibility for project management is designated.

7. Requirements Development and Management

Purpose: To ensure that contractual requirements are clearly defined and understood by the acquisition stakeholders.

Description: Requirements development is the process for developing and documenting contractual requirements, including evaluating opportunities for reusing existing assets. It involves participation from end users to ensure that product requirements are well understood, and that optional versus mandatory requirements are clearly delineated. Requirements management is the process for establishing and maintaining agreement on the contractual requirements among the various stakeholders and for ensuring that the requirements are traceable, verifiable, and controlled. This involves base lining the requirements and controlling subsequent

requirements changes. Requirements development and management begins when the solicitation's requirements are documented and ends when system responsibility is transferred to the support organization.

Activities: (1) Contractual requirements are developed, managed, and maintained. (2) The end user and other affected groups have input into the contractual requirements over the life of the acquisition. (3) Contractual requirements are traceable and verifiable. (4) The contractual requirements baseline is established prior to release of the solicitation package. (5) The acquisition organization has a written policy for establishing and managing the contractual requirements. (6) Responsibility for requirements development and management is designated. (7) Requirements that are mandatory versus optional are clearly delineated and used in deciding what requirements can be eliminated or postponed to meet other project goals, such as cost and schedule constraints.

8. Risk Management

Purpose: To ensure that risks are identified and systematically mitigated.

Description: Risk management is the process for identifying potential acquisition problems and taking appropriate steps to avoid their becoming actual problems. It includes risk identification and categorization based on estimated impact, development of risk mitigation strategies, and execution of and reporting on the strategies. Risk management occurs early and continuously in the acquisition life cycle.

Activities: (1) Project wide participation in the identification and mitigation of risks is encouraged. (2) The defined acquisition process provides for the identification, analysis, and mitigation of risks. (3) Milestone reviews include the status of identified risks. (4) The acquisition organization has a written policy for managing acquisition risk. (5) Responsibility for acquisition risk management activities is designated.

9. Solicitation

Purpose: To ensure that a quality solicitation is produced, and a best qualified contractor selected.

Description: Solicitation is the process for developing, documenting, and issuing the solicitation package; developing and implementing a plan to evaluate responses; conducting contract negotiations; and awarding the contract. Solicitation ends with contract award.

Activities: (1) The solicitation package includes the contractual requirements and the proposal evaluation criteria. (2) The technical and

	management elements of proposals are evaluated to ensure that the requirements of the contract will be satisfied. (3) The selection official selects a supplier who is qualified to satisfy the contract's requirements. (4) The acquiring organization has a written policy for conducting the solicitation. (5) Responsibility for the solicitation is designated. (6) A selection official has been designated to be responsible for the selection process and decision. (7) The acquiring team includes contracting specialists to support contract administration.
10. Transition to Support	*Purpose:* To ensure proper transfer of the system from the acquisition organization to the eventual support organization. *Description:* Transition to support is the process for developing and implementing the plans for transitioning products to the support organization. This includes engaging relevant stakeholders in the acquisition and sharing information about the system's supporting infrastructure. Transition to support begins with requirements development and ends when the responsibility for the products is turned over to the support organization. *Activities:* (1) The acquiring organization ensures that the support organization has the capacity and capability to provide the required support. (2) There is no loss in continuity of support to the products during transition from the supplier to the support organization. (3) Configuration management of the products is maintained throughout the transition. (4) The acquiring organization has a written policy for transitioning products to the support organization. (5) The acquiring organization ensures that the support organization is involved in planning for transition to support. (6) Responsibility for transition to support activities is designated.

Complementary Best Practices Relevant to Commercial Component-Based IT Business Systems Acquisitions

1. Component Modification	*Purpose:* To ensure that commercial product modification is effectively controlled.

Description: Component modification is the process for limiting the chances of a commercial product being modified to the point that it becomes a one-of-a-kind solution because doing so can result in extensive life cycle costs. Such modifications, if not incorporated into the commercially available version of the product by the supplier, mean that every product release has to be modified in accordance with the custom changes, thus precluding realization of some of the benefit of using a commercial product.

Activity: (1) Modification of commercial components is discouraged and allowed only if justified by a thorough analysis of life cycle costs and benefits.

2. Configuration Management

Purpose: To ensure the integrity and consistency of commercial system components.

Description: Configuration management relative to commercial component-based systems is the process for ensuring that changes to the commercial components of a system are strictly controlled. It recognizes that when using commercial components, it is the vendor, not the acquisition or support organization, that controls the release of new component versions and that new versions are released frequently. Thus, acquisition management needs to provide for both receiving new product releases and controlling the implementation of these releases.

Activities: (1) Project plans explicitly provide for evaluation, acquisition, and implementation of new, often frequent, product releases. (2) Modification or upgrades to deployed versions of system components are centrally controlled and unilateral user release changes are precluded.

3. Dependency Analysis

Purpose: To ensure that relationships between commercial products are understood before acquisition decisions are made.

Description: Dependency analysis relative to commercial component-based systems is the process for determining and understanding the characteristics of these products so that inherent dependencies among them can be considered before they are acquired. It involves recognizing that the logical and physical relationships among products impact one another. This is necessary because commercial products are built around each vendor's functional and architectural assumptions and paradigms, such as approaches to error handling and data access, and these assumptions and paradigms are likely to be different among products from different sources. Such differences complicate product integration.

Further, some commercial products have built-in dependencies with other products that, if not known, can further complicate integration.

Activity: (1) Decisions about the acquisition of commercial components are based on deliberate and thorough research, analysis, and evaluation of the components' interdependencies.

4. Legacy Systems Integration Planning

Purpose: To ensure reasonable planning for integration of commercial products with existing systems.

Description: Legacy systems integration planning is the process for ensuring that the time and resources needed to integrate existing systems with the system being acquired are identified and provided for. It involves identifying which legacy systems will interact with the system being acquired and what kinds and levels of testing are required. Integration planning recognizes that, although some commercial products may provide mechanisms and information that are helpful in integration with legacy systems, the unavailability of the source code for commercial products and the different organizations that are responsible for the two will likely require additional time and effort.

Activity: (1) Project plans explicitly provide for the time and resources necessary for integrating commercial components with legacy systems.

5. Organization Change Management

Purpose: To ensure that the organizational impact of using new system functionality is proactively managed.

Description: Organization change management relative to commercial component-based systems is the process for preparing system users for the business process changes that will accompany implementation of the system. It involves engaging users and communicating the nature of anticipated changes to system users through training on how jobs will change. This is necessary because commercial products are created with the developers' expectations of how they will be used, and the products' functionality may require the organization implementing the system to change existing business processes.

Activities: (1) Project plans explicitly provide for preparing users on the impact that the business processes embedded in the commercial components will have on the user's respective roles and responsibilities. (2) The introduction and adoption of changes to how users will be expected to execute their jobs are actively managed.

6. Solicitation	*Purpose:* To ensure that a quality solicitation is produced and a best qualified contractor is selected. *Description:* Solicitation relative to commercial component-based systems is the process for ensuring that a capable contractor is selected. It involves ensuring that the selected contractor has experience with integrating commercial component products. This is important because expertise in developing custom system solutions is different from expertise in implementing commercial components; it requires different core competencies and experiences to be successful. *Activity:* (1) Systems integration contractors are explicitly evaluated on their ability to implement commercial components.
7. Tradeoff Analysis	*Purpose:* To ensure that system requirements alone do not drive the system solution. *Description:* Tradeoff analysis relative to commercial product-based systems is the process for analyzing and understanding the tradeoffs among competing acquisition variables so as to produce informed acquisition decision making. It involves planning and executing acquisitions in a manner that recognizes four competing interests: defined system requirements, the architectural environment (current and future) in which the system needs to operate, acquisition cost and schedule constraints, and the availability of products in the commercial marketplace (current and future). This analysis should be performed early and continuously throughout an acquisition's life cycle. *Activity*: (1) Investment decisions throughout a system's life cycle are based on tradeoffs among the availability of commercial products (current and future), the architectural environment in which the system is to operate (current and future), defined system requirements, and acquisition cost/schedule constraints.
8. Vendor and Product Research and Evaluation	*Purpose:* To ensure that vendor and product characteristics are understood before acquisition decisions are made. *Description:* Vendor and product research and evaluation relative to commercial component-based systems is the process for obtaining reliable information about both the product being considered and the vendor offering the product. It involves taking additional steps beyond vendor representations, such as obtaining information about the vendor's history, obtaining information on the vendor's business strategy relative to

evolution and support of the product, and evaluating copies of the product in a test environment.

Activities: (1) Commercial component and vendor options are researched, evaluated/tested, and understood, both early and continuously. (2) A set of evaluation criteria for selecting among commercial component options is established that includes both defined system requirements and vendor/commercial product characteristics (e.g., customer satisfaction with company and product line).

Appendix III: Sentinel Implementation of Contract Tracking and Oversight Best Practices

Table 9 contains our assessment of the FBI's efforts for contract tracking and oversight for both the prime contractor and the sub-contractors.

Table 9: Sentinel Implementation of Contract Tracking and Oversight Best Practices on Prime Contract

Best practice for contract tracking and oversight	Implemented for Sentinel?	Evidence
The acquiring organization has sufficient insight into the contractor's activities to be able to manage and control the contractor and ensure that contract requirements are met.	yes	FBI ensured sufficient insight into the contractor's activities through such mechanisms as integrated product teams (in which the program office works side by side with contractor staff), weekly meetings with contractor staff, monthly contractor invoice reports, and earned value management. These mechanisms provide the FBI with the means for controlling the contractor's activities and ensuring that requirements are met.
The acquiring organization and contractor maintain ongoing communication and commitments are agreed to and implemented by both parties.	yes	The FBI maintains ongoing communications with the contractor through the above mentioned IPTs, weekly meetings, and periodic reports to ensure that commitments are implemented. Additionally, commitments are agreed to via contract letters. These letters record changes to deliverables or otherwise redirect work defined in the statements of work.
All contract changes are managed throughout the life of the contract.	yes	The FBI has implemented a change control process consisting of several boards that review proposed changes to the program and decide whether to implement the change. According to the FBI, significant changes to any contract deliverables are handled through the previously mentioned contract letters.
Responsibility for contract tracking and oversight activities is designated.	yes	The Sentinel Program Management Plan designates responsibility for contract tracking and oversight. Specifically, this plan designates the Sentinel Contracting Officer (CO) and a Contracting Officer's Technical Representative (COTR) as responsible for ensuring continuing alignment between the set of contracts/task orders being used by the Sentinel program and the program's needs. Both of these contracting officials report to the Sentinel Program Manager, who is ultimately responsible for all areas of program execution, including contract tracking and oversight.
The acquisition organization has a written policy for contract tracking and oversight.	yes	The Sentinel Program Management Plan contains the FBI's policy for contract tracking and oversight. This plan reflects the contract tracking and oversight policies and procedures defined in the FBI's IT Life Cycle Management Directive.
The acquiring organization involves contracting specialists in the execution of the contract.	yes	Both the Sentinel CO and COTR are contracting specialists. In addition, the bureau has hired support contractors to provide contract management expertise.

Best practice for contract tracking and oversight	Implemented for Sentinel?	Evidence
A quantitative set of software and system metrics is used to define and measure product quality and contractor performance.	yes	The Sentinel Measurement Plan defines quantifiable metrics for product quality and provides for contractor reporting on satisfaction of these metrics. Further, the contractor provides monthly reports detailing its performance and laying out expectations for the coming month.
In addition to incentives for meeting cost and schedule estimates, measurable, metrics-based product quality incentives are explicitly cited in the contract.	yes	The FBI created an award fee plan for the contractor that provides metrics-based product quality incentives in addition to cost and schedule incentives.

Source: GAO analysis of FBI data.

Table 10: Sentinel Implementation of Contract Tracking and Oversight Best Practices for Support Contractors

Criteria	Implemented for Sentinel?	Evidence
The acquiring organization has sufficient insight into the contractor's activities to be able to manage and control the contractor and ensure that contract requirements are met.	yes	Support contractor staff is co-located in the program office with FBI program officials, and according to FBI officials, they interact with them and direct their work on a daily basis. Additionally, program officials told us that they also interact with support contractor staff at a weekly status meeting to review deliverables and performance and otherwise ensure that contract requirements are met.
The acquiring organization and contractor maintain ongoing communication and commitments are agreed to and implemented by both parties.	yes	Program officials told us that they maintain ongoing communication with the support contractor's staff through IPTs, day-to-day contact, and during weekly meetings. According to these officials, during these interactions, commitments are agreed to and their implementation is ensured.
All contract changes are managed throughout the life of the contract.	not applicable	Program support contractor staff is largely acquired through existing government contracts that are managed outside of the FBI. As a result, changes to these contracts are beyond the control and authority of the FBI.
Responsibility for contract tracking and oversight activities is designated.	yes	The Sentinel Program Management Plan designates responsibility for contract tracking and oversight. According to the plan, the designated CO and COTR are responsible for contract tracking and oversight.
The acquisition organization has a written policy for contract tracking and oversight.	yes	The Sentinel Program Management Plan specifies the FBI's policy for contract tracking and oversight. This plan reflects the policies and procedures in the FBI's IT Life Cycle Management Directive.
The acquiring organization involves contracting specialists in the execution of the contract.	yes	Both the Sentinel CO and COTR are contracting specialists. In addition, the bureau has hired support contractors to provide contract management expertise.

Criteria	Implemented for Sentinel?	Evidence
A quantitative set of software and system metrics is used to define and measure product quality and contractor performance.	no	The statements of work for the Sentinel support contractors do not establish metrics that define and measure contractor performance relative to, for example, product quality and timeliness and service effectiveness and efficiency.
In addition to incentives for meeting cost and schedule estimates, measurable, metrics-based product quality incentives are explicitly cited in the contract.	not applicable	According to program officials, none of the contracts with support contractors are award fee contracts. Thus, the contract structures do not allow for incentives.

Source: GAO analysis of FBI data.

Appendix IV: Comments from the Federal Bureau of Investigations

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 18, 2007

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

Dear Mr. Hite:

Re: FBI RESPONSE TO GAO'S DRAFT REPORT,
"INFORMATION TECHNOLOGY, FBI FOLLOWING A
NUMBER OF KEY ACQUISITION PRACTICES ON NEW CASE
MANAGEMENT SYSTEM BUT IMPROVEMENTS STILL NEEDED,"
GAO-07-912

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled "Information Security, FBI Following a Number of Key Acquisition Practices on New Case Management System but Improvements Still Needed" (hereafter referred to as "the Report"). The Report has been reviewed by the Federal Bureau of Investigation (FBI), Office of the Chief Information Officer (OCIO). This letter constitutes the formal FBI response.

Based on our review of the Report, the FBI concurs with the GAO's technical recommendation pertaining to the revision of the Information Technology (IT) Handbook and related guidance to address schedule and cost estimating best practices. The Program Management Handbook, referred to as the IT Handbook by the GAO, will be updated in conjunction with Life Cycle Management Directive (LCMD) Version 4, with a targeted publication of late 4th Quarter, Fiscal Year 2007. LCMD Version 4 will address the best practices as related to schedule and costing and will be provided to all offices at the FBI, including SENTINEL.

The FBI does not concur with the GAO's comments that the FBI should establish and implement performance standards in statements of work for SENTINEL support contractors relative to the quality and timeliness of products and the performance of services. The SENTINEL Program Management Office (PMO) support

Mr. Randolph C. Hite

contractors have defined position descriptions and skills required to perform the functions defined in the staffing plan. The majority of the management team's work is task oriented, suspense driven, and requires written products. All products provided by the support contractors, such as minutes, white papers, and comments, are reviewed and approved by government supervisors. Additionally, support contractors submit reports on work accomplishments to their respective contractor Team Lead who then provides a monthly report to the Business Management Unit. This report, along with the invoice that reflects the number of hours billed per contractor, is provided to Unit/Team Leads for their review and concurrence. Therefore, the government leadership has the opportunity to concur/comment on work performed/hours expended by each support contractor. Hence, the FBI believes the PMO provides sufficient government oversight of its support contractors.

Again, thank you for the opportunity to respond to the Report. Should you or your staff have questions regarding our response, please feel free to contact me or one of my executives listed below:

Mr. Dean E. Hall
Deputy Chief Information Officer
Office of the Chief Information Officer
202-324-2307

Mr. John Martin Hope
Program Management Executive
Office of IT Program Management
202-324-9798

Sincerely yours,

Zalmai Azmi
Chief Information Officer

2

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to those named above, Monica Anatalio, Tonia Brown, Carol Cha, Neil Doherty, Jennifer Echard, Nancy Glover, Daniel Gordon, Jim MacAuley, Paula Moore (Assistant Director), Karen Richey, Teresa Tucker, Kevin Walsh, and Jeffrey Woodward made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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