THE FEDERAL BUREAU OF INVESTIGATION'S PRE-ACQUISITION PLANNING FOR AND CONTROLS OVER THE SENTINEL CASE MANAGEMENT SYSTEM

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 06-14
March 2006

THE FEDERAL BUREAU OF INVESTIGATION'S PRE-ACQUISITION PLANNING FOR AND CONTROLS OVER THE SENTINEL CASE MANAGEMENT SYSTEM

EXECUTIVE SUMMARY

In March 2005, the Federal Bureau of Investigation (FBI) terminated a 3-year, $170 million effort to develop a modern case management system called the Virtual Case File (VCF) and announced a new project called Sentinel. As detailed in the Office of the Inspector General's (OIG) February 2005 audit report on the FBI's larger Trilogy Information Technology Modernization Project, the VCF project failed for a variety of reasons, including poorly defined design requirements, lack of mature Information Technology Investment Management (ITIM) processes, and poor management continuity and oversight.[1]

With Sentinel, the FBI is relying on improved management processes, use of commercially available components, and a four-phase approach over 39 to 48 months to develop a replacement for its obsolete Automated Case Support (ACS) system. As of February 2006, the FBI had not disclosed its specific cost estimates for Sentinel because the contract to a private information technology (IT) systems developer had not yet been awarded. However, in response to congressional inquiries, the FBI has cited a cost between $400-$500 million to develop the system. According to the FBI, a more precise cost estimate will be available once the FBI awards the Sentinel contract in calendar year 2006.

The OIG performed this audit of the Sentinel project at the request of the FBI Director and congressional appropriations committees. This audit is the first in a series of audits that the OIG intends to conduct on an ongoing basis to evaluate the development and implementation of Sentinel. The objective of this first audit was to evaluate the FBI's pre-acquisition planning for Sentinel, including the approach, design, cost, funding sources, timeframe, contracting vehicle, and oversight structure. Our future audits will examine the development of the system over its four phases and assess whether cost, schedule, performance, and technical benchmarks are being met.

[1] The Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Audit Report Number 05-7, February 2005.

Background to Sentinel

A major objective of the FBI's IT modernization project is to replace the FBI's antiquated ACS. During a variety of OIG reviews over the past several years, we reported that ACS uses outmoded technology, is cumbersome to operate, and does not provide necessary workflow and information-sharing functions.

The FBI expects that Sentinel will provide it with a web-enabled case management system that includes records management, workflow management, collected item and evidence management, and records search and reporting capabilities, all of which will replace its current paper-based case management system. The FBI intends to implement Sentinel in four phases, with each phase providing distinct capabilities until the overall project is completed in 2009. The FBI expects to complete each of the phases in 12 to 18 months, with the phases overlapping. For example, Phase II will begin about 3 months into Phase I. According to the FBI, the four phases will provide the following capabilities.

- Phase I will provide the web-based Sentinel portal. Initially, the portal will allow access to ACS data and eventually to data in the new case management system. It will also include a case management "workbox" that will summarize a user's workload (the case files an agent or analyst is working on), and provide automatic indexing in case files according to person, place, or thing.

- Phase II will begin the transition to a paperless case records system by providing electronic case document management and a records repository. A workflow tool will support the movement of electronic case files through the review and approval process, while a security framework will provide access controls and electronic signatures.

- Phase III will provide a new Universal Index (UNI), which is a database of people, places, or things that relate to a case. Expanding the number of attributes in the system will enable more precise searching and will enhance agents' ability to "connect the dots" among cases.

- Phase IV will implement Sentinel's new case management and reporting capabilities, including the management of tasks and evidence. During this phase, Sentinel will be connected to

ACS, data on closed cases will be migrated from ACS to Sentinel, and the process to retire ACS will begin.

In reviewing the management processes and controls the FBI has applied to the pre-acquisition phase of Sentinel, we believe that the FBI has adequately planned for the project and this planning provides reasonable assurance that the FBI can successfully complete Sentinel if the processes and controls are implemented as intended. However, we have several concerns about the project that require action and continued monitoring: (1) the incomplete staffing of the PMO, (2) the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, (3) Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (4) the lack of an established Earned Value Management (EVM) process, (5) the FBI's ability to track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's ITIM processes.

New IT Management Processes

In previous reports, we were critical of the FBI's lack of ITIM processes and Enterprise Architecture (the blueprint for its current and future IT environment) in the implementation of Trilogy. We believe that these weaknesses contributed, in large part, to the FBI's past failures in developing IT systems.

In this audit, we found that since the troubled Trilogy project and VCF failure, the FBI has established ITIM processes through its Life Cycle Management Directive (LCMD) and through continued work on fully defining its Enterprise Architecture. The FBI's newly created IT management processes, reviews, and controls, coupled with external oversight by the OIG, contractors, congressional committees, and others, should help the FBI identify and minimize failures to achieve cost, schedule, performance, and technical benchmarks for the Sentinel project.

Life Cycle Management Directive

In November 2004, the FBI established an initial Life Cycle Management Directive, which it has since refined and is applying to the Sentinel project. The LCMD governs all aspects of an IT project, including planning, acquisition, development, testing, and operations and maintenance. The FBI's LCMD contains four overlapping components: life cycle phases, control gates, project level reviews, and key support processes.

Nine life cycle phases require FBI management approvals during the development, implementation, and retirement of IT projects. The approvals occur through seven control gates in which an FBI executive-level review board discusses and approves the project before it proceeds to the next control gate. The control reviews, in turn, are based on the results of project-level reviews described below.

As of December 2005, the FBI's Investment Management Project Review Board (IMPRB) had approved the Sentinel project through two control gates covering three of the nine life cycle phases: concept exploration, requirements development, and acquisition planning. These three phases covered the following planning aspects of Sentinel.

- Concept exploration identified the mission need, evaluated solutions, and developed a business plan.

- Requirements development defined the operational, technical, and testing needs.

- Acquisition planning allocated the requirements among the various development stages, researched and applied lessons learned from previous projects, identified potential product and service providers, and determined funding sources.

The remaining life cycle phases will cover source selection where proposals are solicited and evaluated and the vendor is selected; design of the system's components and connectivity; testing of system components and the overall product; implementation and integration of the operational system, including training; operations and maintenance to support the system; and disposal of Sentinel when it reaches the end of its life cycle.

The FBI completed two Sentinel control gates by the conclusion of our field work for this audit report in December 2005. The review board approved the system concept in mid-July 2005 and the acquisition plan in late-July 2005. The latter review approved documentation of the system specifications and interface controls, as well as the project approach and resource estimates. Sentinel will be required to pass through four more control gates — final design review, deployment readiness, system test readiness, and operational acceptance review — and will be reviewed by four other executive-level review boards as the project proceeds.[2] The next control gate, final design review, is led by the Technical Review Board and seeks to ensure that the project design complies with technical requirements and will meet the FBI's needs.

The various executive-level control gate reviews are based in part on the results of more detailed project-level reviews. The LCMD calls for the FBI's Program Management Office to conduct these project reviews. By December 2005, the FBI-wide Program Management Office had conducted two project-level reviews that fed into the two higher-level control gate reviews. The first was a mission-needs review approving Sentinel's mission requirements, and the second was a system specification review approving documents for the system specifications and the external interface controls. The system specification review was the decision point that led to development of Sentinel's acquisition plan, the allocation of the requirements to the four phases of the project, and the development of project plans to carry out the acquisition.

In addition to the project-level reviews, the LCMD contains 23 key support processes that provide additional support to the development of IT projects within the FBI. Rather than being created for specific projects, these processes cover organization-wide management functions, such as strategic planning. As a result, the key support processes affect how individual projects such as Sentinel are managed within the FBI. Key support processes are also performed independently from the life cycle phases, but the deliverables associated with each key process area are integrated into the project-level and control gate reviews where applicable.

In examining the implementation of the LCMD for Sentinel thus far — a vital element in providing internal management oversight and control over the project — we concluded that the FBI's ITIM processes appear to be sound and were generally being followed. We also found that the FBI successfully completed most of the documentation required for the first three phases of the nine-phase life cycle. However, as of December 2005, the FBI had not yet completed the system security plan or the verification and validation plan as required by the LCMD. Nevertheless, Sentinel was approved to proceed past the second control gate without these two plans. The FBI explained that: (1) the system security plan cannot be completed until

[2] The LCMD has a seventh control gate at the end of a system's life cycle to authorize the termination of operations and maintenance and the disposal of system assets.

Sentinel's vendor provides detailed information on the project's design, and (2) a separate contract will be awarded to develop an Independent Verification and Validation (IV&V) plan.

The FBI further explained that the system security plan will provide detail necessary for the completion of certification and accreditation of the applications being created for Sentinel, while the IV&V plan will provide for an independent control to assess the implementation of the system according to technical and performance baselines. We believe the FBI's explanation for deferring these two plans are reasonable, given the timing of the contract for Sentinel. However, in our next audit, we will monitor whether the FBI completes the system security plan and the IV&V plan during the early stages of Sentinel's development.

Risk Management

The purpose of risk management is to assist the program management team in identifying, assessing, categorizing, monitoring, controlling, and mitigating risks before they negatively affect a program. A risk management plan identifies procedures used to manage risk throughout the life of the program.

We found that the FBI has instituted a risk management process for Sentinel. Although Risk Review Board meetings have been held biweekly since the project began, the FBI stated that it plans to hold weekly meetings once the Sentinel contract is awarded. When the Risk Review Board identifies specific risks, they are discussed at monthly Program Management Review sessions and other Sentinel oversight meetings. Risks are categorized by severity and identified as either open or resolved. Open risks are tracked until resolved.

During the initial life cycle phase of Sentinel, the FBI developed a mission-needs statement that assessed five areas for risk mitigation: (1) user acceptance, (2) implementation plan, (3) system capacity and performance, (4) data migration, and (5) infrastructure support. In addition, the Sentinel acquisition plan identified the following seven risks.

- Several parallel IT initiatives within the FBI can affect the scope of Sentinel.

- The Sentinel project award schedule is very aggressive and the target award date may not be attainable.

- Sentinel must interface with numerous FBI legacy systems operated outside the FBI's Office of the Chief Information Officer (CIO).[3]

- The FBI mission may evolve, or Sentinel user requirements may change, resulting in scope creep prior to system completion.

- Initial project costs may be underestimated.

- Staffing resources (prime and subcontractors) that meet FBI requirements may not be available when needed.

- The development contractor may be unable to meet the proposed notional schedule.

Awareness of these risks and a systematic monitoring and resolution of those risks is critical to keeping Sentinel on track.

Project Oversight

In addition to the management controls incorporated into its LCMD, the FBI has established two additional forms of project management and oversight for Sentinel: a Program Management Office or PMO established specifically for Sentinel, and an array of external oversight bodies. The PMO, as the FBI's direct manager of the Sentinel project, is vital to Sentinel's success. Among the many reasons for the failure of the VCF was a fragmented and ill-equipped PMO that suffered from rapid personnel turnover. Simply put, the VCF was poorly managed. A well functioning PMO can reduce the risks that threaten the successful implementation of the Sentinel project.

While the FBI has established a PMO dedicated exclusively to Sentinel, this PMO has not yet been fully staffed. Without a fully staffed, stable, and capable PMO managing the project on a daily basis, Sentinel is at risk. The FBI intends for the PMO to be comprised of systems engineers, technical assistance personnel, and other subject matter experts from the FBI, other government agencies, federally funded research and development centers, and contractors. As of January 30, 2006, the PMO had 51 of the planned full staffing level of 76 employees and contractors on board.

[3] As discussed previously, Sentinel is to be developed using a phased, or incremental, approach whereby functionality will be added in stages.

In response to our concerns about staffing, Sentinel's program manager stated that because of the pre-award spending caps the FBI placed on the program, fully staffing the PMO during the pre-award phase was premature. As a result, the program manager said the FBI is only hiring essential program management oversight personnel during this initial phase to ensure that the PMO is prepared to handle contract award activities. However, in light of the FBI's aggressive development and deployment schedule for Sentinel, it is critical for the FBI to fully staff the PMO office as soon as possible. In our opinion, the significant turnover of project management during the Trilogy project — 15 different key IT managers over the course of its life, including 10 individuals serving as project managers for various aspects of Trilogy — was a major reason for Trilogy's problems. We believe that sufficiently staffing the Sentinel PMO at the outset of the project is key to establishing the stable management staff required to properly oversee the project.

At the time of our audit, the FBI was working to identify qualified candidates to fill the vacant PMO positions, many of whom will be contractor personnel. Another reason for our concern is that security clearances will be required for the staff of the PMO and, according to the FBI, obtaining the clearances may delay personnel coming onboard.

In addition, it is critical for the PMO to have stable leadership. In November 2005 the FBI appointed a seasoned program manager on detail to the FBI from the Central Intelligence Agency to manage the Sentinel project. However, this program manager's current agreement calls for a 2-year detail with an option to extend to a third year. In light of the likelihood of this manager returning to the CIA before Sentinel is completed, the FBI plans to groom a successor for him. We believe that continuity in this position, or a seamless transition to a qualified successor, is critical for the success of the project.

In addition, continuity in the FBI's CIO position is important. During development of Trilogy and the VCF, the FBI had five different CIOs or Acting CIOs. However, in the last several years, the FBI has had continuity in the CIO position. In July 2004, the FBI reorganized its IT resources and established the Office of the CIO to centrally manage all IT responsibilities, activities, policies, and employees across the FBI. The current CIO, who has been in his position since May 2004, now has responsibility for the FBI's overall IT efforts, including developing the FBI's IT strategic plan and operating budget, developing and maintaining the FBI's technology assets, and providing technical direction for the re-engineering of FBI business processes.

External oversight organizations also play an important role in monitoring the Sentinel project and identifying problems that the FBI may not see. These groups include congressional oversight committees, the OIG, and several other outside organizations. To its credit, the FBI has enlisted the assistance of its Science and Technology Board, RAND, the Markle Foundation, and a retired corporate chief technology officer to advise the FBI on areas of information sharing and privacy, IT strategic planning and investments, and management of large IT acquisitions.[4] In addition, the Department of Justice CIO and the Office of Management and Budget are also tracking the progress of Sentinel.

Earned Value Management

The FBI has developed a Sentinel Program Earned Value Management (EVM) Capability Implementation Plan in which the FBI and the Sentinel vendor will be required to apply EVM practices to the project. EVM is a process that coordinates work scope, schedule, and cost goals and objectively measures progress toward those goals. The Sentinel Program Management Office will use the EVM plan to measure Sentinel's performance and the performance of the vendor and will report the results to oversight entities. As of December 2005, the FBI was in the process of acquiring its EVM tool to track and manage Sentinel. Until the tool is acquired, the plan outlines a methodology for the FBI to obtain earned value measures through other applications. When acquired and implemented, the EVM tool should allow program managers to evaluate Sentinel project performance against baselines and identify potential problems with the project. Due to the importance of EVM in helping to detect problems in a project's development, we will continue to monitor the FBI's implementation of this process in our future audit work.

[4] The FBI's Science and Technology Board provides the FBI Director with independent advice on how the FBI can more effectively exploit and apply science and technology to improve its operations. Board members are not involved in specific procurement actions or contracts but instead focus on identifying current and emerging technologies that can maximize how the FBI conducts investigations, collects and disseminates intelligence, and collaborates with law enforcement and intelligence partners.

Capability Maturity Model Integration

The FBI's Statement of Work for the Sentinel project requires that bidders obtain an independent appraisal certifying that their systems development, software engineering, and integration processes are at a Level 3 or higher on the Carnegie-Mellon University's Capability Maturity Model Integration (CMMI) 5-level maturity scale. This requirement covers all vendors and any subcontractors that will contribute a minimum of 10 percent of the total Sentinel effort in developing or integrating software. Sentinel's Statement of Work also gives the FBI the right to interview the lead appraiser who conducts the assessment and obtain independent assessments during the development of the project to verify compliance with the appraised processes.

We believe that by requiring vendors to perform at a CMMI Level 3, the FBI has reduced the risk of selecting vendors that are not capable of completing the Sentinel project and integrating all four project phases. Additionally, because the vendors will be independently reviewed by a CMMI appraiser, the FBI has greater assurance that the processes the vendor will use to develop Sentinel follow best industry practices. In our upcoming audit work, we plan to verify that the CMMI appraisal is conducted, review its results, and assess the appraiser's independence.

Enterprise Architecture

Since 2000, the FBI has struggled to develop an Enterprise Architecture to help manage its current and planned IT infrastructure and applications. The lack of a mature Enterprise Architecture was one of the reasons for the troubled Trilogy project and the failure of the VCF. However, over the past 5 years the FBI has made significant progress in establishing its Enterprise Architecture. In March 2005, the FBI completed an Enterprise Architecture report that provides a high-level snapshot of current FBI business processes and supporting IT structures and systems. The FBI has also defined its desired IT infrastructure environment, or target architecture. In addition, the FBI has completed an interim architecture report describing how Sentinel will enhance the FBI's current IT capabilities. Like most federal agencies the FBI does not yet have a fully mature architecture, but the FBI's architecture now appears to be sufficiently mature to provide the required management structures and processes needed to guide the Sentinel project and ensure its compatibility with the rest of the FBI's IT environment.

Contracting

The process to identify a contractor for the Sentinel project began in late June 2005, with the FBI providing information to potential bidders. In early August 2005, the FBI issued a Request for Proposals (RFP). Initially, responses were due by September 19 and the contract was to be awarded on November 15. However, because of technical questions arising from potential bidders, the FBI extended the response date to September 26 and the award date to December 31. As of February 2006, however, the contract had not been awarded and the FBI had not provided a revised award date. According to the Sentinel program manager, the award date was postponed because initial reviews by the source selection evaluation team identified a need for additional data from the companies that submitted proposals. Once the data is received, the source selection evaluation team will complete the formal review and present its results to the awarding committee. The program manager said an award date cannot be determined until the FBI receives and reviews the additional data.

The Sentinel development contract will be cost-plus-award-fee in which the vendor will be rewarded for meeting established goals in four areas: project management, cost management, schedule, and technical performance. The award fee can not exceed 12 percent of the total development costs for Sentinel and will be allocated across the four areas based on the degree of risk agreed to by the FBI and the vendor at the signing of the contract. This type of contract is common for large government IT projects. In our 2005 report on the FBI's Trilogy project, we stated our concerns with the cost-plus-award-fee contract as it was implemented by the FBI in that project. The cost-plus-award-fee contract used for Trilogy did not: (1) require specific completion milestones, (2) include critical decision review points, and (3) provide for penalties if the milestones were not met. However, the FBI's improved management processes and controls should reduce the risk of such problems recurring for Sentinel because the FBI intends to establish clear milestones, impose penalties for missed milestones, and include critical decision review points.

To identify a prime contractor for Sentinel, the FBI used a contracting vehicle provided through the National Institutes of Health (NIH), one of 16 government-wide acquisition contracts the FBI evaluated before narrowing the field to 5 suitable for a large IT project such as Sentinel. The FBI selected the NIH CIO Solutions Partners 2 *Innovations* contracting vehicle because it had 37 prime contractors and could provide a greater number of potential bidders and a greater opportunity for competition.

The FBI has closely guarded information about potential contractors and costs as procurement sensitive, and has not informed the OIG of the identities of the potential contractors. However, several publications have reported that two major defense contractors have bid on Sentinel.

According to the Sentinel program manager, as of February 2006 the FBI was evaluating the bids based on the following five factors:

- Past performance on programs of similar size, scope, technical complexity, and managerial complexity as Sentinel.

- Technical approach regarding phased development and application of off-the-shelf components.

- Management approach to Sentinel's design, development, integration and testing, deployment, and operations and maintenance.

- Security approach to personnel, infrastructure, and the Sentinel lifecycle.

- Cost, including reasonableness and completeness.

Funding

Because this first OIG audit of Sentinel was focused on the FBI's pre-acquisition planning, and given the procurement sensitive nature of cost information at this stage of the award process, the FBI did not provide us with details regarding the estimated cost of the planned four-phase Sentinel project. However, in response to a Senate Appropriations Committee inquiry in October 2005, the FBI estimated that it would cost the government between $400 and $500 million to develop Sentinel. The FBI stated that the precise cost estimate will not be disclosed until the FBI awards the contract, a decision which as mentioned previously has been postponed to early 2006. In our upcoming audit work, we plan to examine in detail the winning bidder's cost estimates.

The FBI has stated, however, that it plans to fund the first two phases of Sentinel by seeking congressional approval to reprogram FBI funds through two separate requests. According to the FBI's plan, the third and fourth phases would be funded by appropriations.

In accord with this plan, in September 2005 the FBI requested a $97 million reprogramming of fiscal year (FY) 2005 funds for the first phase of Sentinel. Congress approved the reprogramming in mid-November 2005. According to the FBI's submission, more than $14 million of the initial reprogramming will come from the Counterterrorism Division budget, $13 million from intelligence-related activities, and $2 million from the Cyber Division.

We interviewed officials at FBI headquarters to assess the effect of this $97 million reprogramming on FBI operations. Generally, these officials said their divisions and offices can withstand the diversion of funds to Sentinel for the first reprogramming. However, we are concerned that diverting substantial funds from such mission-critical areas could begin eroding the FBI's operational effectiveness, only to be compounded by an anticipated second reprogramming.

Although the FBI divisions and offices seemed confident about their ability to absorb the initial reprogramming of funds to Sentinel, they stated that a second reprogramming of the same magnitude would damage their ability to fulfill their mission. According to the FBI CIO, the FBI intends to send another reprogramming request to Congress to fund the second phase of the Sentinel program in FY 2006.

The OIG plans to assess the operational impact of these reprogrammings in subsequent Sentinel audits to ensure the FBI's critical missions are not adversely affected by the reprogramming of funds to the Sentinel project.

Training

At the time of our audit in February 2006, the FBI had not yet developed a training plan or complete cost estimates for Sentinel training. The FBI's first reprogramming request estimated $1.2 million for training in the first phase, although the FBI recognized that total training costs over the life of the project will be substantially higher. Consequently, we recommend that the FBI develop a comprehensive training plan with more accurate cost estimates as soon as possible so that complete training costs can be included in the overall Sentinel budget.

Cost Tracking

In the Trilogy project, the FBI lacked an effective, reliable system to track and validate the contractors' costs. We highlighted this concern in our February 2005 report on Trilogy and the VCF. Although the FBI stated during the current audit that it was evaluating a tool to track project costs, we recommend that the FBI implement an effective method to track and control costs as soon as possible. We view the potential weaknesses in cost control over the Sentinel project as a significant project risk.

Information Sharing

According to the Sentinel requirements document, the FBI's ability to share information not only internally but also with its law enforcement and intelligence community partners is an important design requirement for Sentinel. In addition, according to the Senior Policy Advisor to the Department of Justice's CIO, through the interagency Federal Investigative Case Management System (FICMS) effort, Sentinel is intended to provide the core elements of a case management system that other law enforcement and intelligence agencies can adapt to meet their unique requirements. While the FBI has considered its internal needs in developing Sentinel's requirements, we are concerned that the FBI has not yet adequately examined or discussed Sentinel's ability to connect with external systems in other Department of Justice components, the Department of Homeland Security (DHS), and other intelligence community agencies. If such connectivity is not built into Sentinel's design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system.

The FBI CIO told us that the FBI invited representatives of the DHS, Drug Enforcement Administration (DEA), and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) to participate in the development of Sentinel's requirements. In addition, the CIO said the FBI has discussed Sentinel interface issues with the Office of Management and Budget (OMB) and the Directorate of National Intelligence (DNI). We interviewed officials from the DHS, DEA, and ATF concerning Sentinel. DHS officials told us that it reviewed the system requirements the FBI had already prepared, but that the DHS did not participate in developing them. DHS officials said that the DHS does not have enough information at this stage of Sentinel's development to assess whether Sentinel and DHS systems will be able to share information or what will be required to achieve compatibility.

According to a DHS official, the DHS hopes to "piggyback" onto Sentinel and use at least parts for its own investigative case management system. In addition, the DHS said it plans to assign IT subject-matter experts to the FBI to assist in advising on and managing Sentinel, but is not certain of the specific role the personnel would play.

The DEA plans to deploy its own new case management system to DEA field offices in early 2006. According to the DEA's Deputy CIO, its new case management system is not compatible with Sentinel as currently designed. To address this incompatibility, DEA officials said they plan to monitor Sentinel's development to identify any modifications in the DEA system needed to achieve compatibility with Sentinel.

The ATF said it had not reviewed the requirements for Sentinel and did not know at this early stage whether it would need to modify its systems to achieve compatibility.

Conclusions

In our judgment, the FBI has taken important steps to address its past mistakes with the VCF in planning for the development of Sentinel. In reviewing the management processes and controls the FBI has applied to the pre-acquisition phase of Sentinel, we believe that the FBI has adequately planned for the project and this planning provides reasonable assurance that the FBI can successfully complete Sentinel if the processes and controls are implemented as intended. However, we have several concerns about the project that we believe require action and continued monitoring by the FBI, the OIG, and other interested parties. These concerns include: (1) the incomplete staffing of the PMO, (2) the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, (3) Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (4) the lack of an established EVM process, (5) the FBI's ability to track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's ITIM processes.

The OIG will continue to monitor and periodically issue audit reports throughout the Sentinel project in an effort to track the FBI's progress and identify any emerging concerns over the cost, schedule, technical, and performance aspects of the project.

OIG Recommendations

In this initial Sentinel audit, we make seven recommendations for the FBI to help ensure the success of the Sentinel case management system. The recommendations are:

- Ensure that the system security and Independent Verification and Validation plans are completed as soon as possible after the contract is signed.
- Ensure that the Sentinel Program Management Office is staffed to a level that will support Sentinel's aggressive delivery schedule.
- Obtain a tool that will allow the effective implementation of an Earned Value Management process and fully implement this process.
- Discuss with other intelligence community and law enforcement agencies their information-sharing requirements to ensure compatibility with those systems in the requirements and design of Sentinel.
- Ensure that an effective system is in place to accurately track and control Sentinel's development costs.
- Complete a comprehensive training plan with realistic schedule and cost estimates and include the training cost estimates in estimates of the overall project's costs.
- Establish a method to monitor the operational impact of a potential second reprogramming and identify any degrading of the FBI's mission-critical functions due to the diversion of funds to the Sentinel project.

TABLE OF CONTENTS

INTRODUCTION

Background

In testimony before the House Appropriations Committee on March 8, 2005, the Director of the Federal Bureau of Investigation (FBI) discussed the FBI's plan to develop and implement a state-of-the-art case management system called Sentinel over 4 phases taking about 42 months. The Sentinel project replaces the FBI's unsuccessful efforts over the previous 3 years to develop an automated case management system called the Virtual Case File (VCF), which was intended to replace its obsolete Automated Case Support (ACS) system. Because of the FBI's failed $170 million VCF project, congressional appropriations and oversight committees questioned whether the FBI could successfully develop and implement a case management system of Sentinel's magnitude.

Because of the importance of the Sentinel project, the congressional appropriations committees and the FBI Director asked the Department of Justice Office of the Inspector General (OIG) to monitor and periodically report on the FBI's development of Sentinel. Over the past few years, the OIG and others have reviewed various aspects of the FBI's information technology (IT) infrastructure and cited a critical need for the FBI to modernize its case management system. In previous reports, the OIG concluded that current FBI systems do not permit agents, analysts, and managers to readily access and share case-related information throughout the FBI, and without this capability, the FBI cannot perform its critical missions as efficiently and effectively as it should.

In its mission-needs statement for Sentinel, the FBI stated that its current case management system must be upgraded to utilize new information technologies by moving from a primarily paper-based case management process to an electronic records system. The FBI noted that this transition would enable agents and analysts to more effectively perform their investigative and intelligence duties.

The FBI's attempt to move from a paper-based to an electronic case management system began with the Trilogy project in mid-2001. The objectives of Trilogy were to update the FBI's aging and limited IT infrastructure; provide needed IT applications for FBI agents, analysts, and others to efficiently and effectively do their jobs; and lay the foundation for future IT improvements. Trilogy consisted of upgrading the FBI's: (1) hardware and software; (2) communications network;

and (3) the five most important investigative applications, including the antiquated ACS. The first two components of Trilogy were completed in April 2004 at a cost of $337 million, almost $100 million more than originally planned. Among other improvements, the FBI enhanced its IT infrastructure with new desktop computers for its employees and deployed a wide area network to enhance electronic communication among FBI offices and with other law enforcement organizations. However, despite additional funding the FBI had received to accelerate Trilogy, these first two phases were not completed any faster than originally planned.

In early 2004, after nearly 3 years of development, the FBI engaged several external organizations and contractors to evaluate the VCF, the third prong of the Trilogy project. The National Research Council, in its May 2004 report, concluded that the VCF project was not on a path to success because of: (1) inadequate contingency planning for the transition from the existing case management system to a new one, (2) the absence of a completed enterprise architecture, (3) inadequate time allowed for testing, (4) weaknesses in contract management, and (5) an inadequate IT human resources base.[5]

In light of these conclusions, the FBI began to consider alternative approaches to developing the VCF, including terminating the project or developing a completely new case management system. In late 2004, the FBI commissioned Aerospace Corporation to perform a trade study evaluating the functionality of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technology to meet the FBI's case management needs. Aerospace followed this study with an Independent Verification and Validation (IV&V) report on the VCF, issued in January 2005, which recommended that the FBI pursue a COTS-based, service-oriented architecture.[6] The IV&V report concluded that a lack of effective engineering discipline led to inadequate specification, design, and development of the VCF.

In late 2004, the FBI modified its approach to developing the VCF by dividing the project into Initial Operational Capability (IOC) and Full Operational Capability segments. The IOC segment assessed the

[5] The National Research Council of the National Academies. *A Review of the FBI's Trilogy Information Technology Program*, May 2004.

[6] A service-oriented architecture is a collection of services that communicate with each other. The communication can involve a simple data exchange or two or more services coordinating on an activity.

VCF project and involved a pilot test of the most advanced version of VCF in an FBI field office. The Project Management Executive for the FBI's Office of Information Technology Program Management stated that the results of the pilot validated that ending the VCF project was the right decision.

The FBI issued a final report on the IOC at the end of April 2005.[7] According to the report, the FBI terminated work on the VCF due to the lack of progress on its development. The FBI stated that it was concerned that the computer code being used to develop the VCF lacked a modular structure, thereby making enhancements and maintenance difficult. In addition, the FBI report said that the "marketplace" had changed significantly since the VCF development had begun, and appropriate COTS products, which were previously unavailable, were now available. In his March 2005 testimony before the House Appropriations Committee, the FBI Director said the FBI would apply lessons learned from the VCF to develop and deploy Sentinel.

Sentinel

Similar to what the FBI had envisioned for the final version of the VCF, Sentinel is intended to not only provide a new electronic case management system, transitioning the FBI files from paper-based to electronic records, but also to result in streamlined processes for agents to maintain investigative lead and case data.[8] In essence, the FBI expects Sentinel to be an integrated system supporting the processing, storage, and management of information to allow the FBI to more effectively perform its investigative and intelligence operations.

According to the FBI, the use of Sentinel in the future will depend on the system's ability to be easily adapted to evolving investigative and intelligence business requirements over time. Therefore, the FBI intends to develop Sentinel using a flexible software architecture that allows future changes to software components as needed. According to the FBI, a key element of the Sentinel architecture contributing to achieving this flexibility will be the use of

[7] Department of Justice, Federal Bureau of Investigation. *Federal Bureau of Investigation: Virtual Case File Initial Operational Capability Final Report*, version 1.0, April 29, 2005.

[8] A lead is a request from any FBI field office or headquarters for assistance in the investigation of a case.

COTS and GOTS applications software. The FBI intends to integrate the off-the-shelf products with an Oracle database, thereby separating the applications code from the underlying data being managed in order to simplify any future upgrades.

FBI agents are required to document investigative activity and information obtained during an investigation. The case file is the central system for holding these records and managing investigative resources. As a result, the case file includes documentation from the inception of a case to its conclusion. FBI agents and analysts create paper files in performing their work, making the process of adding a document to a case file a highly paper-intensive, manual process. Files for major cases can contain over 100,000 documents, leads, and evidence items.

Currently, the documentation within case files is electronically managed through the ACS system. The ACS system maintains electronic copies of most documents in the case file, providing references to those documents that exist in hardcopy only. Upon approval of a paper document, an electronic copy of the completed document is uploaded to the electronic case file of the ACS system. However, the ACS is a severely outdated system that is cumbersome to use effectively and does not facilitate the searching and sharing of information. For example, a former FBI project management executive testified before the Senate Judiciary Committee in July 2002 that "there's no mouse, there's no icon, there's no year 2000 look to it, it's all very keyboard intensive." The limited capabilities of the ACS and its lack of user-friendliness mean that agents and analysts cannot easily acquire and link information across the FBI.

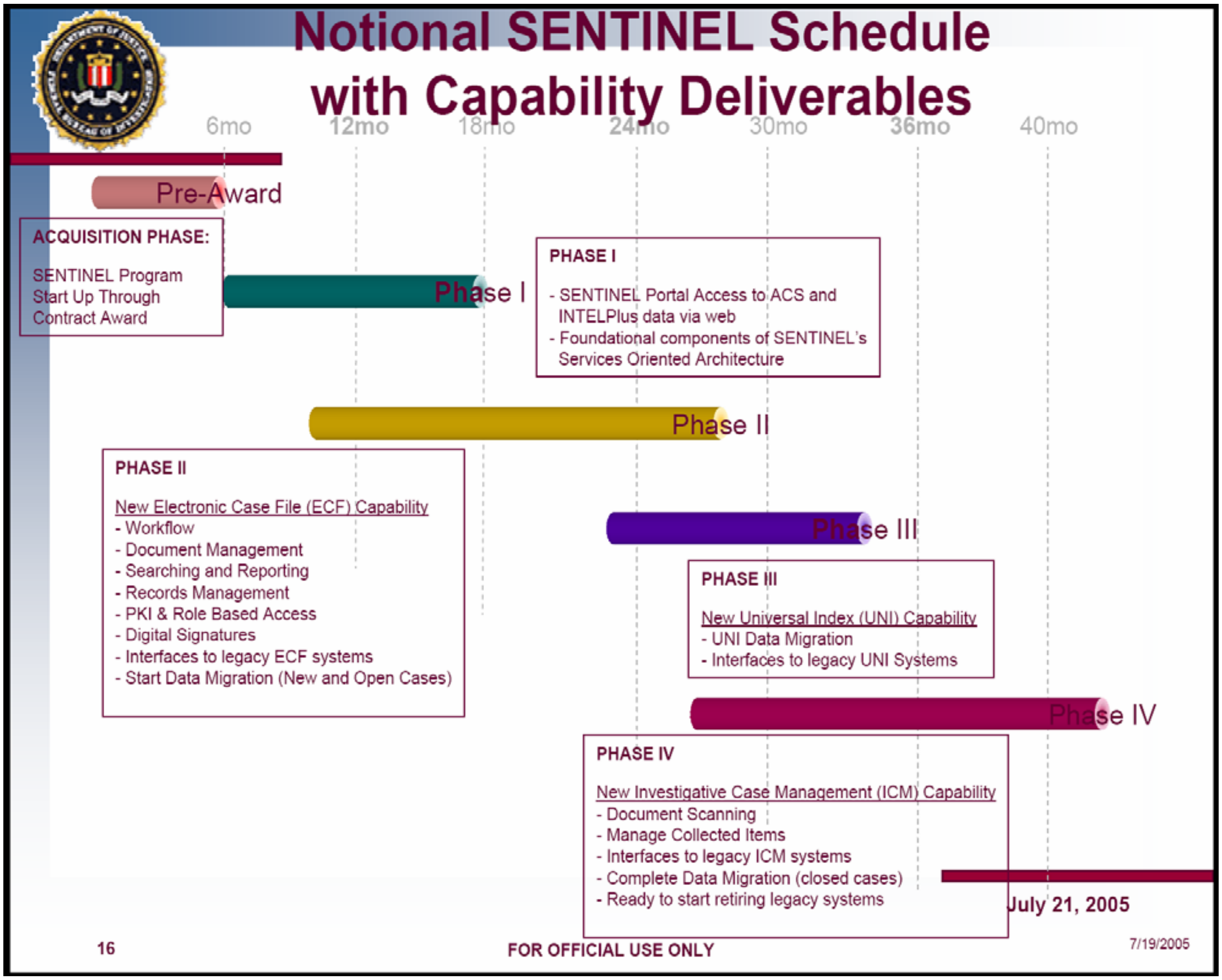
In contrast, the FBI expects Sentinel to greatly enhance the usability of case files for agents and analysts, both in terms of adding information to case files as well as searching for case information. FBI supervisors, reviewers, and others involved in the approval process also will be able to review, comment, and approve the insertion of documents into appropriate FBI electronic case files through Sentinel.

In addition to enhancing the investigative capabilities within the FBI, Sentinel is intended to serve as the pilot project in the development of the Federal Investigative Case Management System (FICMS) framework as part of the e-government case management line of business. The FBI was named the lead agency for the FICMS initiative, which, according to a June 2005 memorandum of understanding (MOU) signed by the FBI, DOJ, and DHS Chief

Information Officers (CIO), is intended to produce an architectural framework designed to: (1) bring federal law enforcement and investigative resources into a common electronic environment that promotes collaboration and optimum deployment of federal resources; and (2) create investigative case management solutions that provide state-of-the-art capabilities to collect, share, and analyze information from internal and external sources and initiate appropriate enforcement responses. According to a Senior Policy Advisor to the Department's CIO, other federal agencies can use Sentinel's core solution because of its standard set of case management tools and adaptability. Additionally, according to the FBI CIO, the Office of Management and Budget (OMB) has begun to encourage other agencies to become involved with the development of Sentinel and its interfaces in order to ensure future information sharing capability among all agencies.

Sentinel's Phased Approach

The FBI expects to develop the Sentinel project in 4 overlapping phases, each with a 12- to 18-month timeframe. For example, Phase II is anticipated to begin approximately 3 months after the start of Phase I. Each phase, when deployed, will result in a stand-alone set of capabilities that can be added to by subsequent phases to complete the Sentinel project. The following chart shows the phases and general timeframes for Sentinel, according to the FBI.



Notional SENTINEL Schedule with Capability Deliverables

ACQUISITION PHASE:

SENTINEL Program Start Up Through Contract Award

PHASE I

- SENTINEL Portal Access to ACS and INTELPlus data via web
- Foundational components of SENTINEL's Services Oriented Architecture

PHASE II

New Electronic Case File (ECF) Capability
- Workflow
- Document Management
- Searching and Reporting
- Records Management
- PKI & Role Based Access
- Digital Signatures
- Interfaces to legacy ECF systems
- Start Data Migration (New and Open Cases)

PHASE III

New Universal Index (UNI) Capability
- UNI Data Migration
- Interfaces to legacy UNI Systems

PHASE IV

New Investigative Case Management (ICM) Capability
- Document Scanning
- Manage Collected Items
- Interfaces to legacy ICM systems
- Complete Data Migration (closed cases)
- Ready to start retiring legacy systems

July 21, 2005

16

FOR OFFICIAL USE ONLY

7/19/2005

Source: FBI

Phase I will introduce the Sentinel portal, which will provide access to data from the existing ACS system and eventually, through incremental changes, support access to a newly created investigative case management system. Phase I will also provide a case management "workbox" that will present a summary of all cases the user is involved with, rather than requiring the user to perform a series of queries to find the cases as is currently necessary with the ACS. Additionally, the FBI will acquire software to identify persons, places, or things within the case files for automated indexing to allow the files to be searchable by these categories. The FBI will also select the core infrastructure components of the system in Phase I.

Phase II will provide case document management and a records management repository. The second phase will begin the transition to paperless case records and the implementation of electronic records management. A workflow tool will support the flow of electronic case documents through the review and approval cycles. A new security framework will be implemented to support access controls and electronic signatures.

Phase III will replace the Universal Index (UNI), which is used to determine if a piece of information about a person, place, or thing exists within the FBI's current case management system. The UNI is a database of persons, places, and things that have relevance to a case. While the current UNI supports only a limited number of attributes, Phase III will expand the number of attributes within the case management system. Improving the attributes associated with the entities will allow more precise and comprehensive searching and increase the ability to "connect the dots" while performing casework.

Phase IV will implement Sentinel's new case management and reporting capabilities, and will consolidate the various case management components into one overall system. At the end of this phase, the legacy systems will be shut down and the remaining cases in the legacy electronic case file will be migrated to the new case management system. In this phase, as in all the others, changes to the Sentinel portal will be required to accommodate the new features being introduced.

Prior Reports

Over the past 3 years, several oversight entities have issued reports examining the FBI's attempts to update its case management system through the VCF. These reports the OIG, the Government Accountability Office (GAO), the House of Representatives' Surveys and Investigations Staff, the FBI, and other entities made a variety of recommendations focusing on the FBI's management of the VCF project and the continuing need to replace the outdated ACS system. A discussion of key points from these reports follows. (A more comprehensive description of the reports appears in Appendix 3.)

In February 2005, the OIG reported on the critical need to replace the ACS, finding that without an effective case management system the FBI remained significantly hampered due to the poor functionality and lack of information-sharing capabilities of its current IT systems.[9] The report concluded that the difficulties the FBI

[9] Department of Justice, Office of the Inspector General. *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Management Project*, Audit Report Number 05-07, February 2005.

experienced in replacing the ACS were attributable to: (1) poorly defined and slowly evolving design requirements, (2) contracting weaknesses, (3) IT investment management weaknesses, (4) lack of an Enterprise Architecture, (5) lack of management continuity and oversight, (6) unrealistic scheduling of tasks, (7) lack of adequate project integration, and (8) inadequate resolution of issues raised in reports on Trilogy.

In April 2005, the House Appropriation Committee's Surveys and Investigations staff similarly concluded in its report that:[10]

- VCF development suffered due to a lack of program management expertise, disciplined systems engineering practices, and contract management. The project also was harmed by a high turnover of CIOs and program managers.

- VCF development was negatively affected by the FBI's lack of an empowered and centralized CIO office and sound business processes by which IT projects are managed.

- The FBI's decision to terminate VCF was related to deficiencies in the VCF product delivered, failure of a pilot project to meet user needs, and the new direction the FBI planned to take for its case management system.

- The FBI's IT program management business structure and processes at the time of the report were, for the most part, in place, although some of these processes needed to mature.

In September 2004, the GAO reported that although improvements were under way and more were planned, the FBI did not have an integrated plan for modernizing its IT system.[11] The GAO reported that each of the FBI's divisions and other organizational units that manage IT projects performed integrated planning for its respective IT projects. However, the plans did not provide a common, authoritative, and integrated view of how IT investments will help

[10] U.S. Congress, House of Representatives, House Surveys and Investigations. *A Report to the Committee on Appropriations, U.S. House of Representatives,* April 2005.

[11] U.S. Government Accountability Office. *Information Technology: Foundational Steps Being Taken to Made Needed FBI Systems Modernization Management Improvements*, Report Number GAO 04-842, September 2004.

optimize mission performance, and they did not consistently contain the elements expected to be found in effective systems modernization plans. The GAO recommended that the FBI limit its near-term investments in IT systems until it developed an integrated systems and modernization plan and effective policies and procedures for systems acquisition and investment management. Additionally, the GAO recommended that the FBI's CIO be provided with the responsibility and authority to effectively manage IT FBI-wide.

We now turn to our findings from the OIG's first audit of the FBI's Sentinel program, which as noted above focused on the FBI's pre-acquisition planning for Sentinel.

FINDINGS AND RECOMMENDATIONS

PLANNING THE DEVELOPMENT OF SENTINEL

> The FBI has applied lessons learned from the Trilogy project and failed VCF effort to the planning and management of the Sentinel project. Specifically, the FBI has made significant progress by developing Information Technology Investment Management (ITIM) processes, a more mature Enterprise Architecture, and other management improvements since the Trilogy project including establishing a Sentinel Program Management Office (PMO). Despite these improvements, we have several concerns about the project that require action and continued monitoring: (1) the incomplete staffing of the PMO, (2) the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, (3) Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (4) the lack of an established Earned Value Management (EVM) process, (5) the FBI's ability to track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's ITIM processes.

Improved Management Processes and Controls

In the early stages of the Trilogy project, the OIG and GAO recommended that the FBI establish an ITIM process to guide the development of its IT investments. In response, the FBI instituted a Life Cycle Management Directive (LCMD) in 2004 while Trilogy was well underway. The LCMD established policies and guidance applicable to all FBI IT programs and projects, including Sentinel. We believe the structure and controls imposed by the LCMD can help prevent many of the problems encountered with the failed development of the VCF.

The LCMD covers the entire IT system life cycle, including planning, acquisition, development, testing, and operations and maintenance. As a result, the LCMD provides the framework for standardized, repeatable, and sustainable processes and best practices in developing IT systems. Application of the IT systems life cycle within the LCMD can also enhance guidance for IT programs and projects, leverage technology, build institutional knowledge, and ensure that development is based on industry and government best practices.

The LCMD is comprised of four integrated components: life cycle phases, control gates, project level reviews, and key support processes. A diagram showing how these components relate to each other is found in Appendix 4**.**

According to the FBI CIO, since the inception of the LCMD all FBI IT programs and projects have been reviewed and managed according to the processes described in the LCMD. New IT programs and projects have been managed under the LCMD from inception and will continue to be managed through retirement or replacement. Existing IT programs and projects were reviewed and placed within the relevant life cycle phase according to their maturity and other factors.

System Life Cycle Phases

The LCMD has established nine phases that occur during the development, implementation, and retirement of IT projects. During these phases, specific requirements must be met for the project to obtain the necessary FBI management approvals to proceed to the next phase. The approvals occur through seven control gates, where management boards meet to discuss and approve or disapprove a project's progression to future phases of development, implementation, or retirement. As of December 6, 2005, the Sentinel project had passed through the first three of the nine phases and is currently in the fourth phase – Source Selection. The following table shows the nine phases of development, implementation, and retirement.

FBI LCMD DEVELOPMENT PHASES

PHASE NAME	DESCRIPTION
1. Concept Exploration	Identifies the mission need, develops and evaluates alternate solutions, and develops the business plan.
2. Requirements Development	Defines the operational, technical and test requirements, and initiates project planning.
3. Acquisition Planning	Allocates the requirements among the development segments, researches and applies lessons learned from previous projects, identifies potential product and service providers, and identifies funding.
4. Source Selection	Solicits and evaluates proposals and selects the product and service providers.
5. Design	Creates detailed designs for system components, products, and interfaces; establishes testing procedures for a system's individual components and products and for the testing of the entire system once completed.
6. Development and Test	Produces and tests all system components, assembles and tests all products, and plans for system testing.
7. Implementation and Integration	Executes functional, interface, system, and integration testing; provides user training; and accepts and transitions the product to operations.
8. Operations and Maintenance	Maintains and supports the product, and manages and implements necessary modifications.
9. Disposal	Shuts down the system operations and arranges for the orderly disposition of system assets

Source: FBI

Control Gate Reviews

The seven control gate reviews provide management control and direction, decision-making, coordination, confirmation of successful performance of activities, and determination of a system's readiness to proceed to the next life cycle phase. Decisions made at each control gate review dictate the next step for the IT program or project and may include: allowing an IT program or project to proceed to the next segment or phase, directing rework before proceeding to the next segment or phase, or terminating the IT program or project. The FBI's Investment Management Project Review Board (IMPRB) — comprised of 12 representatives from each FBI division at the Assistant Director level and 4 representatives from the Office of the Chief Information Office, including the CIO — is responsible for approving an IT project's passing through each control gate. The Sentinel project has been approved through the first two of the LCMD control gates: the system concept on July 15, 2005, and the acquisition plan on July 29, 2005.

The following table shows the seven control gate reviews that govern the approval of an IT project and the related LCMD phases.

FBI LCMD CONTROL GATE REVIEWS

GATE	DESCRIPTION
Gate 1	System Concept Review approves the recommended system concept of operations and occurs at the end of Phase 1 of LCMD.
Gate 2	Acquisition Plan Review approves the Systems Specification and Interface Control documents as developed in Phase 2 and the approach and resources required to acquire the system as defined in the Acquisition Plan as developed in Phase 3.
Gate 3	Final Design Review approves the build-to and code-to documentation and associated draft verification procedures. It also ensures that the design presented can be produced and will meet its design-to specification at verification. The gate review occurs after the contractor is selected in Phase 4 and system design is completed in Phase 5.
Gate 4	Deployment Readiness Review approves the readiness of the system for deployment in the operational environment. The gate review occurs after the system is developed and tested in Phase 6. Approval through the Gate 4 signifies readiness for the system implementation.
Gate 5	System Test Readiness Review verifies readiness to perform an official system-wide data gathering verification test for either qualification or acceptance. The gate review occurs mid-way through Phase 7.
Gate 6	Operational Acceptance Review approves overall system and product validation by obtaining customer acceptance and determining whether the operations and maintenance organization agrees to, and has the ability to, support continuous operations of the system. The gate review occurs at the end of Phase 7.
Gate 7	Disposal Review authorizes termination of the Operations and Maintenance life cycle phase and disposes of system resources. The gate review occurs at the end of Phase 8 and results in Phase 9.

Source: FBI

At each control gate, executive-level reviews determine system readiness to proceed to the next phase of the IT systems life cycle. Evidence of readiness is presented and discussed at each control gate review in the form of deliverables, checklists, and documented decisions. Regardless of the development model used for a particular program or project, all control gate reviews should be performed unless an agreement is made to skip or combine them. Depending upon the development model employed, programs or projects may pass through the control gates more than once. Because Sentinel is being developed in phases, and the contractor must provide a system design for each phase, the project will pass through Control Gate 3 four times.

The control gate reviews also provide executive-level controls to ensure that IT projects are adequately supported and reviewed before a project receives additional funding. Five executive-level review boards serve as the decision authority for the control gate reviews.

- The IMPRB leads the System Concept Review and the Acquisition Plan Review (Control Gates 1 and 2) and ensures that all IT acquisitions are aligned and comply with FBI policies, strategic plans, and investment management requirements.

- The Technical Review Board leads the Final Design Review (Control Gate 3) and ensures that IT systems comply with technical requirements and meet FBI needs.

- The Change Management Board leads the Deployment Readiness Review, System Test Readiness Review, Operational Acceptance Review and the Disposal Review (Control Gates 4 through 7) and controls and manages developmental and operational efforts that change the FBI's operational IT environment.

- The Enterprise Architecture Board ensures that IT systems comply with Enterprise Architecture requirements.

- The IT Policy Review Board establishes, coordinates, maintains and oversees implementation of IT policies.

The Gate 2 approval for Sentinel on July 29, 2005, signified that the IMPRB accepted the overall project approach and cost estimate for acquiring the Sentinel system. Our review of the approval documents showed that the FBI generally complied with the requirements of the LCMD in performing the control gate reviews for Sentinel. However, two documents required by the LCMD had not been completed at the time the control gate review was conducted because: (1) the system security plan could not be developed since the vendor needs to provide the project design details and, as of the date of the control gate review, the vendor had not been selected, and (2) the IV&V plan has to be carried out by a separate contractor to provide for an independent control to assess the implementation of the system according to technical and performance baselines. As of February 2006, the FBI had not yet awarded the IV&V contract. The system security plan will provide the detail necessary for the completion of certification and accreditation of the applications being created for Sentinel. The IV&V plan is, in our opinion, crucial to ensuring the success of the Sentinel project. We will continue to monitor these two items in our subsequent audit work, including whether the IV&V is being implemented by an independent contractor.

At the Gate 2 review, the IMPRB approved Sentinel prior to the approval of the acquisition plan. The OMB requires non-phased IT projects to demonstrate funding for the entire project prior to the signing of a contract. The FBI's LCMD incorporates this process for most of its IT projects. However, because Sentinel is a multi-phased project, the FBI has modified this part of the LCMD. According to the FBI, for Sentinel the FBI will identify funds for each phase of the project prior to work being initiated for that phase rather than identifying the funds for all four phases from the outset. The FBI will perform separate acquisition plan reviews for each phase prior to its initiation, and each phase must receive Control Gate 2 approval before proceeding. We agree with this modification to the LCMD for Sentinel because it provides greater oversight of the project and requires a distinct commitment of funds prior to the initiation of each phase.

Had such control gates and management reviews been in place during the Trilogy project, many of the problems with that project could have been avoided or identified earlier for corrective action.

Project-Level Reviews

Project-level reviews help determine a project's readiness to proceed to the next phase of the project life cycle. Each project-level review provides information to the executive-level control gates as data is developed and milestones are completed. At the conclusion of our field work for this audit in December 2005, the FBI had conducted two project-level reviews for Sentinel:

- The Mission-Needs Review is a technical progress review that approves the set of mission goals that will be satisfied through the project. The mission goals are documented in the Mission Requirement and Concept of Operations document.

- The System Specification Review is a technical progress review that approves the System Specification and External Interface Control Documents. The review is the decision point that determines whether to proceed with the development of an Acquisition Plan, the allocation of system requirements to segment specifications, and the development of Project Plans that will execute the acquisition.

Key Support Processes

The LCMD also contains 23 key support processes that provide additional support to the development of projects within the FBI. While the key support processes are not developed for projects specifically, these processes cover organization-wide management functions, and as a result the key support processes affect how individual projects are managed. For example, one key support process is the FBI's Strategic Plan. For Sentinel, the Strategic Plan defines the organizational need that Sentinel will address once it is implemented. However the FBI's Strategic Plan was not created specifically for Sentinel. Key process areas are performed independently of the life cycle phases and the deliverables associated with each key process are integrated into the control gate and project-level reviews where applicable. Appendix 5 lists the 23 key process areas.

Management and Oversight

Based on our review of planning documents and interviews with key FBI personnel including the CIO, we believe that the FBI is applying more rigorous management controls and ITIM processes in planning for Sentinel. Moreover, during the 3 years of Trilogy's development, the FBI had five different CIOs or acting CIOs. Since the start of Sentinel's development, the FBI has had stability in the CIO position. In addition, as a result of a July 2004 reorganization, the CIO's office has much greater authority over all FBI IT management and resources than it did in the pre-Sentinel era.

Sentinel Program Management Office

The PMO plays a critical role in assuring that the FBI implements a case management system that meets its needs. The PMO's contract and program execution responsibilities include: (1) cost, schedule, and performance oversight; (2) LCMD project reviews; (3) award fee evaluations; (4) primary contractor's documentation review and acceptance; (5) requirements and risk management; and (6) budget and financial management. In light of these responsibilities, having a qualified, dedicated PMO staff focused on program execution is critical to the success of the Sentinel project.

Since the PMO's creation soon after the inception of the Sentinel project, the FBI has made progress in staffing the office. As of January 30, 2006, the PMO consisted of 51 of the 76 IT personnel identified in the FBI's Sentinel Staffing Plan (67 percent) as required to properly oversee the project. According to the FBI, the objective in staffing the PMO is to form an integrated team of subject matter experts from government, federally funded research and development centers, and system engineers and technical assistance contractors to maximize program expertise.[12] The Sentinel program manager told the OIG that because of the pre-award spending caps placed on the program, it was premature to staff the entire PMO during the pre-award effort. As a result, he said the FBI is hiring essential program management oversight personnel to ensure that the PMO is prepared to handle contract award activities. In addition, another FBI official told us that delays in hiring PMO staff have resulted from the FBI's lengthy background investigation and clearance process. However, due to the aggressive scheduling of Sentinel, it is critical for the FBI to fully staff the PMO office as soon as possible. In our opinion, the significant turnover of project management during the Trilogy project — 15 different key IT managers over the course of its life, including 10 individuals serving as project managers for various aspects of Trilogy — was a major reason for Trilogy's problems. We believe that fully staffing the Sentinel PMO before the project begins is key to establishing the stable management staff required to properly oversee the project.

The Sentinel program manager, on loan to the FBI from the Central Intelligence Agency since November 2005, is experienced with large IT systems acquisitions and should provide strong leadership. However, he is detailed to the FBI for 2 years, with an option to extend for another year. As a result, he is expected to return to his home agency before Sentinel is completed. When questioned about the program manager's planned tenure, the FBI CIO said that a

[12] Federally funded research and development centers are nonprofit organizations sponsored and funded by the U.S. government to assist government agencies with scientific research and analysis, systems development, and systems acquisition.

potential replacement will be assigned to work directly with the program manager in the event of the program manger's departure. In addition, the FBI said that it continues to build management depth in the Sentinel PMO to ensure that each position has a trained backup to ensure continuity.

In light of the likelihood of the program manager's return to the CIA before Sentinel is completed, we believe that the FBI needs to ensure a seamless transition to a qualified successor.

Moreover, as discussed in our February 2005 report on Trilogy, given the turnover of key personnel during that effort and the resulting lack of continuity and oversight, it is important for the FBI to maximize leadership stability throughout the project, not only with respect to the program manager but also other key PMO positions.

The following table summarizes the PMO's staffing level as of January 31, 2006.

SENTINEL PMO STAFFING REQUIREMENTS

Organizational Units	Planned Staff	Staff on Board
Program Leadership	2	2
Direct Reporting Staff	8	6
Organization Change Management Team	5	2
Business Management	5	4
Administrative Support	11	5
Program Integration	10	10
System Development	23	21
Transition	9	1
Operations & Maintenance	3	0
Total	**76**	**51**

Source: The FBI
Notes: (a) The staffing requirement plan does not include individuals who are on temporary duty assignment to the project.

For a more complete description of PMO staff and their duties, see Appendix 6.

Although we are concerned about the incomplete staffing of the PMO given its vital role in helping ensure the success of the Sentinel project — particularly since project management was one of the major reasons for the VCF failure — the FBI has filled some of the more critical PMO positions, such as program leadership, system engineers, contracting officer, and business manager. The OIG will continue to monitor the staffing of the PMO and the stability of the program's leadership in future audit reports to ensure that Sentinel has the needed staff in place to help ensure its success.

Sentinel Oversight

In addition to its ITIM processes represented by the LCMD, the FBI has identified four external oversight or advisory entities in addition to the OIG and congressional committees that will provide feedback on Sentinel's development: (1) the FBI's Science and Technology Board, (2) RAND, (3) the Markle Foundation, and (4) a retired corporate chief technology officer to advise the FBI on areas of information sharing and privacy, IT strategic planning and investments, and management of large IT acquisitions.[13] The FBI also holds monthly meetings with representatives of the OMB and the Department — and weekly meetings with the FBI Director — to track Sentinel's progress. We found that progress briefings during the VCF-development process proved ineffective. Therefore, we believe that vigorous reporting and analysis of Sentinel is needed to maintain transparency over the project's progress and identify any problems encountered as Sentinel unfolds. Our future audits of Sentinel will examine the extent and effectiveness of such project oversight.

Enterprise Architecture

In its February 2005 audit report on the Trilogy project, the OIG cited the lack of an Enterprise Architecture as one of the reasons for the failure of the VCF effort. Since then, the FBI has made progress in

[13] The FBI's Science and Technology Board provides the Director with independent advice on how the FBI can more effectively exploit and apply science and technology to improve its operations. Board members are not involved in specific procurement actions or contracts but instead focus on identifying current and emerging technologies that can maximize how the FBI conducts investigations, collects and disseminates intelligence, and collaborates with law enforcement and intelligence partners.

establishing an Enterprise Architecture to more effectively and efficiently manage its current and future IT infrastructure. In March 2005, the FBI completed an Enterprise Architecture baseline report on the status of its "as is" Enterprise Architecture activities. The purpose of the report was to provide a high-level snapshot of current FBI business processes and supporting IT structures and systems. In May 2005, the FBI issued a similar report on its "to be" architecture activities and an interim architecture report showing how Sentinel will help the FBI in attaining the future IT environment outlined in the "to be" architecture report. The FBI stated that while its Enterprise Architecture continues to mature, it now provides a roadmap to help the FBI more effectively develop systems that directly support its mission.

Currently, the FBI is in the approval process for its Enterprise Architecture development methodology documentation, which will help ensure that each FBI component follows the same set of guidelines when developing IT systems. If the FBI continues to use the new Enterprise Architecture documentation to drive its IT investments, it minimizes the risk of investing in IT that is duplicative, poorly integrated, costly, or not supportive of the FBI's mission. The FBI still needs to develop a transition plan, a step-by-step process to move from the current architecture to the target architecture. In addition to establishing a fully mature Enterprise Architecture, the FBI must also begin to use the Enterprise Architecture to drive its IT investments. In our opinion, the FBI's lack of a fully mature Enterprise Architecture, which few federal agencies have achieved, should not prevent the Sentinel project from going forward.

Risk Management

The FBI has instituted a risk management process to identify and mitigate the risks associated with the Sentinel project. The Sentinel IT risk process is managed by the Sentinel program manager and a Risk Review Board. While Risk Review Board meetings have been held biweekly during the pre-acquisition phase, the FBI plans to hold weekly meetings once the Sentinel contract is awarded. The most significant risks identified by the board are examined at monthly Program Management Review sessions and other Sentinel oversight meetings in accordance with the LCMD.

The purpose of risk management is to assist the program management team in identifying, assessing, categorizing, monitoring, controlling, and mitigating risks before they negatively affect a program. A risk management plan identifies the procedures used to manage risk throughout the life of the program. In addition to documenting the risk approach, the plan focuses on how the risk process is to be implemented; the roles and responsibilities of the program manager, program team, and development contractors for managing risk; how risks are to be tracked throughout the program life cycle; and how mitigation and contingency plans are implemented.

Program risks include risks that are identified and managed by the development contractor as well as risks that can only be identified and managed by the FBI. This requires that risk management be performed by the vendor and subcontractors to identify risks from the contractor perspective, and by the FBI program management team to identify risks from the FBI's perspective.

According to Sentinel Risk Management Plan, Sentinel risks are to be identified, assessed, and tracked throughout the life of the program. The PMO is responsible for reviewing new or "proposed" risks to determine if the items should be accepted as an "open" risk. Open, or unresolved, risks are supposed to be analyzed, updated, and assigned impact and severity ratings by each voting board member. The program manager ranks the risks so that the highest priority risks get immediate attention. The PMO has the responsibility to track and periodically review risks that are closed or resolved to prevent recurrence and to document the effectiveness and any unintended consequences of the mitigation strategy employed.

In the initial Concept Exploration Phase of the life cycle, the PMO developed a mission-needs statement that identified the following five potential areas of risk in the Sentinel project.

- User Acceptance — Ensuring user friendliness, identifying possible performance problems, and addressing the cultural change employees will face in redefining their business processes are important considerations.

- Comprehensive Implementation Plan — The implementation plan needs to balance infrastructure requirements against operational functionality, assess operational impacts in a timely manner, and plan for training.

- System Capacity and Performance — Increases in workload resulting from a greatly improved ability to import documents may erode system performance. Additionally, an increased demand for interoperability with other new systems may also degrade performance.

- Data Migration — The legacy systems are known to have data integrity problems, including missing data fields. A comprehensive data migration strategy must address the scope of data to be converted to ensure performance and analysis expectations are met.

- Infrastructure Support — Sentinel will be hosted on the Trilogy Transportation Network Component and will be supported by the Enterprise Operations Center and Enterprise Security Operations Center. Inadequate support from these centers would greatly affect user acceptance of the system.[14]

In addition, the acquisition plan created in the planning phase of the life cycle identified the following risks for the Sentinel project:

- Several parallel IT initiatives within the FBI can affect the scope of Sentinel.

- The project award schedule is very aggressive and the target award date may not be attainable.

- Sentinel increments must interface with numerous legacy systems operated outside the Office of the CIO.

- The FBI mission may evolve or user requirements may change prior to system completion, resulting in scope creep.

- Initial project costs may be underestimated.

- Staffing resources (prime and subcontractors) that meet FBI requirements may not be available when needed.

- The development contractor may be unable to meet the proposed notional schedule.

The plan also considered consequences for each risk area and offered mitigation plans. We agree with the risks the FBI has identified. However, the FBI's mitigation plans, along with its LCMD

[14] The Trilogy Transportation Network Component is composed of high-speed connections linking FBI offices.

processes and other controls, if followed, will reduce the potential effects of each risk. A detailed listing of each risk and the FBI's mitigation strategy is outlined in Appendix 7.

Leveraging the VCF for Sentinel

In his February 2005 congressional testimony, the FBI Director cited a loss of $104.5 million out of the $170 million spent on the 3-year VCF development effort. However, during the current audit we were unable to determine how much of the VCF investment the FBI was able to transfer to the Sentinel project.[15] The FBI did not maintain records identifying or estimating the cost of any VCF products that can be incorporated into Sentinel. According to independent evaluations of the VCF product by Aerospace Corporation, the code used for developing the VCF was inadequate and therefore should not be useful for Sentinel. Further, the FBI intends to maximize the use of off-the-shelf products for Sentinel. Although the FBI likely applied lessons learned from the VCF effort, including a better understanding of what features it wanted in a case management system, we were unable to quantify what, if anything, was transferable from the VCF to Sentinel. One FBI system engineer said he thought that as much as 40 percent of the VCF specifications would apply to Sentinel, but he was uncertain and had no documentation to support his estimate. Another FBI official explained that a limited amount of hardware left over from the VCF effort was used by the FBI for purposes other than Sentinel. The only clear-cut transfer from the VCF was $3,542,000 in fiscal year (FY) 2004-2005 funding that has been redirected to Sentinel.

Sentinel Cost and Funding

Because this first Sentinel audit focused on the FBI's pre-acquisition planning, and given the procurement sensitive nature of the information, the FBI did not disclose to the OIG the estimated cost of the planned four-phase Sentinel project. However, in response to a Senate Appropriations Committee inquiry in October 2005, the FBI estimated that it would cost between $400 and $500 million to develop Sentinel. According to the Sentinel program manager, the precise cost estimate will not be known until the FBI awards the contract, which

[15] The hardware and communications infrastructure deployed as a part of Trilogy will be used by Sentinel.

has been postponed to early 2006.[16] Our next audit will examine in detail the winning bidder's cost estimates.

According to the FBI's Deputy Assistant Director of Finance, during the summer of 2005 the FBI met with representatives from the Department of Justice and the OMB to discuss options to fund the project. In the end, the FBI decided to seek funding for Sentinel using both reprogrammed and appropriated funds: the first two phases would be funded using FBI funds reprogrammed from other projects and operations and the third and fourth phases would be funded using appropriated funds.

Reprogramming Request

According to an FBI official, the OMB required the FBI to identify the funding for each phase of Sentinel before work on that phase could begin. As a result, on September 27, 2005, the FBI submitted a $97 million reprogramming request to Congress for the first phase of Sentinel. Congress approved the request on November 15, 2005. The FBI's reprogramming request did not offer sufficient detail for us to render a detailed opinion on the specific amount of the request. Yet, because of the FBI's extreme need for a new case management system, this initial reprogramming request appears reasonable, and in our judgment, the Sentinel program should move forward.

The FBI currently is developing a second reprogramming request to fund the second phase of Sentinel at an amount which we believe will be similar to the first request — approximately $100 million. The size of the appropriations the FBI expects to seek from Congress to complete the third and fourth phases of the Sentinel program are unknown to us, as are the funds that will be needed to operate and maintain the program on an ongoing basis. The FBI has agreed to provide a more precise cost estimate for the remainder of the project after the Sentinel contract is awarded.

With regard to training, the FBI's initial $97 million reprogramming request includes $1.2 million in training costs in the first phase of the Sentinel program. However, the FBI has not yet developed a comprehensive training plan for Sentinel or an estimate for its full training costs. In our judgment, training costs over the life of the project will be substantial.

[16] According to the FBI, the contract award was postponed because the FBI needed additional information from the bidders.

The reprogramming request also cites approximately $10 million as management reserve. In our judgment, maintaining a management reserve is a prudent practice given the uncertainties of developing a new IT system. However, when attempting to calculate the amount of the management reserve required for a major IT project, an organization should consider the degree of risk associated with the project and use Earned Value Management (EVM) tools to quantify the effect on the project should the potential risk materialize. We do not have enough information at this time to evaluate the adequacy of the FBI's proposed reserve for the first phase of Sentinel or what amount of reserve might be required over the life of the entire program. As the project progresses, the FBI must continue to monitor and reassess the level of the reserve fund.

According to the FBI, more than $14 million of the initial reprogramming will come from the Counterterrorism Division budget, $13 million from intelligence-related activities, and $2 million from the Cyber Division. We interviewed officials at FBI headquarters to assess the effect of the $97 million reprogramming on FBI operations. Generally, these officials said their divisions and offices can withstand the diversion of funds to Sentinel for the first reprogramming. However, we are concerned that diverting substantial funds from such mission-critical areas could begin eroding the FBI's operational effectiveness, only to be compounded by an anticipated second reprogramming.

Although most FBI divisions and offices seemed confident about their ability to absorb the initial reprogramming of funds to Sentinel, they stated that a second reprogramming of the same magnitude would damage their ability to fulfill their mission. According to FBI CIO, the FBI intends to send another reprogramming request to Congress to fund the second phase of the Sentinel program in FY 2006.

The OIG plans to assess the operational impact of these reprogrammings in subsequent Sentinel audits to assess whether the FBI's critical missions are adversely affected while the FBI also seeks to provide its employees with a case management system that will help them do their jobs more effectively and efficiently.

Cost Tracking and Control

In the Trilogy project, the FBI lacked an effective, reliable system to track and validate the contractors' costs. We highlighted this concern in our February 2005 report on Trilogy and the VCF. Further, in February 2006 draft report, the GAO stated its preliminary finding that the FBI's poor cost controls resulted in the payment of about $10 million in questionable contractor costs.[17] Although the FBI stated that it is evaluating a tool to track Sentinel project costs, we view the potential weaknesses in cost control as a project risk.

Earned Value Management

One approach to achieving reliable program cost estimates, evaluating current progress, and analyzing schedule and cost performance trends is to employ the discipline of EVM. EVM enables project teams to report progress to program managers to evaluate performance against initial baselines. In essence, EVM is a method of imposing accountability on a project and exposing potential problems while there is still time to fix them.

In a memorandum dated August 4, 2005, the OMB required federal CIOs to manage and measure all major IT projects to within 10 percent of baseline goals by using an EVM system. The OMB required each agency to develop agency policies for full implementation of EVM on IT projects by December 31, 2005. In August 2005, the FBI developed a Sentinel Program EVM Capability Implementation Plan which, in our judgment, satisfied the OMB requirement for the project.

According to the plan, the Sentinel PMO will use the plan to measure its earned value performance, and the performance of the vendor, and report the result to oversight entities. The Statement of Work requires that Sentinel's vendor and its contractors implement EVM in accordance with the plan.

According to the FBI, it has evaluated several tools to track and manage EVM results. The evaluation consisted of examining technical and functional capabilities of the tools, learning about the requirements for the associated system environment, reviewing implementation methodologies and training materials, evaluating tool acquisition and installation costs, and viewing demonstration sessions

[17] U.S. Government Accountability Office. *(DRAFT) Federal Bureau of Investigation: Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets*, Report Number GAO-06-306, February 2006.

of potential tools. As a result of this review, the FBI intends to use the following tools to track and manage Sentinel in the short term.

- Program schedules, including milestones, will be developed and maintained using the existing Microsoft Project 2003 software.

- Program risks will be documented and managed using the Risk Register software suite developed and maintained by the FBI Office of IT Planning and Policy.

- Budgets will be prepared and managed using Microsoft Office Professional software resident in the FBI's Trilogy software suite.

In the long term, the FBI expects that its EVM performance metrics will be developed, maintained, and reported using Métier's WorkLenz software suite. The FBI is acquiring the software but will need to complete security certification and accreditation for the software to be certified for use on FBI systems. According to the FBI, full implementation and execution of the EVM capabilities for the Sentinel project are scheduled to be completed after the Integrated Baseline Review occurs approximately 2 months after the award of the Sentinel contract. Based on our initial review, the FBI's EVM strategy appears adequate. We will monitor the FBI's implementation of EVM in future audits.

Capability Maturity Model Integration

The FBI's Statement of Work for the Sentinel project requires that bidders obtain an independent appraisal certifying that their systems development, software engineering, and integration processes are at a Level 3 or higher on the Carnegie-Mellon University's Capability Maturity Model Integration (CMMI) 5-level maturity scale. This requirement includes all vendors and any subcontractor that will contribute a minimum of 10 percent of the total Sentinel effort in developing or integrating software. Sentinel's Statement of Work also gives the FBI the right to interview the lead appraiser who conducted the assessment and to conduct independent assessments during the development of the project to verify compliance with the appraised processes.

We believe that by requiring the vendor to perform at a CMMI Level 3, the FBI reduces the risk of selecting a vendor that is not capable of completing the Sentinel project and integrating all four project phases. Additionally, because the vendor will be independently reviewed by a CMMI appraiser, the FBI has assurance that the processes the vendor will use to develop Sentinel are rated favorably in relation to best industry practices. In our upcoming audit work, we plan to verify that the appraisal was conducted, review its results, validate the appraiser's independence, and review the results of the appraisal.

Contracting

In selecting the appropriate contract type for the development of Sentinel, the FBI originally identified 16 Government-wide Acquisition Contracts (GWAC) that were suitable for a project as extensive as Sentinel. The FBI eliminated 11 of the 16 GWACs as inappropriate vehicles for Sentinel because the contract vehicle's task scope was inadequate, task-order cost reimbursement was not allowed, or the contractors available through the GWAC lacked the expertise needed for the project. The FBI further analyzed the other five GWACs to determine which were the most suitable for the project. The analysis included a 29-item questionnaire with 6 discriminator areas.[18] The discriminator areas are listed below.

- FBI Audit Capability — The FBI believed that its ability to audit the contractor's financial records would be critical to determine invoice accuracy and program progress.

- Use of FBI Contracting Officer Post Award Administration — The FBI wanted to ensure that the contracting vehicle would allow the FBI to manage the contract using the FBI Contracting Officer.

- Number of Prime Contractors on the GWAC — The FBI believed that the more prime contractors available on the GWAC the greater the possibility of selecting the most qualified contractor.

- Period of Performance Limitations — The FBI wanted to ensure that the GWAC would not expire before the completion of the Sentinel project.

[18] See Appendix 8 for a list of 29 items from the questionnaire.

- Ability to Add Subcontractors — The FBI wanted to ensure that the prime contractor's ability to add a new or specialized subcontractor to resolve unique problems would not be affected by GWAC constraints.

- Interagency Fee Structure — The FBI wanted to ensure that interagency fee charged by the GWAC for use of its contract vehicle was reasonable.

Based on the information obtained from the questionnaires, the FBI eliminated two of the remaining five GWACs for two reasons: (1) the GWAC did not allow direct order, and (2) the GWAC may not support the acquisition strategy of having all task orders awarded by January 2006 and be of no more than five years in duration.[19] From the other three GWACs, the FBI chose the National Institute of Health's (NIH) Chief Information Officer–Solutions Partners 2 *Innovations* (CIO-SP2i) contract vehicle because it gave the FBI the greatest flexibility and included 37 potential bidders.

The Federal Acquisition Regulations (FAR) § 15.201 encourages agencies to promote early exchanges of information prior to the release of the Request for Proposals (RFP). The purpose of exchanging information is to improve the understanding of government requirements and industry capabilities, thereby allowing potential bidders to judge whether or how they can satisfy the government's requirements. An early exchange of information can identify and resolve concerns regarding: the acquisition strategy, including the proposed contract type; terms and conditions; acquisition planning schedules; requirements; statements of work; data requirements; and any other industry concerns or questions. The FAR also identifies techniques to promote early exchanges of information, including industry or small business conferences, public hearings, market research, and one-on-one meetings with potential bidders.

On June 27, 2005, the FBI held an Industry Day to exchange information with potential bidders. All NIH CIO-SP2i contractors were invited to participate. According to the FBI, the potential contract bidders attending the session submitted both contractual and technical questions. However, the FBI would not provide these questions for our review because they were deemed procurement sensitive.

[19] Direct order allows the agency, not the GWAC, to issue and manage the task orders associated with the contract.

On August 5, 2005, the FBI issued an RFP with responses due by September 19 and a contract award date of November 15. According to FBI officials, the due date for the proposals was extended one week to September 26, 2005, because vendors needed more time to complete the technical, management, and cost sections of the proposal. Subsequently, the contract award date was rescheduled for December 31, 2005, and later postponed again to an unspecified date in 2006. The FBI said that the source selection evaluation team, during its initial review of the proposals, identified the need for additional data from the bidders. As a result, the FBI said it will not establish a new contract award date until the source selection evaluation team receives and reviews the additional data.

According to the FAR § 15.203, RFPs for competitive acquisitions should state the government's requirements, anticipated terms and conditions that apply to the contract, information required in the bidder's proposal, and factors that will be used to evaluate the proposal. To meet this requirement, the Sentinel RFP contained the following documents.

- System Requirements Specification — This document outlined the specific requirements that the Sentinel system will satisfy.

- Statement of Work — This document described the FBI's requirements for Sentinel.

- Proposal Preparation Instructions — This document provided instructions on how proposals should be prepared and submitted. It also included limited terms and conditions that will apply to the contract, including the award fee structure.

- Evaluation Criteria — This document was a part of the Sentinel Statement of Work and described the factors to be used in evaluating each proposal.

Based on the above, in our judgment the FBI issued the Sentinel RFP in accordance with the FAR requirements. While delays have occurred in awarding a contract for Sentinel, we believe it better for the FBI to take a reasonable amount of time at the outset of the project to ensure that the bidders fully understand the FBI's needs, system specifications, and expectations.

According to Sentinel program manager, The FBI is evaluating the proposals based on the following criteria.

- Past Performance — This item examines the quality of the bidder’s past performance on programs that are similar in size, scope, and technological and managerial complexity to the Sentinel program. Specifically, the FBI is evaluating the bidder’s technical and management performance and a functional system the bidder developed.

- Technical Approach — This item examines the quality of the bidder’s phased development approach and the sufficiency of the proposed off-the-shelf selection approach.

- Management Approach — This item examines the bidder’s proposed management approach for executing Sentinel’s design, development, integration and testing, deployment, and operations and maintenance.

- Security Approach — This item examines the bidder’s proposed approach to meeting the Sentinel security requirements including personnel, infrastructure, and lifecycle security.

- Cost — This item examines the realism, reasonableness, and completeness of the bidder’s proposed cost.

The FBI solicited assistance from federally funded research and development centers and other organizations for administrative, technical, and cost analysis support during source selection. These companies were also used as advisors in the evaluation of the proposals. However, the FBI retained the responsibility for selecting the contractor.

At the end of source selection, the FBI intends to award a cost-plus-award-fee task order contract to develop the Sentinel system. A cost-plus-award-fee contract provides an estimated cost plus a fee consisting of a base amount fixed at inception of the contract and an award amount. The award amount is a pool of dollars available to the vendor to earn based on performance. The government makes the award fee determination based on periodic evaluations of vendor performance. One important aspect of a cost-plus-award-fee contract is that the award fee amount must be sufficient to motivate the vendor’s performance. According to the Sentinel Award Fee Plan, the FBI anticipates capping the overall contract award amount for the development of Sentinel at 12 percent of development costs.

This type of contract is common for large government IT projects. In our 2005 report on Trilogy, we stated our concerns with the cost-plus-award-fee contract as it was implemented by the FBI in that project. The cost-plus-award-fee contract used for Trilogy did not: (1) require specific completion milestones, (2) include critical decision review points, and (3) provide for penalties if the milestones were not met. However, the FBI's improved management processes and controls should minimize the risk of such problems recurring for Sentinel since the FBI intends to establish clear milestones, penalties for not meeting milestones, and critical decision review points.

Information Sharing

Executive Order 13356 requires that federal agencies design information systems with priority given to the interchange of terrorism information among agencies. Although the FBI has planned extensively for information to be shared among its divisions and offices, we found that it has expended little effort in assessing information sharing needs with other federal agencies. In particular, we have no assurance that the FBI has identified all external systems with which Sentinel must connect. While the Sentinel PMO told us that all external interfaces have been identified, we found that the external information sharing requirements for Sentinel have not yet been fully established but are scheduled to be completed by April 2006. Because these requirements have yet to be established, we anticipate a modification to the contract. In our opinion, such modifications represent a potential risk of requirements creep.

The FBI is developing Sentinel using architectural models not widely used in the Department of Justice, which may require retrofitting or modifying other Department information systems as well as those of other agencies to effectively share information with Sentinel. The cost, extent, and timing of those modifications are not known. In our judgment, the FBI needs to focus more attention on the sharing of information between Sentinel and other agencies' data systems in these early stages of Sentinel's development. As discussed below, if Sentinel is developed without defining adequate external information sharing requirements, the system may not meet the information sharing mandate of Executive Order 13356, and costs may escalate due to the addition of these requirements later.

Information Sharing Requirements

During our audit, we interviewed several FBI and Department officials to better understand the process used to identify Sentinel's information sharing requirements. We found that the process the FBI used to identify the internal information sharing requirements was extensive, while the process to identify external information sharing requirements and compatibility appeared non-existent.

According to the FBI, during the development of Sentinel's requirements system engineers held working sessions with future Sentinel users in the FBI to gain an understanding of what the system needed to do. The results of these sessions were compiled into a working draft of the Sentinel system requirements, which was then circulated to internal users for comment. According to FBI officials, approximately 1,200 comments were received, and many were integrated into the final systems requirements document. As a result of this interaction with internal users, the Sentinel requirements detailed how the system should interact with internal systems. For example, the system requirements show how data would be entered into and extracted from Sentinel as well as how Sentinel will generate reports currently produced by other FBI systems.

In response to our concerns about information sharing, the FBI CIO stated that the FBI is working with the OMB, DHS, and the Directorate of National Intelligence (DNI) to ensure external interface requirements are adequately considered. However, the FBI CIO noted that while the OMB is taking steps to encourage external agencies' involvement, the level of involvement of these agencies cannot be controlled by the FBI. With respect to external IT system connections with Sentinel, the FBI said that in July 2005 it invited the Department of Homeland Security (DHS), the Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) to participate in its development of Sentinel's requirements and has since begun discussions with the OMB and DNI on the need for system connections.

We interviewed representatives from the DHS, DEA, and ATF to determine the extent of each agency's involvement in the development of Sentinel's requirements. The DHS representative stated that the DHS was given the opportunity to review the requirements document after the document was finalized by the FBI. The DHS has committed to providing the FBI with subject matter experts for 3 years in the areas of Enterprise Architecture, system engineering, security, privacy, and data to the project. At the time of our audit, the DHS was in the process of identifying the personnel to detail to the FBI.

A DEA official stated that the FBI initially wanted the DEA to participate in an advisory capacity on the Sentinel steering committee and to have someone assigned full-time to Sentinel. While the DEA was not able to provide a full-time staff member, two officials participated on the steering committee. In addition, a DEA official reviewed the requirements for Sentinel to ensure that Sentinel addressed DEA information sharing needs. Although the DEA plans to deploy its own new case management system to its field offices in early 2006, the DEA said it intends to stay abreast of any developments with Sentinel. The DEA anticipates that staying informed about Sentinel will enable it to make changes to its case management system as the Sentinel project develops, thereby reducing the need of major retrofitting after Sentinel is completed. However, before Sentinel can connect with the DEA's case management system, a gateway from the classified operating environment of Sentinel to the sensitive but unclassified environment of the DEA's case management system must be established. Overall, DEA managers said they believe that Sentinel will meet the agency's information sharing needs as long as the FBI executes the project as planned.

ATF officials told us that in late September 2005, an ATF official met with the Sentinel program manager to introduce himself as a point of contact for the ATF and provide information about the ATF's research into off-the-shelf products to enhance case management inquiry capability and facilitate information sharing. ATF officials said that they had not reviewed any of the requirements for Sentinel, and have had no other involvement with Sentinel. According to the ATF, it is too early in the Sentinel project for it to determine whether any retrofitting of ATF programs will be required once Sentinel is completed to enable information sharing to occur between the two agencies.

During our audit work, we reviewed briefing documents, prepared by the FBI Office of IT Program Management for the FBI Deputy Director, in which the FBI indicated that the external interfaces for information sharing with the intelligence and law enforcement communities were not well-defined. When questioned about its uncertainty regarding Sentinel's compatibility with other agencies' systems, the FBI said that it has identified all known external interfaces that would fall under the FBI's information-sharing requirements. In addition, the FBI said that previously agreed-upon standards for information sharing across the law enforcement, intelligence, and defense communities will be followed in the development of Sentinel. However, we have not seen evidence of a comprehensive list of these information-sharing requirements. In fact, an FBI division head told us that the FBI's list of external information-sharing requirements should be completed by April 2006. As noted previously, if Sentinel is developed without adequately defining such external information sharing requirements, the system may not meet the information sharing mandate of Executive Order 13356 and the cost of the project may escalate because of the inclusion of these requirements at a later date.

Target Architecture

Sentinel will be developed using the Global Justice Extensible Markup Language (XML) Data Reference Model (GJXDM) and its extension, the National Information Exchange Model (NIEM). (See Appendix 9 for a discussion of these models.) The GJXDM and NIEM can make information exchange substantially more efficient by defining how information should be documented. In addition, the intelligence agencies connected to Sentinel will use the Terrorist Watchlist Person Data Exchange Standard.[20] The FBI expects its new investigative case management architecture to capture and define processes for performing investigations and for collecting, controlling, analyzing, and sharing law enforcement data. Consequently, the target architecture for Sentinel that is expected to enable greater information sharing and improved management reporting is a key deliverable of the Sentinel case management system.

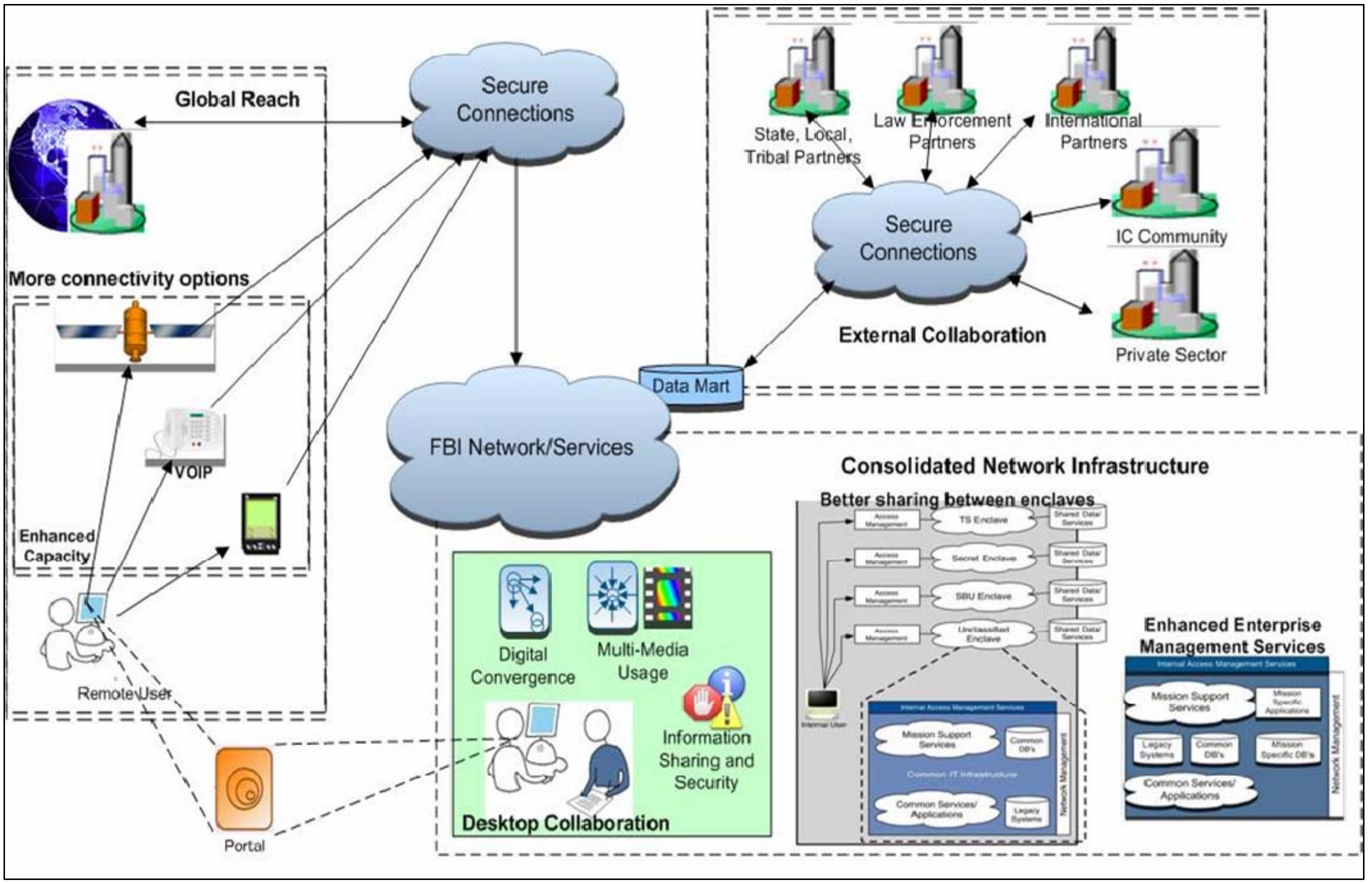
According to a Department of Justice system architect, the GJXDM is not yet in use in most of the systems in the Department. However, he said the Department is moving forward on a number of initiatives to ensure its broader implementation. We believe the FBI and the Department need to focus more attention on this connectivity issue, because external entities' systems have not been developed with the same architectural model. Therefore, retrofitting or modifying the external agencies' systems may be necessary, and the cost, extent, and timing of such retrofitting is unknown at this time.

According to FBI officials, external collaboration, including information sharing with the intelligence community and law

[20] The Terrorist Watchlist Person Data Exchange Standard is a data exchange format for terrorist watchlist data that supports the Departments of State, Justice, Homeland Security, and the intelligence community.

enforcement partners, is envisioned with secure connections to a data mart.[21] The following figure depicts the FBI's target architecture for such external information sharing.

VISION of FBI TARGET ARCHITECTURE



Source: Department of Justice Office of the CIO

The terrorist attacks of September 11, 2001, underscore the need for agencies involved in combating terrorism to be able to communicate with one another effectively. An intelligence agency may have only partial information on a suspected terrorist, but when coupled with information that other agencies possess, a threat may become more clear. In our judgment, there is no assurance that the requirements for Sentinel have been sufficiently defined to allow such interagency information sharing without potentially costly and time-consuming modification of agencies' existing systems to achieve

[21] A data mart is a specialized version of a data warehouse. Like data warehouses, data marts contain a snapshot of operational data that aids strategizing based on analyses of past trends and experiences.

compatibility with Sentinel. While Sentinel is first and foremost a system that must address the FBI's needs, in our judgment it may not serve the FBI's goal to prevent future terrorist attacks if this new system is isolated from information that exists within other agencies' information systems.

Federal Investigative Case Management System

In addition to developing its own case management system, the FBI is also the lead agency for the interagency Federal Investigative Case Management System (FICMS) initiative, as stated in a memorandum of understanding (MOU) signed by the FBI, DOJ, and DHS CIOs in June 2005. As lead agency, the FBI is expected to develop an architectural framework that will establish case management data and technology standards that enable electronic information sharing among government agencies. In April 2005, the FBI developed a draft FICMS framework which, according to the FBI CIO, was submitted to the Department for consideration. He added that the Department is refining the draft framework into a more mature framework. The June 2005 MOU also states that Sentinel will be the first implementation of the FICMS framework. The FBI CIO stated that the FBI is using the draft framework to drive the development of Sentinel, and when Sentinel is completed it will provide the FICMS framework with various case management services that can be adopted by other agencies.

According to the 2005 MOU, two mission needs drive the development of the Sentinel project as the initial implementation of the FICMS:

- bring all federal law enforcement and investigative resources into a common electronic environment that promotes collaboration and optimum deployment of federal resources, and

- create investigative case management solutions that provide state-of-the-art capabilities to collect, share, and analyze information from internal and external sources, and initiate appropriate enforcement responses.

The DHS said it provided $500,000 in FY 2005 to the Department of Justice for FICMS and will contribute up to that amount in FY 2006. A DHS official said that the DHS would have to wait and see if the FBI establishes its business processes within Sentinel in such a way that allows the processes to be modified to meet the needs of other agencies or not. However, if the FBI develops Sentinel as intended — using a service-oriented architecture — the DHS anticipates using approximately 40 to 60 percent of the system. Other potential users of the FICMS framework outside the Department of Justice include the Departments of Energy and Treasury, and the DNI. Therefore, the FBI should more closely consult with other intelligence and law enforcement agencies as the FBI moves forward in developing Sentinel.

Conclusion

In our judgment, the FBI has taken a variety of positive steps to address its past IT development mistakes and to plan for the development of Sentinel. Specifically, the FBI has made significant progress by developing ITIM processes, a more mature Enterprise Architecture, and other management improvements since the Trilogy project, including establishing a Sentinel Program Management Office.

However, we have several concerns about the project that require action and continued monitoring by the FBI, the OIG, and other interested parties: (1) the incomplete staffing of the PMO, (2) the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, (3) Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (4) the lack of an established EVM process, (5) the FBI's ability to track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's ITIM processes.

Unlike during its failed VCF effort, the FBI now has a maturing Enterprise Architecture and a sound ITIM process in its LCMD. We found that the FBI generally is managing the Sentinel project in accordance with the LCMD. By following the LCMD, the FBI appears to have implemented adequate management controls through a variety of review boards and other oversight structures. This includes the identification of project risks and the development of mitigation strategies for those risks. The addition of an effective EVM process will also enhance the FBI's control over the project cost and schedule. According to the FBI, full implementation of an EVM process for the Sentinel project is scheduled to occur approximately 2 months after the Sentinel contract is awarded. Based on our initial review, the FBI's

EVM strategy appears adequate. We will monitor the FBI's implementation of EVM in future audits.

The FBI continues to build a PMO specific to the Sentinel project, an entity critical to the project's successful management continuity and oversight. However, as of January 30, 2006, the Sentinel PMO was staffed with 51 of the 76 staff the FBI determined are needed to successfully manage Sentinel. Unless the FBI fully staffs the PMO during the first phase of the project, the FBI runs the risk of not being able to oversee adequately Sentinel's aggressive delivery schedule. We believe that it is imperative for the FBI to fully staff the PMO with qualified personnel as quickly as possible and to continue to follow the guidelines, requirements, and controls established in the LCMD.

While we support in principle the FBI's initial $97 million reprogramming request for the Sentinel program, we have concerns about the effect of a second large reprogramming request on the FBI's mission-essential operations. It is not clear to us how the FBI can effectively carry out its wide-ranging and complex mission if funds of this magnitude need to be diverted from other FBI programs in a second reprogramming. Additionally, the FBI's ability to track Sentinel's costs needs to be firmly established by the time the contract is signed to ensure that all of the funding for the project is adequately accounted for.

Although the FBI has tried to use its past work on VCF in the Sentinel effort, neither the FBI nor we could quantify how much hardware and development work from the VCF had been transferred to the Sentinel project.

With regard to information sharing, we found that the development of Sentinel and the architecture for the interagency FICMS are being performed largely in parallel. Sentinel is being developed to be compliant with the GJXDM language and data reference and the Terrorist Watchlist Person Data Exchange Standard. There are risks associated with this tandem development approach, because Sentinel is essentially defining the standards for FICMS. Furthermore, the ultimate connectivity between Sentinel and external systems remains unclear, as most Department of Justice systems are not using the GJXDM model and may require significant modifications to facilitate information exchange. The cost and extent of those modifications are unknown at this time.

In our judgment, Sentinel's requirements, including those for information sharing, must be firm before work begins on the project in order to avoid delays and cost increases and if Sentinel is to serve one of its intended purposes — to provide an investigative case management system that other federal law enforcement agencies can adapt for their own use and that will allow for information sharing among federal law enforcement and intelligence community agencies. Although the FBI appears to have thoroughly examined internal FBI information sharing requirements in developing Sentinel, it has not ensured compatibility with other agencies' systems.

We have found that in addition to continuing to develop an EVM process and the capability to track costs, the FBI has yet to complete system security and verification and validation plans as established in the FBI's ITIM. These plans, which the FBI intends to complete after the Sentinel contract is awarded, are required to ensure that the system meets the FBI's security requirements and is implemented according to established control mechanisms.

The OIG will continue to monitor and periodically issue audit reports throughout the Sentinel project in an effort to track the FBI's progress and identify any emerging concerns over the cost, schedule, technical, and performance aspects of the project. As a result of our review of the pre-acquisition phase of the Sentinel project, we make the following recommendations.

Recommendations

We recommend that the FBI:

1. Ensure that the system security and Independent Verification and Validation plans are completed as soon as possible after the contract is signed.

2. Ensure that the Sentinel Program Management Office is staffed to a level that will support Sentinel's aggressive delivery schedule.

3. Obtain a tool that will allow for the effective implementation of an Earned Value Management process and fully implement this process.

4. Discuss with other intelligence community and law enforcement agencies their information sharing requirements to ensure compatibility with those systems in the requirements and design of Sentinel.

5. Ensure that an effective system is in place to accurately track and control Sentinel's development costs.

6. Complete a comprehensive Sentinel training plan with realistic schedule and cost estimates and include these training cost estimates in the estimates of overall project costs.

7. Establish a method to monitor the operational impact of a potential second reprogramming and identify for resolution any degrading of the FBI's mission-critical functions due to the diversion of funds to the Sentinel project.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

This audit assessed the FBI's planning for its Sentinel case management project. In connection with the audit, as required by the *Government Auditing Standards*, we reviewed management processes and records to obtain reasonable assurance that the FBI's compliance with laws and regulations that, if not complied with, in our judgment, could have a material effect on FBI operations. Compliance with laws and regulations applicable to the FBI's management of the Sentinel project is the responsibility of the FBI's management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations against which we conducted our tests are contained in the relevant portions of:

- President's Management Agenda,
- OMB Circulars A-11 and A-130,
- Executive Order 13356 (superseded by "Executive Order: Further Strengthening the Sharing of Terrorism Information to Protect Americans," dated October 25, 2005),
- Federal Acquisition Regulations,
- E-Government Act,
- Clinger-Cohen Act,
- Paperwork Reduction Act,
- DOJ IT Strategic Plan,
- Federal Investigative Case Management System Framework,
- FBI IT Strategic Plan, and
- FBI Life Cycle Management Directive.

Our audit identified no areas where the FBI was not in compliance with the laws and regulations referred to above. With respect to transactions that were not tested, nothing came to our attention that caused us to believe that FBI management was not in compliance with the laws and regulations cited above.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the FBI's pre-acquisition planning for its Sentinel project, we considered the FBI's internal controls for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the internal control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the FBI's ability to manage its Sentinel project. During our audit, we found the following internal control deficiencies.

- The FBI's Program Management Office for Sentinel is not yet fully staffed to effectively manage the Sentinel project.

- Sentinel's information sharing requirements are not yet clearly defined to meet the federal intelligence sharing mandate.

Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI in planning for the Sentinel project. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

The objective of the audit was to evaluate the FBI's planning for Sentinel, including the approach, design, cost and funding sources, timeframe, contracting vehicle, and oversight structure.

Scope and Methodology

The audit was performed in accordance with the *Government Auditing Standards*, and included tests and procedures necessary to accomplish the audit objective. We conducted work at the FBI Headquarters in Washington, D.C.

To perform our audit, we interviewed officials from the FBI, DEA, ATF, DHS, and the Department of Justice. We also reviewed documents related to the planning for the Sentinel project, budget documentation, organizational structures, congressional testimony, and prior GAO and OIG reports.

To evaluate the FBI's planning for Sentinel including the approach, design, cost and funding sources, timeframe, contracting vehicle, and oversight structure, we examined the FBI's compliance with its Life Cycle Management Directive. We did this by reviewing the FBI's plans for each completed phase of the directive. We also interviewed FBI division heads to determine if, in their opinion, the system requirements are comprehensive enough to meet user expectations. In addition, we reviewed the FBI's methodology for selecting the contracting vehicle and developing the system requirements. We examined the FBI's proposed funding for the project including the reprogramming request for the first phase. We also discussed with FBI officials the potential risk to the FBI's operations if a second reprogramming is necessary. We analyzed the FBI's staffing procedures for the management and oversight for Sentinel.

To examine the issue of information sharing, we reviewed the Sentinel statement of work and the system requirements. We also discussed this issue with representatives from the CIO offices of the FBI, DEA, ATF, and the Departments of Justice and Homeland Security.

ACRONYMS

ACS	Automated Case Support
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CIO	Chief Information Office
CMMI	Capability Maturity Model Integration
COTS	Commercial Off-the-Shelf
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
EVM	Earned Value Management
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FICMS	Federal Investigative Case Management System
FY	Fiscal Year
GAO	Government Accountability Office
GJXDM	Global Justice XML Data Reference Model
GOTS	Government Off-the-Shelf
GWAC	Government-wide Acquisition Contract
IOC	Initial Operational Capability
IMPRB	Investment Management Project Review Board
IT	Information Technology
ITIM	Information Technology Investment Management
IV&V	Independent Verification & Validation
LCMD	Life Cycle Management Directive
MOU	Memorandum of Understanding
NIEM	National Information Exchange Model
NIH	National Institutes of Health
OCM	Organization Change Management
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PMO	Program Management Office
RFP	Request for Proposal
UNI	Universal Index
VCF	Virtual Case File
XML	Extensible Markup Language

APPENDIX 3

PRIOR REPORTS ON THE FBI'S INFORMATION TECHNOLOGY

Below is a listing of relevant reports discussing the FBI's information technology systems. These include reports issued by the Department of Justice, Office of the Inspector General (OIG), the Government Accountability Office (GAO), and by other external entities as well as FBI internal reports.

External Reports on FBI Case Management Efforts

In February 2005, the OIG issued a report entitled, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Management Project*, which encompassed Sentinel's predecessor, the Virtual Case File (VCF). The OIG recommended the FBI take the following steps:

- Replace the obsolete ACS system as quickly and as cost effectively as feasible.

- Reprogram FBI resources to meet the critical need for a functional case management system.

- Freeze the critical design requirements for the case management system before initiating a new contract and ensure that the contractor fully understands the requirements and has the capability to meet them.

- Incorporate development efforts for the VCF into the development of the requirements for any successor case management system.

- Validate and improve as necessary financial systems for tracking project costs to ensure complete and accurate data.

- Develop policies and procedures to ensure that future contracts for IT-related projects include defined requirements, progress milestones, and penalties for deviations from the baselines.

- Establish management controls and accountability to ensure that baselines for the remainder of the current user applications contract and any successor Trilogy-related contracts are met.

- Apply ITIM processes to all Trilogy-related and any successor projects.

- Monitor the Enterprise Architecture being developed to ensure timely completion as scheduled.

The report concluded that the difficulties experienced in completing the Trilogy project were partially attributable to: (1) design modifications the FBI made as a result of refocusing its mission from traditional criminal investigations to preventing terrorism, (2) poor management decisions early in the project, (3) inadequate project oversight, (4) a lack of sound IT investment practices, and (5) not applying lessons learned over the course of the project.

The National Research Council issued a report in May 2004 entitled *A Review of the FBI's Trilogy Information Technology Modernization Program*. The report found that the program was not on a path to success, and identified the following needs:

- valid contingency plan for transitioning from the old case management system to the new one,

- completed Enterprise Architecture,

- adequate time for testing the new system prior to deployment,

- improved contract management processes, and

- expanded IT human resources base.

The report concluded that the FBI had made significant progress in some areas of its IT modernization efforts, such as the modernization of the computing hardware and baseline software and the deployment of its networking infrastructure. However, because the FBI's IT infrastructure was inadequate in the past, there was still an enormous gap between the FBI's IT capabilities and the capabilities that were urgently needed.

The report was updated in June 2004 as a result of what the Council deemed clear evidence of progress being made by the FBI to move ahead in its IT modernization program. This included the appointment of a permanent CIO and the formation of a staffed program office for improved IT contract management. The progress being made by the FBI appeared to the Council to have been more rapid than expected, although many challenges remained. The Council also emphasized that the FBI's missions constitute increasingly information-intensive challenges, and the ability to integrate and exploit rapid advances in IT capabilities will only become more critical with time. The update concluded that even with perfect program management and execution, substantial IT expenses on an ongoing basis are inevitable and must be anticipated in the budget process if the FBI is to maximize the operational leverage that IT offers.

In September 2004, the GAO issued a report entitled, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements.* This report stated that although improvements were under way and more were planned, the FBI did not have an integrated plan for modernizing its IT systems. Each of the FBI's divisions and other organizational units that manage IT projects performs integrated planning for its respective IT projects. However, the plans did not provide a common, authoritative, and integrated view of how IT investments will help optimize mission performance, and they did not consistently contain the elements expected to be found in effective systems modernization plans. The GAO recommended that the FBI limit its near-term investments in IT systems until the FBI developed an integrated systems and modernization plan and effective policies and procedures for systems acquisition and investment management. Additionally, the GAO recommended that the FBI's CIO be provided with the responsibility and authority to effectively manage IT FBI-wide.

In April 2005, the House Surveys and Investigations staff issued *A Report to the Committee on Appropriations, U.S. House of Representatives*, which concluded the following.

- VCF development suffered from a lack of program management expertise, disciplined systems engineering practices, and contract management. The project also was affected by a high turnover of Chief Information Officers and program managers.

- VCF development was negatively impacted by the FBI’s lack of an empowered and centralized Office of Chief Information Officer and sound business processes by which IT projects are managed.

- The FBI’s decision to terminate VCF was related to deficiencies in the VCF product delivered, failure of a pilot project to meet user needs, and the new direction the FBI planned to take for its case management system.

- The FBI’s IT program management business structure and processes were, for the most part, in place, although some of these processes needed to mature.

FBI Internal Reports on Case Management

The FBI hired the Aerospace Corporation to perform an assessment of Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS) systems that could be used in developing a case management system and also an Independent Verification and Validation of Trilogy’s Virtual Case File. In December 2004, the contractor issued the *COTS/GOTS Trade Study*, which recommended that the FBI look to systems that have an emphasis on data sharing. The contractor further recommended that an acquisition strategy be developed that includes an incremental deployment of core capabilities and the incremental addition of such components as intelligent search and reporting and specific analytic capabilities.

The contractor released the *Independent Verification and Validation of the Trilogy Virtual Case File, Delivery 1: Final Report* in January 2005. The report recommended discarding the VCF and starting over with a COTS-based solution. The contractor concluded that a lack of effective engineering discipline had led to inadequate specification, design, and development of VCF. Further, the contractor could find no assurance that the architecture, concept of operations and requirements were correct or complete, and no assurance that they could be made so without substantial rework. In sum, the contractor reported that VCF was a system whose true capability was unknown, and whose capability may remain unknown without substantial time and resources applied to remediation.

Other OIG Reports on the FBI's IT

OIG reports issued over the past 15 years have highlighted issues concerning the FBI's utilization of IT, including its investigative systems. In 1990, the OIG issued a report entitled *The FBI's Automatic Data Processing General Controls*. This report described 11 internal control weaknesses and found that:

- The FBI's phased implementation of its 10-year Long Range Automation Strategy, scheduled for completion in 1990, was severely behind schedule and may not be accomplished;

- The FBI's Information Resources Management program was fragmented and ineffective, and the FBI's Information Resources Management official did not have effective organization-wide authority;

- The FBI had not developed and implemented a data architecture; and

- The FBI's major mainframe investigative systems were labor intensive, complex, untimely, and non-user friendly and few agents used these systems.

The OIG's July 1999 special report, *The Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation,* stated that FBI personnel were not well-versed in the ACS system and other databases. Additionally, a November 1999 OIG report entitled *A Review of the Justice Department's Handling of the Death of Kenneth Michael Trentadue at the Bureau of Prison's Federal Transfer Center in Oklahoma City*, noted deficiencies in uploading key evidence into the ACS.

A March 2002 OIG report entitled, *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case*, analyzed the causes for the FBI's belated delivery of many documents in the Oklahoma City bombing case. This report concluded that the ACS system was extraordinarily difficult to use, had significant deficiencies, and was not the vehicle for moving the FBI into the 21 century. The report noted that inefficiencies and complexities in the ACS, combined with the lack of a true information management system, were contributing factors in the FBI's failure to provide hundreds of investigative documents to the defendants in the Oklahoma City bombing case.

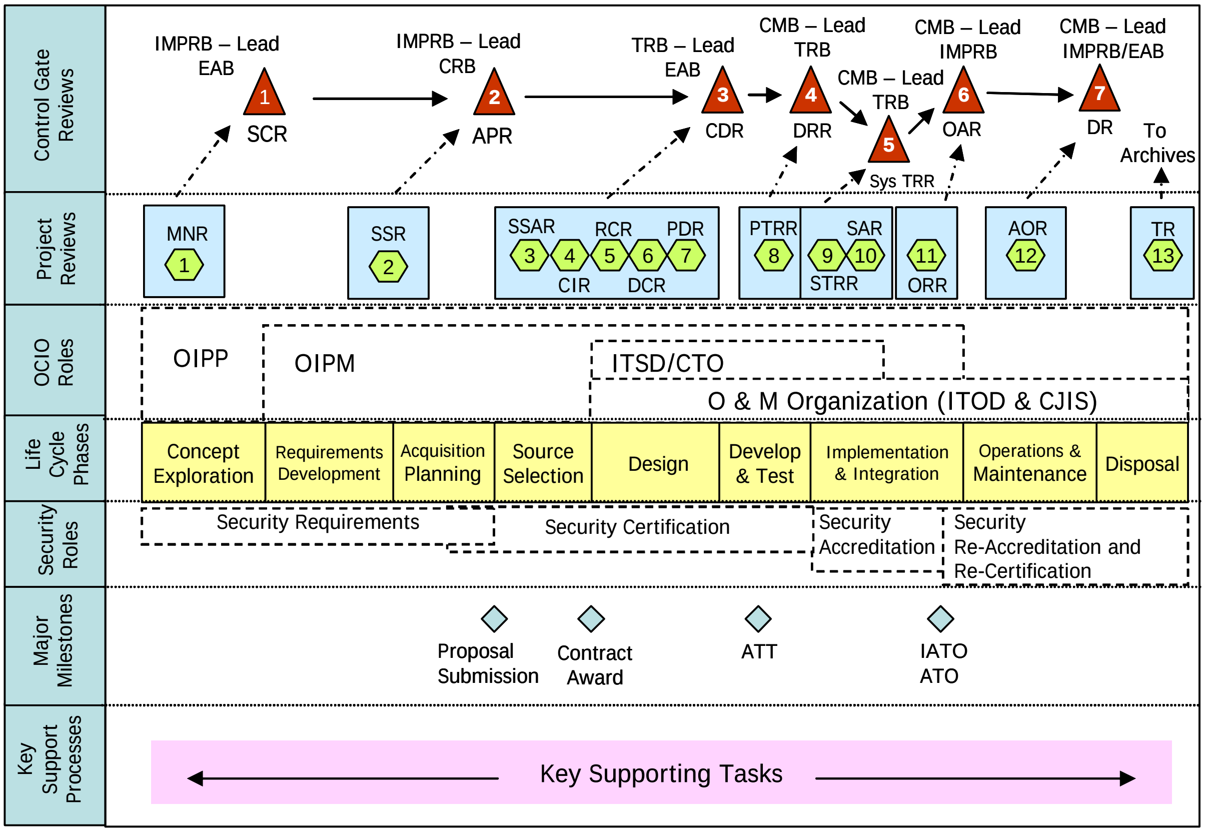
In May 2002, the OIG issued a report on the FBI's administrative and investigative mainframe systems entitled the *Independent Evaluation Pursuant to the Government Information Security Reform Act, Fiscal Year 2002*. The report identified continued vulnerabilities with management, operational, and technical controls within the FBI. The report stated that these vulnerabilities occurred because the Department and FBI security management had not enforced compliance with existing security policies, developed a complete set of policies to effectively secure the administrative and investigative mainframes, or held FBI personnel responsible for timely correction of recurring findings. Further, the report stated that FBI management had been slow to correct identified weaknesses and implement corrective action and, as a result, many of these deficiencies repeated year after year in subsequent audits.

In December 2002, the OIG issued a report on *The FBI's Management of Information Technology Investments*, which included a case study of the Trilogy project. The report made 30 recommendations, 8 of which addressed the Trilogy project. The report's focus was on the need to adopt sound investment management practices as recommended by the GAO. The report also stated that the FBI did not fully implement the management processes associated with successful IT investments. Specifically, the FBI had failed to implement the following critical processes:

- defining and developing IT investment boards,
- following a disciplined process of tracking and overseeing each project's cost and schedule milestones over time,
- identifying existing IT systems and projects,
- identifying the business needs for each IT project, and
- using defined processes to select new IT project proposals.

The audit found that the lack of critical IT investment management processes for Trilogy contributed to missed milestones and led to uncertainties about cost, schedule, and technical goals.

FBI'S LCMD IT SYSTEMS LIFE CYCLE



LEGEND

AOR	Annual Operational Review	MNR	Mission Needs Review
APR	Acquisition Plan Review	OAR	Operational Acceptance Review
ATO	Authority to Operate	ORR	Operational Readiness Review
ATT	Authorization to Test	PDR	Preliminary Design Review
CDR	Critical Design Review	PTRR	Product Test Readiness Review
CIR	Contract Implementation Review	RCR	Requirements Clarification Review
CMB	Change Management Board	SAR	Site Acceptance Review
CRB	Contract Review Board	SCR	System Concept Review
DCR	Design Concept Review	SSAR	Source Selection Authorization Review
DR	Disposal Review	SSR	System Specification Review
DRR	Deployment Readiness Review	STRR	Site Test Readiness Review
EAB	Enterprise Architecture Board	Sys TRR	System Test Readiness Review
FDR	Final Design Review Board	TR	Termination Review
IATO	Interim Authority to Operate	TRB	Technical Review Board
IMPRB	Investment Management Project Review Board		

APPENDIX 5

THE FBI LCMD KEY PROCESS AREAS

Key Process Areas	Purpose
Configuration Management (CM)	Establishes and maintains the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits.
Continuity of Operations Planning (COOP)	Provides plans for continuity of operations in the event of major crises.
Information Sharing	Maximizes information sharing across IT systems.
Enterprise Architecture (EA)	Develops and maintains the FBI IT architecture including the "as-is" and "to-be" (target) architectures and the transition plan for moving to the target architecture.
Information Security Management (ISM)	Establishes and applies safeguards within systems, processes, and organizations to protect data, software, and hardware from accidental or malicious modification, destruction, or disclosure.
Information Technology Investment Management (ITIM)	Provides the process for planning, selecting and controlling the IT resources required to effectively support the performance of the FBI operational and administrative mission areas.
Logistics Management (LOG)	Ensures that support considerations are an integral part of an IT system's requirements, design, implementation, and ongoing maintenance and that the infrastructure necessary for deployment and continued operational support of the system is identified, developed, and acquired.
Measurement and Analysis (MA)	Develops and sustains a measurement capability that is used to support management information needs.

Organizational Process Definition (OPD)	Establishes and maintains a usable set of organizational process assets.
Organizational Process Focus (OPF)	Plans and implements organizational process improvement based on a thorough understanding of the current strengths and weaknesses of the organization's processes and process assets.
Organizational Training (OT)	Develops the skills and knowledge of individuals so they can perform their roles effectively and efficiently.
Portfolio Management (PORT)	Manages the legacy IT system portfolio.
Process and Product Quality Assurance (PPQA)	Ensures the quality of the product or service and the processes used to create or provide them, and provides staff and management with objective insight into processes and associated work products.
Project Monitoring & Control (PMC)	Provides an understanding of the project's progress so that appropriate corrective actions can be taken when the project's performance deviates significantly from the plan.
Project Planning (PP)	Establishes and maintains plans that define project activities.
Records Management (RM)	Establishes and maintains effective plans, guidelines, and procedures for the collection, dissemination, organization, and protection of government records.
Requirements Development (RD)	Produces and analyzes customer, product, and product-component requirements.
Requirements Management (REQM)	Manages the requirements of the project's products and their components and identifies inconsistencies between those requirements and the project's plans and work products.

Risk Management (RSKM)	Identifies potential problems before they occur so that risk-handling activities may be planned and invoked as needed during the life of the product or project, to mitigate adverse impacts on achieving objectives.
Strategic Planning (SP)	Identifies FBI goals, objectives, and strategies to accomplish the FBI's mission and vision, guides annual budget and performance planning, and sets the framework for measuring progress and ensuring accountability.
Supplier Agreement Management (SAM)	Manages the acquisition of products from suppliers for which there exists a formal agreement.
Validation (VAL)	Demonstrates that a product or its component fulfills its intended use when placed in an intended environment.
Verification (VER)	Ensures that selected work products meet their specified requirements.

APPENDIX 6

PMO STAFF POSITIONS AND RESPONSIBILITIES

Program Leadership

The Sentinel program leadership consists of a program manager and a deputy program manager who are responsible for ensuring the overall success of the Sentinel project.

Direct Reporting Staff

The direct reporting staff includes the following:

- Contract Officer — oversees all Sentinel contract executions, including contractor task-order compliance, prepares change orders or other contract modifications as required, and also monitors contractual performance.

- Contract Officer Technical Representative — assists Contracting Officer in technical oversight.

- General Counsel — provides legal advice to the program manager and deputy program manager.

- Communications — assists the program manager in relaying program information.

Organization Change Management (OCM)

OCM is responsible for preparing Sentinel users to accept and utilize Sentinel's capabilities. OCM provides a formal path for receiving new user-originated requirements during the implementation of the system. The OCM team includes special agents, intelligence analysts, and professional staff who are on temporary duty assignments to the Sentinel program.

Business Management

The Business Management organizational unit develops and maintains program investments, budget, and spending plans. The team also monitors, analyzes, and reports on the program's Earned Value Management (EVM) status.

Administrative Support

The Administrative Support staff directs the administrative and support services required by the PMO.

Program Integration

The Program Integration staff is responsible for developing and maintaining the Sentinel project baseline and then tracking progress and risks against that baseline. This team is also responsible for coordinating external interfaces development plans and dependency schedules.

System Development.

The System Development staff is responsible for the overall system design and its implementation increments. This team is also responsible for the technical performance outcome of the Sentinel program and is accountable for the systems requirements and the delivery of a system whose technical performance meets users' expectations.

Transition

The Transition team is responsible for all activities associated with the transition of Sentinel phase capability from its development to eventual use by the FBI user community.

Operations and Maintenance

The Operations and Maintenance staff is responsible for the operations and maintenance of the deployed Sentinel capabilities until it reaches full operation capability. At which time this responsibility will be transferred to the FBI's Information Technology Operations Division.

APPENDIX 7

THE FBI'S RISK MITIGATION STRATEGY

Rank	Risk Condition	Risk Consequence	Mitigation Plan
1	There are a number of parallel initiatives within the FBI that can impact the scope of Sentinel	Parallel development efforts may result in changes to Sentinel functional content or interface requirements	M1. Monitor parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into Sentinel plans as appropriate
2	The project award schedule is very aggressive and the target award date may not be attainable	The target award slip delays identification of resources	M1. Develop the draft Request For Proposal M2. Develop OMB 300 M3. Establish schedule baseline
3	Sentinel increments must interface with numerous legacy systems operated outside the OCIO	The coordination and information required to develop the interfaces may consume significant, unforeseen schedule and resources	M1. Document external systems and interface requirements for inclusion in the solicitation M2. Establish a working partnership and collaborate with the legacy systems" owning organization
4	FBI mission evolves or user requirements change, resulting in scope creep prior to system completion	Funding and schedule will not support project completion	M1. Place the System Requirements Specifications (SRS) under configuration control prior to RFP release M2. Maintain strict requirements and configuration controls throughout the project M3. Ensure user advocacy group is the focal point for all user changes or needs M4. Ensure contractors are aware and adhere to change process, including communication with user community M5. Ensure FBI capabilities are addressed early in system development M6. Ensure continuous feedback with user community M7. Concurrence of SRS contents to be achieved by each division
5	Initial project costs are underestimated	Budgeted costs are not sufficient to complete project	M1. Establish the SRS early enough to serve as a baseline for the initial cost estimate M2. Perform a market survey of COTS and GOTS products to support baseline development M3. Generate multiple, independent cost estimates
6	Availability of staffing resources (prime and	Project plans, schedules, and scope	M1. Identify the government and support contractor resources, (and associated

	subcontractors) that meet FBI requirements may not be available when needed	will required modification; Sentinel vision prolonged or not achieved	timeline, skills, et al.) in the Sentinel Project Plan M2. Assess the realism of contractor staffing during source selection M3. Define security clearance requirements consistent with the access required by development contractor personnel, likely reducing the number of Top Secret security clearances required M4. Require staffing plan submission, with clearance status, in project review reporting M5. Ensure active government involvement
7	The development contractor may be unable to meet the proposed notional schedule	Delivery schedule will be delayed, having a cascading effect on project	M1. Evaluate realism of proposed schedules during source selection M2. Perform Integrated Baseline Reviews, as needed, to ensure that the government and contractor have a common understanding of the project baselines and risks M3. Use an integrated master schedule and regular status/remediation reporting to support schedule control M4. Implement Earned Value Management in accordance with ANSI/EIA Standard M7M4M8A M5. Hold weekly project status meetings and regular risk management meetings with the development contractor M6. Impose Resource Loaded Schedule (RLS) submission

APPENDIX 8

QUESTIONNAIRE USED TO DETERMINE THE MOST VIABLE CONTRACT VEHICLE

A. Contract Conditions

1. Are there specific limitations on the types of services or products that may be acquired?

2. Are there limitations on the dollar amount/percentage of services to computer hardware/software?

3. Are there specifics restrictions or terms/conditions on the purchase of computer hardware/software?

4. Describe the interagency fee structure. Is this fee structure flexible depending on the level of support required, or the amount of funds obligated?

5. What type of operating agreement will be put in place between the FBI and your agency?

6. Are there period of performance limitations that apply to this GWAC?

7. Can the contract/task order cross fiscal years or exceed 12-months?

8. Can the task order be incrementally funded?

9. How are interagency funds transfers handled?

10. What happens to funds that are not obligated?

11. Are there limitations/caps on the prime contractor rates charged under this vehicle?

12. What escalations factors are built into the rate structures?

13. Can labor categories be added to the contract?

14. Does the GWAC contracting officer periodically audit the prime contracts? If so, will the FBI receive a copy of the audit?

15. Are there any provisions in the GWAC contract that would preclude the FBI from conducting their own audits (e.g. timecards, invoices) at their discretion?

16. Are there maximum/minimum order limitations?

17. Are there any particular or unique terms and conditions of which the FBI should be aware?

18. What is the process for handling modifications? Are there limitations on the scope of changes?

B. <u>Government Roles and Responsibilities</u>

1. What services are provided by your agency both pre and post award?

2. Can we retain specific oversight of the contract post-award using FBI Contracting Officers?

3. Will you provide dedicated personnel responsible for this particular action?

C. <u>Source Selection</u>

1. Can the FBI perform an independent proposal evaluation using internal best value source selection procedures?

2. Can the FBI limit competition to certain primes based on the use of a white paper down-selection, an advisory multi-step process, or other FAR-compliant mechanisms?

3. Despite limited distribution of the RFP, are other primes able to submit a proposal even if they did not receive the RFP?

4. What will be your role in the source selection process?

5. Upon completion of the source selection how long will it take to award the contract?

D. Contractor Teams

1. What are the restrictions on adding additional primes or subcontractors?

2. Are there restrictions on the percentage of work that primes must perform versus subs?

3. Are there any restrictions on teaming arrangements? Are there any restrictions on prime contractors teaming with each other?

APPENDIX 9

GLOBAL JUSTICE XML DATA REFERENCE MODEL AND NATIONAL INFORMATION EXCHANGE MODEL

The Global Justice XML Data Reference Model (GJXDM) is an Extensible Markup Language (XML) standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner. The GJXDM removes the burden from agencies to independently create exchange standards, and because of its ability to cover a variety of sources, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system to system, GJXDM enables access from multiple sources and reuse in multiple applications.

The National Information Exchange Model (NIEM) is an "umbrella" model that synchronizes domain-specific models such as GJXDM. According to a Department of Justice system architect, the NIEM project vision is to develop a national enterprise-wide framework to facilitate information sharing across all levels of government in support of justice, public safety, intelligence, and homeland security thereby improving America's security, while respecting the privacy rights of citizens and the autonomy of external agencies and domains.

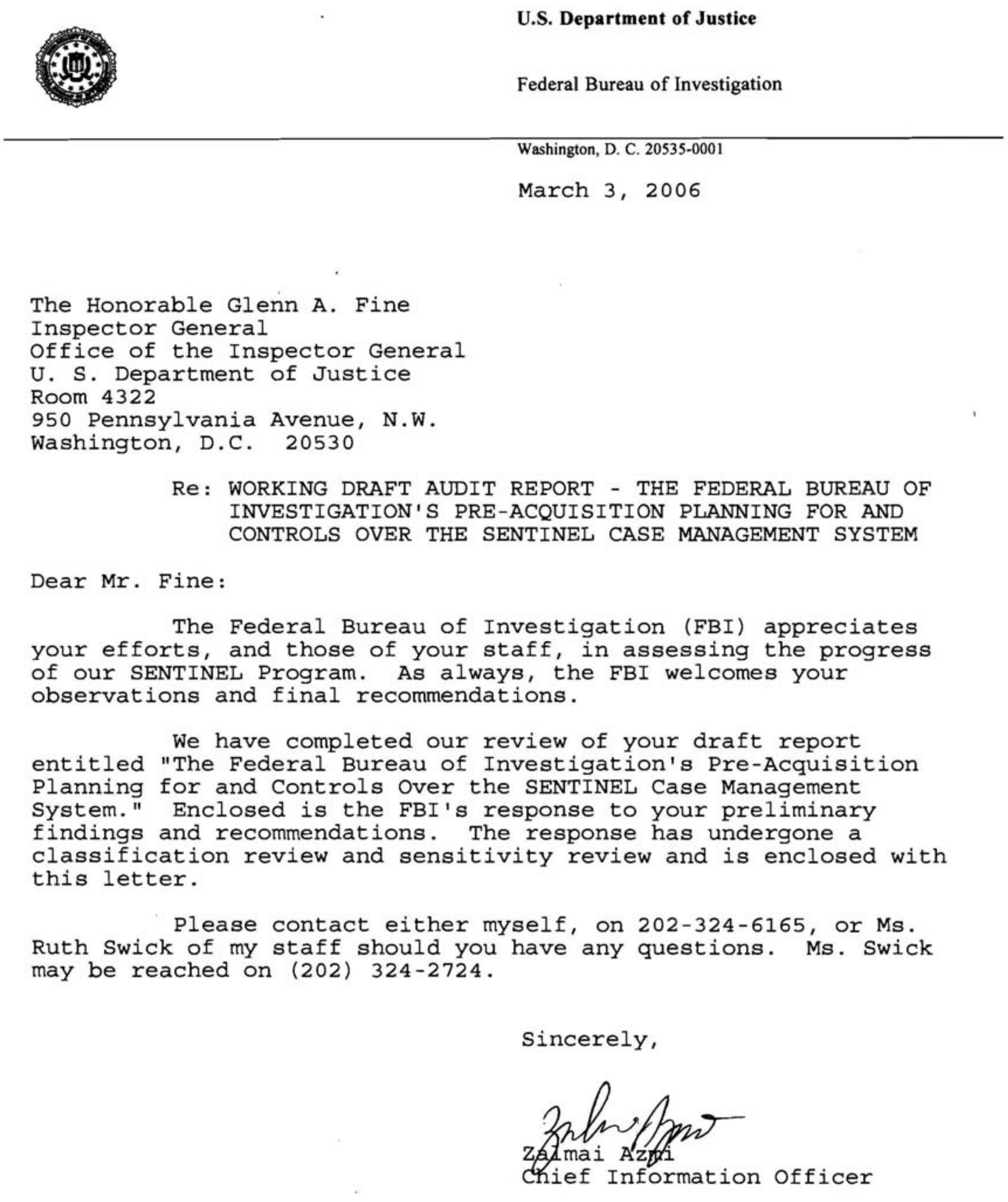
The GJXDM and NIEM models can make information exchange substantially more efficient by serving as guidance on how to document information. The models provide a standardized language where everyone understands what each term means as well as provide a vocabulary where people would be more likely to choose the same terms to describe the same thing. Upon that foundation, more specific standards are created for more specific kinds of information sharing, particularly for Sentinel and the Federal Investigative Case Management System (FICMS).

The various ways in which a FICMS system will exchange information must be identified and documented, and then exchange standards are built for each interface using GJXDM and NIEM. These exchange standards will define a significant portion of what FICMS is, in that compliance with these standards will be a necessary attribute of any FICMS system. In turn, these standards will be incorporated back into GJXDM and NIEM for reuse in other kinds of systems as appropriate.

The Department created the GJXDM by gathering approximately 16,000 data elements from 35 data dictionaries comprised of Department agencies as well as various local and state government sources. Currently, GJXDM consists of a defined and organized vocabulary of 2,754 reusable components.

APPENDIX 10

THE FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 3, 2006

The Honorable Glenn A. Fine
Inspector General
Office of the Inspector General
U. S. Department of Justice
Room 4322
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Re: WORKING DRAFT AUDIT REPORT - THE FEDERAL BUREAU OF INVESTIGATION'S PRE-ACQUISITION PLANNING FOR AND CONTROLS OVER THE SENTINEL CASE MANAGEMENT SYSTEM

Dear Mr. Fine:

The Federal Bureau of Investigation (FBI) appreciates your efforts, and those of your staff, in assessing the progress of our SENTINEL Program. As always, the FBI welcomes your observations and final recommendations.

We have completed our review of your draft report entitled "The Federal Bureau of Investigation's Pre-Acquisition Planning for and Controls Over the SENTINEL Case Management System." Enclosed is the FBI's response to your preliminary findings and recommendations. The response has undergone a classification review and sensitivity review and is enclosed with this letter.

Please contact either myself, on 202-324-6165, or Ms. Ruth Swick of my staff should you have any questions. Ms. Swick may be reached on (202) 324-2724.

Sincerely,

Zalmai Azmi
Chief Information Officer

FBI Response to the DOJ/OIG Working Draft Report
The Federal Bureau of Investigation's Pre-Acquisition Planning for and Controls Over the SENTINEL Case Management System

Recommendation # 1: Ensure that the system security and Independent Verification and Validation plans are completed as soon as possible after the contract is signed.

FBI Response: Concur. The SENTINEL Program Manager has assigned an Information Officer (ISSO) and Information System Security Manager (ISSM) to coordinate system security requirements with the prime developer. As the system security plan is dependent on the system design, the system security plan will not be finalized until the program's Critical Design Review (CDR), which will be determined when the schedule for the Phase 1 is finalized with the selected prime contractor.

Plans to obtain Independent Verification and Validation (IV&V) services from an independent contractor to support SENTINEL and other FBI projects are nearing completion. It is anticipated that an IV&V plan will be established during the design phase of development.

Recommendation # 2: Ensure that the SENTINEL Program Management Office is staffed to a level that will support SENTINEL's aggressive delivery schedule.

FBI Response: Concur. The Program Management Office (PMO) has an approved Staffing Plan (provided to the IG). The Program Manager (PM) continues hiring critical government employees and support service contractors as authorized by the staffing plan. As of February, more than two thirds of the program staff was in place, including all necessary staff to initiate contract award and commence Phase 1 development. Staffing of some of the SENTINEL transition and operations and maintenance positions was deferred until after commencement of development. PMO staffing is projected to be completed by June 2006.

Recommendation # 3: Obtain a tool that will allow for the effective implementation of an Earned Value Management process and fully implement this process.

FBI Response: Concur. The SENTINEL PMO is procuring a tool to effectively implement the Earned Value Management process, wInsight. wInsight provides ANSI compliant data transfer, analysis and reporting, enhance analysis, security, and reporting of EVMS data. SENTINEL PMO has already been providing EVM reports to DOJ/OMB concerning PMO contracts through the well-established IT Governance process including the DOJ Dashboard monthly reporting. The SENTINEL tool will be fully compliant with the enterprise IT Portfolio Tool, Metier Worklenz and Ms. Project Server. The Metier Worklenz and MS Project Server 2003 enterprise IT tool is in the final stages of being successfully certified and accredited with an Authority to Operate (ATO) by June 2006.

Recommendation # 4: Discuss with other intelligence community and law enforcement agencies their information sharing requirement to ensure compatibility with those systems in the requirements and design of SENTINEL.

FBI Response: Concur. We recognize the importance of information sharing and are working to ensure SENTINEL provides that capability. The PMO has a dedicated data architect working closely on this matter with the intelligence and law enforcement communities. We also participate—on a regular basis—with the FBI's Information Sharing Policy Board.

Recommendation # 5: Ensure that an effective system is in place to accurately track and control SENTINEL's development costs.

FBI Response: Concur. The FBI has already implemented steps to ensure that all costs are authorized in advance, verified when delivered, and validated when invoiced. The SENTINEL PMO has a dedicated Business Management Unit (BMU) to track, monitor and control all program and development costs, consisting of a government Business Manager, Budget Analyst, EVM Analyst, and is obtaining the services of a Cost Estimator. Additionally, the BMU has developed detailing invoicing procedures to validate all internal and external costs. A separate, dedicated cost code has been set up by the Chief Financial Officer (CFO) for SENTINEL within the OCIO (a first), which allows for SENTINEL, OCIO budget administration, and CFO teams to jointly track and control SENTINEL costs through a Budgetary Evaluation and Analysis Reporting System (BEARS) tool and oversight process.

Recommendation # 6: Complete a comprehensive SENTINEL training plan with realistic schedule and cost estimates and include these training estimates in the estimates of overall project costs.

FBI Response: Concur. SENTINEL has included extensive requirements in the Statement of Work for Organizational Change Management which includes training to all FBI staff at all locations including Legats. The development contractor is required to develop a SENTINEL training plan as part of their tasking. The FBI's cost estimates for SENTINEL already include funding for this activity.

Recommendation # 7: Establish a method to monitor the operational impact of a potential second reprogramming and identify for resolution any degrading of the FBI's mission-critical functions due to the diversion of funds to the SENTINEL project.

FBI Response: Concur. The FBI routinely evaluates the operational impact of any reprogramming. Those evaluations are included in the FBI's decision whether to submit a request to Congress for the necessary approval to reprogram resources. All reprogramming proposals include statements summarizing the impact on current operations, and the FBI provides additional detail to the Department of Justice, Office of Management and Budget, and Congress.

APPENDIX 11

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

Pursuant to the OIG's standard audit process, the OIG provided a draft of this audit report to the FBI on February 22, 2006, for its review and comment. The FBI's March 3, 2006, response is included as Appendix 10 of this final report. The FBI concurred with the seven recommendations in the audit report. Our analysis of the FBI's response to the seven recommendations is provided below.

Status of Recommendations

1. **Resolved.** In response to this recommendation, the FBI stated that steps are being taken to ensure that the system security and Independent Verification and Validation (IV&V) plans will be completed as soon as possible. Because the system security plan is dependent on the system design, the system security plan will not be finalized until the program's Critical Design Review. In the meantime, the Sentinel Program Manager has assigned an Information Officer and Information System Security Manager to coordinate system security requirements with the prime developer. For the IV&V plan, the FBI is nearing completion of its efforts to obtain the services of an independent contractor to support Sentinel and other projects. The FBI said it anticipates that an IV&V plan will be established during the design phase of development. This recommendation can be closed when we receive documentation demonstrating that the system security and IV&V plans have been completed.

2. **Resolved.** The FBI's response states that the Sentinel Program Manager continues hiring critical government employees and support service contractors as authorized by the Sentinel staffing plan. The FBI states that as of February 2006, more than two thirds of the program staff was in place, including all necessary staff to initiate the contract award and commence Phase 1 development of Sentinel. Full staffing is projected to be completed by June 2006, with some of the transition and operations and maintenance positions being deferred until after commencement of the project's development. This recommendation can be closed when we receive documentation demonstrating that the Sentinel Program Management Office is staffed to fully support Sentinel.

3. **Resolved.** In its response, the FBI stated that the Sentinel Program Management Office (PMO) is procuring a tool to effectively implement the Earned Value Management process, wInsight. According to the FBI, this tool will be fully compliant with the FBI's enterprise IT Portfolio Tool that is in the final stages of being certified and accredited by June 2006. This recommendation can be closed when we receive documentation demonstrating that the FBI has obtained and implemented a tool that will allow for the effective implementation of an Earned Value Management process.

4. **Resolved.** The FBI's response to this recommendation states that the Sentinel PMO has a dedicated data architect working with the intelligence and law enforcement communities on information sharing capabilities. This recommendation can be closed when we receive documentation demonstrating that the FBI has discussed with other intelligence and law enforcement agencies their information sharing requirements to ensure compatibility with those systems in the requirements and design of Sentinel.

5. **Resolved.** In its response, the FBI states that it has already implemented steps to ensure that all costs are authorized in advance, verified when delivered, and validated when invoiced. The Sentinel PMO has a dedicated Business Management Unit to track, monitor, and control all program and development costs. Additionally, a separate, dedicated cost code has been established by the FBI's Chief Financial Officer for Sentinel within the Office of the Chief Information Officer (OCIO) that allows for Sentinel, OCIO budget administration, and CFO teams to jointly track and control Sentinel costs through a Budgetary Evaluation and Analysis Reporting System tool and oversight process. This recommendation can be closed when we receive documentation demonstrating that the FBI has ensured that an effective system is in place to accurately track and control Sentinel's development costs.

6. **Resolved.** The FBI's response states that the FBI has included extensive requirements in Sentinel's Statement of Work for Organizational Change Management to include training of all FBI staff at all locations. The development contractor is required to develop a Sentinel training plan as part of its tasking, and Sentinel cost estimates already include this activity. This recommendation can be closed when we receive documentation demonstrating that a comprehensive training plan with realistic schedule and cost estimates has been developed and that the training cost estimate is included in overall Sentinel project costs.

7. **Resolved.** In response to this recommendation, the FBI said that it routinely evaluates the operational impact of any reprogramming. Such evaluations are included in the FBI's decision whether to submit a request to Congress for the necessary approval to reprogram resources, and all reprogramming proposals include statements summarizing the impact on current operations. This recommendation can be closed when we receive documentation on the FBI's method for monitoring the operational impact of a potential second reprogramming during Sentinel's development to identify for resolution any degrading of the FBI's mission-critical functions due to the diversion of funds to the Sentinel project.