REDACTED – PUBLIC VERSION

SENTINEL AUDIT II: STATUS OF THE FEDERAL BUREAU OF INVESTIGATION'S CASE MANAGEMENT SYSTEM

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

Audit Report 07-03
December 2006

REDACTED – PUBLIC VERSION

SENTINEL AUDIT II: STATUS OF THE FEDERAL BUREAU OF INVESTIGATION'S CASE MANAGEMENT SYSTEM*

EXECUTIVE SUMMARY

On March 16, 2006, the Federal Bureau of Investigation (FBI) announced that it had awarded a contract to Lockheed Martin Services, Incorporated (Lockheed Martin) to develop the Sentinel information and investigative case management system in 4 phases. The cost of the four phases of the Lockheed contract was $305 million, and the FBI estimated that it would cost an additional $120 million to provide various contractor support and staff the FBI's Sentinel Program Office, with the total estimated cost of Sentinel at $425 million. The initial schedule for the Lockheed Martin contract calls for all phases to be completed in December 2009.

The Sentinel project, which uses commercial off-the-shelf components, is intended to provide the FBI with an electronic information management system, automated workflow processes, search capabilities, and information sharing with other law enforcement agencies and the intelligence community. The FBI Director has stated, "Sentinel will strengthen the FBI's capabilities by replacing its primarily paper-based reporting system with an electronic system designed for information sharing. Sentinel will support our current priorities, including our number one priority: preventing terrorist attacks."[1]

Sentinel follows the FBI's unsuccessful 3-year, $170 million effort to develop a modern investigative case management system called the Virtual Case File (VCF) as part of the FBI's Trilogy information technology (IT) modernization project. The VCF, and now Sentinel, was intended to provide the FBI with a modern system so that the existing obsolete Automated Case Support (ACS) system could be retired. As detailed in the Office of the Inspector General's (OIG) February 2005 audit report on the FBI's Trilogy project, the VCF project failed for a variety of reasons, including poorly defined design

* THE FULL VERSION OF THIS REPORT INCLUDED INFORMATION THAT THE FBI CONSIDERED TO BE SENSITIVE PROPRIETARY INFORMATION. TO CREATE THIS PUBLIC VERSION OF THE REPORT, THE OIG REDACTED (DELETED) THE SENSITIVE PORTIONS AND NOTED THAT THE INFORMATION WAS REDACTED.

[1] FBI Press Release entitled *FBI Announces Award of Sentinel Contract*, March 16, 2006.

requirements, lack of mature Information Technology Investment Management (ITIM) processes, and poor management continuity and oversight.[2]

The Sentinel contract, awarded to Lockheed Martin through a Government-Wide Acquisition Contract (GWAC), is a cost-plus-award-fee contract that uses task orders to complete work for each phase of the project.[3] While this type of contract proved problematic under Trilogy, we have found that the FBI has made considerable progress in establishing controls and processes required to adequately manage a major IT development project such as Sentinel and to bring it to a successful conclusion – if the processes are followed and controls are implemented as intended.

The OIG performed this audit of the Sentinel project at the request of the FBI Director and congressional appropriations and oversight committees. This audit is the second in a series of audits that the OIG intends to conduct, as Sentinel progresses, to evaluate the progress and implementation of Sentinel. The first audit, issued in March 2006, assessed the FBI's pre-acquisition planning for and controls over Sentinel.

The objective of this second audit was to determine: (1) the progress the FBI has made in resolving the concerns identified in our first report on the planning for Sentinel, and (2) if the contract with Lockheed Martin and the FBI's ITIM processes and project management are likely to contribute to the successful implementation of Sentinel. Our future audits will examine the progress of Sentinel over its four phases and assess whether cost, schedule, performance, and technical benchmarks are being met.

Background of Sentinel

A major objective of the FBI's IT modernization project is to replace the FBI's antiquated ACS system. 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.

---

[2] 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.

[3] An award fee is a financial incentive provided to a contractor based on the contractor's performance.

The FBI expects that Sentinel will provide it with a web-enabled case management system that includes records management, workflow management, 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 over 45 months, with each phase providing distinct capabilities until the overall project is completed in December 2009. The FBI expects to complete each of the phases in 12 to 16 months, with the phases overlapping by 1 to 2 months. For example, Phase 2 will begin about 2 months before Phase 1 is completed.

According to the FBI, the four phases will provide the following capabilities.

- Phase 1 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 2 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 3 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 4 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.

We reviewed the progress the FBI has made since our March 2006 report, the requirements of the Sentinel contract, the FBI's

application of its ITIM processes through its Life Cycle Management Directive (LCMD), and the controls the FBI has established over the Sentinel project to help avoid the problems the FBI encountered with the Trilogy project.

We found that the FBI has resolved most of the concerns we identified in our first Sentinel audit, although some aspects of those concerns as well as some new concerns identified in our current audit bear continued monitoring. Specifically, the FBI has made progress in: (1) establishing cost tracking and control processes, (2) implementing an Earned Value Management (EVM) system to help measure progress toward project baselines, (3) developing plans for the Independent Verification and Validation (IV&V) of the system software to ensure it will operate as intended, (4) developing information sharing capabilities, and (5) hiring more Program Management Office (PMO) staff.

Among the areas warranting continued monitoring by the FBI, the OIG, and other oversight entities are the: (1) funding of the Sentinel project and the effect on the FBI's operations or other FBI projects of any reprogramming of funds that might be required (2) accuracy of the estimated cost of the project, (3) availability of contingency plans for identified project risks, and (4) completion of Sentinel PMO staffing.

In sum, the project is still in its early stages and has not yet reached the most difficult phases. However, we believe that the processes the FBI has established to manage and control the Sentinel project – if implemented and carefully followed as Sentinel develops – can provide reasonable assurance that Sentinel can be successful and that any deviations from cost, schedule, technical, or performance baselines can be identified.

Sentinel Contract

The FBI awarded to Lockheed Martin a cost-plus-award-fee contract through a National Institutes of Health government-wide acquisition contract (GWAC).[4] Actual work under the contract will occur project phase by project phase through task orders.[5] The cost

[4] The development contract under the GWAC is cost-plus-award-fee. However, all materials are cost-plus-fixed-fee and travel is cost reimbursable only.

[5] A task order specifies the services required and the negotiated terms at which they will be provided, subject to the terms of the contract.

of the task order for Phase 1 of Sentinel is $57 million. According to the contract, the FBI may exercise options for $248 million to cover three additional phases of the project plus operations and maintenance. Therefore, the total contract with Lockheed Martin could total $305 million. According to the contract, Lockheed Martin can also be rewarded for meeting established goals in four areas: project management, cost management, schedule, and technical performance. The award fee cannot exceed [redacted] percent of the $232.4 million total development costs for Sentinel, or approximately $26 million, and will be allocated across the four areas based on risk. This type of contract and award fee structure is common for large government IT projects.

In our 2005 report on the FBI's Trilogy project, we described 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. With regard to the Sentinel contract, the FBI is establishing clear milestones and requiring critical decision review points. If the contractor does not meet its milestones, it will be penalized by loss of the award fee.

Progress in Addressing the OIG's Past Concerns

The FBI has made good progress in addressing the concerns we identified in our March 2006 audit report. As we describe in the following sections, our audit found that although some concerns remain, the FBI has: (1) hired or selected staff to meet current vacancies for the Sentinel PMO and has had management stability, (2) required that Sentinel meet a new joint Department of Justice and Department of Homeland Security information sharing standard, which will allow Sentinel to communicate with other systems built to the standard, (3) established an EVM system to monitor the Sentinel project's costs and schedule, (4) established layers of review, approval, and reporting for Sentinel spending, and (5) completed plans for the IV&V of Sentinel's software to ensure it will perform as intended.

Staffing

The FBI has made progress in staffing the Sentinel PMO since our first report. Of a total planned staff of 73, as of October 2006, 65

positions had been filled compared to 51 in March 2006.[6] The FBI said it has intentionally delayed filling six of the vacant positions until the second phase of Sentinel. Two other positions remain vacant, an intelligence analyst and a planner. The Chief of the Business Management Unit said the PMO has taken steps to expedite hiring, including interviewing applicants who had applied to an FBI-wide job announcement for computer scientists.

Information Sharing

In our March 2006 report, we expressed concerns that the FBI was focused on sharing information within the FBI but had not paid sufficient attention to Sentinel's ability to share information with other law enforcement and intelligence agencies' systems. Since that report, the FBI has focused more attention on external information sharing needs and has been coordinating with the Departments of Justice and Homeland Security and other federal entities, including the Drug Enforcement Administration, Immigration and Customs Enforcement, and the Office of the Director of National Intelligence. Sentinel will be built to meet the standards of the new National Information Exchange Model, a joint Department of Justice and Department of Homeland Security standard, which is also supported by the Director of National Intelligence. When finalized, the standard will become the government-wide standard for any new law enforcement and intelligence systems being developed.[7] However, the standard is still evolving, and Sentinel's design may have to be modified as the standard evolves.

Earned Value Management

EVM is a tool that measures the performance of a project by comparing the variance between established cost, schedule, and performance baselines with what is actually taking place. These variances are measured periodically to give project managers a perspective on the status of a project and an early warning if a project

[6] The number of filled positions includes three candidates who had accepted positions and were in the process of being hired.

[7] The Sentinel statement of work, which was developed prior to the release of the draft National Information Exchange Model, requires Sentinel to be built to the Global Justice XML Model. However, the Sentinel Program Manager said that Sentinel's design will ultimately conform to the new National Information Exchange Model standards.

is heading for trouble. EVM reporting is an important risk-management tool for a major IT development project.

The FBI and Lockheed Martin have implemented EVM systems in accord with Office of Management and Budget (OMB) requirements to track and validate Sentinel project costs throughout the life of the project. In addition to data provided by Lockheed Martin, the FBI's EVM system relies on cost data provided through invoices from support services contractors and the FBI's Budget Execution and Analysis Reporting System, which extracts purchase order information from the FBI's Financial Management System and generates reports on funds requested, amounts approved and spent, and obligations that have not yet entered the FBI's overall Financial Management System. The FBI is required to report to the OMB any net cost or schedule variations by the FBI and the contractor that meet a reporting threshold.

The FBI is using the EVM system to help manage project risks by providing an early warning of unexpected costs and problems that could delay Sentinel's completion. We are monitoring the FBI's EVM reporting to identify any unexplained growth in overall project costs or any schedule delays. Three early EVM reports indicated some variances, but the variances were due to estimating errors by the contractor, which have been corrected.

Cost Tracking and Controls

The OIG's prior reviews of the Trilogy project found that the FBI lacked an effective, reliable system to track and validate the Trilogy project's costs. In our current audit work, we found that in addition to EVM reporting, the FBI has established controls to help ensure that Sentinel expenditures are authorized in advance and that items are verified when delivered and validated when invoiced. For example, the FBI has developed a system of overlapping responsibilities for the oversight of Sentinel's costs that include: accounting, auditing, and budget monitoring by the FBI's Finance Division; detailed tracking of Sentinel's costs by the Office of the Chief Information Officer's IT Financial Management Unit; and tracking and controlling program and development costs and developing policies and procedures for processing invoices, requisitioning and procuring equipment, reviewing contractor time charges, and resolving discrepancies by the Sentinel PMO Business Management Unit. We believe that the tracking systems and controls the FBI has implemented will allow the FBI to be better monitor and control project costs for Sentinel than was the case under Trilogy.

Documentation Required by ITIM Processes

Although the FBI had established sound IT investment management processes through its Life Cycle Management Directive (LCMD), we noted in our last report on Sentinel that two key plans had not yet been developed because the project design had not been completed: IV&V and the system security plan. The IV&V process provides an independent control to monitor the testing of the system software and ensure it functions as intended. The FBI's Chief Information Officer (CIO) recently told us that the FBI awarded its IV&V contracts to eight vendors and that it had awarded a task order to Booz Allen Hamilton to monitor Lockheed Martin's testing of the system software during the development of the Sentinel system.[8]

A system security plan is also critical to help ensure that Sentinel will meet the FBI's security standards and can be certified and accredited for use within the FBI's operating environment. The CIO recently told us that the security plan has been drafted and is in the approval process.

In accordance with the FBI's LCMD, the final design for the first phase of the Sentinel project will occur in October 2006. However, because Lockheed Martin will be using off-the-shelf components to develop Sentinel, the complication and risk of the project design should be lessened, although configuring all of the components into one seamless system will remain a greater challenge. The FBI stated that it will conduct future planning, including requirements verification, prior to the initiation of subsequent phases in order to solidify the design and deliverables for each phase

Current Concerns

The FBI has made strides in resolving most of the concerns discussed in our March 2006 audit report, although some aspects of those concerns remain. Also, in our current audit work we have identified additional concerns that warrant continued monitoring by both the FBI and the OIG. One concern carries over from our previous report – the possibility of a reprogramming of the FBI's non-IT funds to cover fiscal year 2007 Sentinel expenses, which may have an adverse affect on the FBI's mission capabilities. In addition, we were

[8] At the time our audit, the specific IV&V activities for Sentinel had not been determined. However, IV&V may include oversight of program management processes and assessments related to the development contractor's performance.

unable to validate the FBI's cost estimate for Sentinel, and we found that the FBI lacks contingency plans for all of the highly rated project risks it has identified.

Project Funding and Reprogramming

We found that the FBI faces uncertainty over the source of the approximately $150 million the FBI says it needs in fiscal year (FY) 2007 to continue the Sentinel project. The President's FY 2007 budget request includes $100 million for Sentinel, and the FBI would need an additional $56.7 million to bridge the gap between the requested funds and its FY 2007 requirements for Sentinel. The FBI expects to have about $50 million remaining from the first phase of Sentinel and prior year unexpended balances from other sources. Moreover, the FBI's CIO recently told us that an FY 2007 appropriation of less than $100 million would be cause for concern and could result in an unanticipated level of reprogramming of FBI resources to fund the Sentinel project. In our judgment, any reprogramming significantly above $50 million will require the FBI to carefully consider which programs and activities will be affected and how to monitor the overall impact on the FBI's mission.

As we reported in our first Sentinel audit, various FBI managers told us that a second reprogramming of FBI funds similar in size to the $97 million reprogramming that occurred in November 2005 could erode the FBI's mission capability in counterterrorism, cybercrime, and other important operational areas. Therefore, until the funding issues are addressed, we remain concerned about the impact that reprogramming significant amounts of non-IT funds to support Sentinel would have on other critical FBI priorities.

With respect to total project costs, the FBI CIO told us that he stands by the FBI's estimate that the full cost of Sentinel will be $425 million, with $305 million to cover work by Lockheed Martin on a variety of task orders and an additional $120 million to cover costs such as staffing the FBI's Program Management Office, contractor support, and management or risk reserve for contingencies. Training costs are included in the Lockheed Martin portion of the estimate, which was a concern we noted in our last Sentinel report when the FBI had not yet developed a complete cost estimate for its training plans.

Cost Estimates

We reviewed the processes used to derive the $425 million cost estimate for the Sentinel project, noted some inconsistencies in the process and the results, and concluded that the estimate is a rough approximation of Sentinel's overall costs. The estimate is, in our view, tentative given the variances in the supporting cost estimates and the inherent complexity of estimating costs for a major IT system before the design is finalized.

In examining the underlying estimates for the overall project cost, we are unclear as to whether the initial cost estimate accurately included the project's operations and maintenance costs through FY 2011. We found that some portions of the estimate provide costs for 2 years, while other portions include costs for 3 years. Another estimate showed significant disparities in Lockheed Martin's labor costs. Variations in the estimates of Sentinel's projected costs demonstrate the difficulty of estimating the cost of such a complex information technology project at its outset.

Because of these estimation difficulties, and because the project is in its early stages, we could not validate the FBI's overall estimate of $425 million for Sentinel, and we believe that the ultimate cost could be lower or higher. We noted that the overall management reserve for the project – a budgeted amount to cover any unanticipated expenses – currently amounts to about 15 percent of Sentinel's development costs. The Sentinel Program Manager told us that based on his experience, an 11 percent reserve would be adequate (the difference amounts to about $8.6 million). The FBI expects to adjust the amount of the reserve so that over the length of the project the reserve will equal 11 percent of the development cost. As the FBI finalizes Sentinel's design and gains experience with actual project costs, the FBI should regularly update its estimate of the overall project costs to keep Congress and the Department informed. In addition, we intend to continue to monitor the cost of the project as it progresses.

In addition to the Sentinel project cost estimates, we identified costs that could be considered as associated with Sentinel but are separate projects and therefore not included as part of Sentinel's projected $425 million cost. For example, the implementation of Sentinel will require changes to the FBI's National Name Check system. In response to a request from a federal, state, or local agency, the National Name Check Program queries FBI records to

determine whether the person named in the request has been the subject of an FBI investigation or mentioned in an FBI investigation. The data system used by the program relies very heavily on the ACS system, which Sentinel is intended to replace. The estimated cost of updating the existing name check system to work with Sentinel is over [redacted]. In addition, the FBI has ongoing agency-wide security efforts that will benefit Sentinel. If these separate projects were included as Sentinel costs, the $425 million cost estimate could be at least $25 million higher.

The FBI's position is that these separate projects are enterprise-wide endeavors that will benefit the FBI's overall IT structure, including Sentinel but also many other FBI systems. The CIO and the Sentinel Program Manager contend that these other projects were initiated on their own merits, would be undertaken regardless of Sentinel, and their costs ought not be considered as Sentinel costs. While we agree that these Sentinel-related projects may not be direct Sentinel costs, in our view the scope of the Sentinel project would be larger if it was not supported by these other investments.

Risk Management

The purpose of risk management is to assist the project 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. Risks are categorized by severity and identified as either open or resolved. Open risks are tracked until resolved.

The FBI has created a list of 20 risks associated with the Sentinel project that it is monitoring. While the FBI's establishment of a risk management program is a positive step, contingency plans, and the triggers for activating such plans, currently exist for only three risks – including only one of the top five risks. The Program Manager told us that in some cases it is difficult to develop a contingency plan before the FBI's preventive actions mitigate the likelihood or severity of the risk or before the risk. He explained that the focus is on preventing problems that would rise to the level of requiring mitigation, and that if a problem occurs, a corrective action will be developed. He also told us that many risks are temporary and as a project phase progresses, the risk may become moot and is closed. However, we believe the FBI should have a plan for risks that have the potential to result in a

significant cost, schedule, or performance deviation from the project baselines.

With respect to currently identified project risks, we view the FBI's ability to successfully migrate data from the antiquated ACS system to Sentinel as a potentially significant challenge. If the migration were to fail or be seriously delayed, the FBI would need to try maintaining its legacy ACS system with all of its flaws. An inability to migrate the ACS data would also result in a Sentinel system that builds its data from the present day forward, without the benefit of years of investigative data compiled in the old system. Further, should ACS cease to be maintainable, that data could effectively be lost. The Sentinel Program Manager told us that the task of "cleaning" and reconciling the ACS data for migration into Sentinel is not technically difficult and the FBI plans to use an available software tool for that purpose. However, he pointed out that it will take a significant amount of work to accomplish. He also said that as a preventative measure intended to eliminate any delays in the overall project due to data cleansing, the FBI plans to cleanse data in the phase preceding the phase in which the data will be transferred to Sentinel.

Another potential risk is the extent to which Sentinel will actually use commercial-off-the-shelf software modules as intended. A high degree of customization of the software could result in increased costs and schedule delays. The Program Manager told us that the components for Sentinel are all off-the-shelf and little or no customization is anticipated. However, the key task will be configuring Sentinel's various applications – such as the workflow, document management, searching and reporting, and electronic signatures – to all work together. The Program Manager noted that Lockheed Martin has successfully configured similar systems in other major projects, using some of the same software modules, including one at the Social Security Administration.

IT Investment Management Processes

In November 2004, the FBI established its IT investment management processes through its LCMD, 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.

The LCMD has established nine phases that occur during the development, implementation, and retirement of IT projects: (1) concept exploration, (2) requirements development, (3) acquisition planning, (4) source selection, (5) design, (6) development and testing, (7) implementation and integration, (8) operations and maintenance, and (9) retirement.[9] As of August 2006, the Sentinel project had passed through the first four life cycle phases and is currently in the fifth phase – Design.

During the life cycle phases, specific requirements must be met for the project to obtain the necessary FBI management approvals to proceed to the next life cycle phase. The approvals occur through control gates, where FBI management boards meet to discuss and approve or disapprove a project's progression to future phases of development or implementation. The 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 Sentinel project has received management approval for the first two of the LCMD control gates: the system concept on July 15, 2005, and the acquisition plan on July 29, 2005. As of September 2006, the Sentinel program had not requested or received approval for the third control gate. According to the Sentinel Program Manager, Phase 1 of the Sentinel project is scheduled to pass through Control Gate 3, the Final Design Review, in late October 2006. 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.

[9] The life cycle phases are not to be confused with the Sentinel project's four development phases.

Conclusions

By establishing stronger IT investment management processes and an array of monitoring and control mechanisms, the FBI has positioned itself to better manage the Sentinel project and avoid the problems that occurred in the Trilogy and VCF projects. However, FBI officials agree this does not mean that the development of Sentinel is risk-free. While the FBI has corrected or alleviated most of the concerns we raised in our March 2006 audit report on Sentinel, several areas warrant attention to avoid potentially serious problems as the project progresses:

- the ability to fully fund the project and, if required, reprogram funds without adversely affecting other FBI mission-critical operations,
- monitoring and adjusting as necessary the estimates of total project costs,
- developing contingency plans for high-risk areas that could affect project costs, schedule, or performance, and
- completely staffing the PMO.

In future audits, we will continue to monitor Sentinel's progress and whether the project is meeting the cost, schedule, technical, and performance baselines.

OIG Recommendations

In this second Sentinel audit, we make five recommendations to the FBI to help ensure the success of the Sentinel case management system and manage project costs. The recommendations are:

- Ensure the management reserve is based on an assessment of project risks for each phase and for the project overall.
- Periodically update the estimate of total project costs as actual cost data is available.
- Complete contingency plans as required by the Sentinel Risk Management Plan.

- Ensure that the independent verification and validation process is conducted through project completion.

- Complete hiring as soon as possible for the vacant PMO positions needed during the current project phase.

TABLE OF CONTENTS

INTRODUCTION

Background

On March 16, 2006, the Federal Bureau of Investigation (FBI) announced that it had awarded a contract to Lockheed Martin Services, Incorporated (Lockheed Martin) to develop the Sentinel information and investigative case management system in 4 phases. The cost of the four phases of the Lockheed Martin contract was $305 million, and the FBI estimated that it would cost an additional $120 million to staff the FBI's Sentinel Program Office, provide contractor support, and establish a management reserve for contingencies, with the total estimated cost of Sentinel at $425 million. The initial schedule for the Lockheed Martin contract calls for all phases to be completed in December 2009, or 45 months from the start of work.

According to the contract, Lockheed Martin can be rewarded for meeting established goals in four areas: project management, cost management, schedule, and technical performance. The award fee cannot exceed [redacted] percent of the $232.4 million total development costs for Sentinel, or approximately $26 million, and will be allocated across the four areas based on risk. This type of contract and award fee structure is common for large government IT projects.

The Sentinel project, which uses commercial-off-the-shelf (COTS) components, is intended to provide the FBI with a web-enabled electronic case management system that includes records management, workflow management, evidence management, search and reporting capabilities, and information sharing capability with other law enforcement agencies and the intelligence community. According to the FBI Director, "Sentinel will strengthen the FBI's capabilities by replacing its primarily paper-based reporting system with an electronic system designed for information sharing. Sentinel will support our current priorities, including our number one priority: preventing terrorist attacks."[10]

The Sentinel project follows the FBI's unsuccessful efforts to develop an automated case management system called the Virtual

[10] FBI Press Release entitled *FBI Announces Award of Sentinel Contract*, March 16, 2006.

Case File (VCF), which was intended to replace the FBI's 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. Given 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 continually review and report on the progress of the FBI's development of Sentinel.

This report is the second OIG report on Sentinel, and covers the progress the FBI has made in resolving the concerns identified in our March 2006 report on the planning for Sentinel, whether the FBI's Information Technology Investment Management (ITIM) processes and project management are likely to contribute to the successful implementation of Sentinel, and the contract with Lockheed Martin to develop 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 received to accelerate completion of 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. Based on critical comments by these organizations, 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 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 VCF, issued in January 2005, which recommended that the FBI pursue a COTS-based, service-oriented architecture.[11] 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 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.[12] According to the report, the FBI terminated work on the VCF

---

[11] IV&V is a standard ITIM process whereby an independent entity assesses the system as it is developed in order to evaluate if the software will perform as intended. 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.

[12] 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.

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. The FBI has said that of the $170 million VCF project, $104.5 million was lost but that $53.3 million in contractor services and equipment could be used and $12.2 million was unspent.[13]

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.[14] 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 economical and efficient changes to software components as needed in the future. According to the FBI, a key element of the Sentinel architecture contributing to achieving this flexibility will be the use of COTS and GOTS applications software. The FBI intends to integrate the off-the-shelf products with an Oracle

---

[13] The OIG has not verified these figures, including the services and equipment the FBI said could be reused.

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

database, thereby separating the applications code from the underlying data being managed in order to simplify 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 currently 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, and provides references to 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, ACS is a severely outdated system that is cumbersome to use effectively and does not facilitate the searching and sharing of information. The limited capabilities of the ACS mean that agents and analysts cannot easily acquire and link information across the FBI.

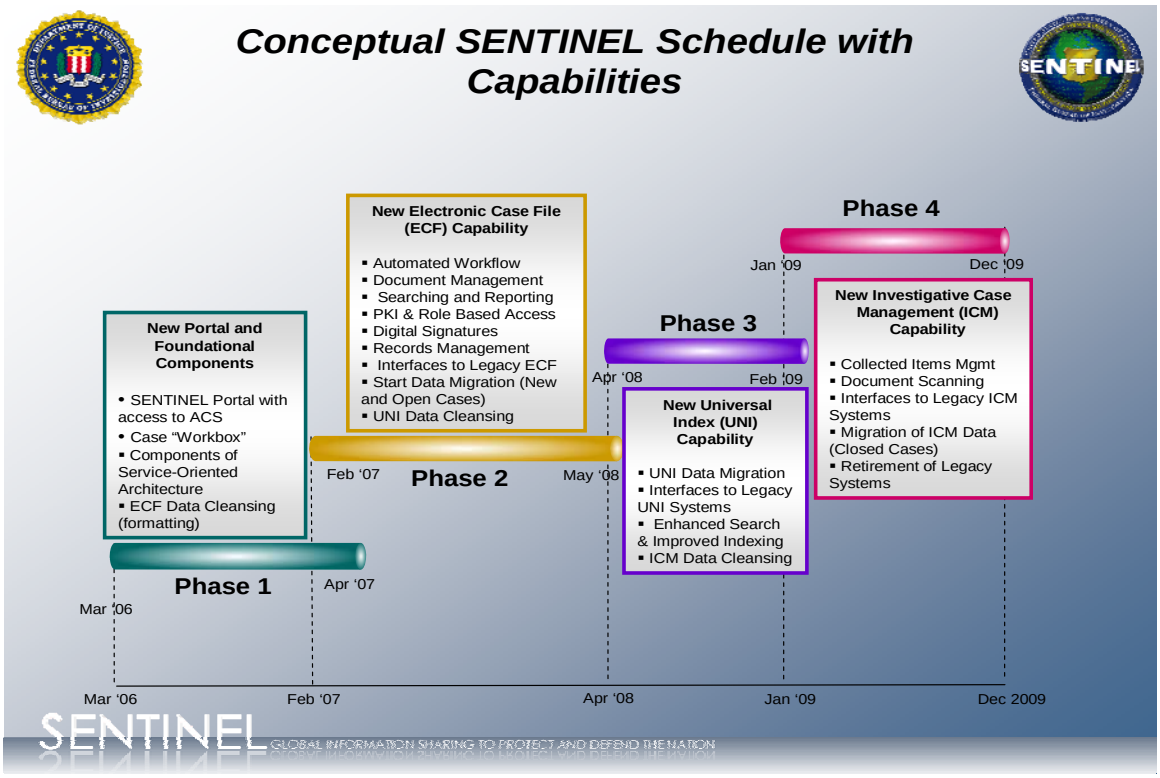
In contrast, the FBI expects Sentinel to greatly enhance the usability of case files for agents and analysts, both in terms of adding information to case files as well as searching for case information. FBI supervisors, reviewers, and others involved in the approval process also will be able to review, comment, and approve the insertion of documents into appropriate FBI electronic 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 federal government's 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 the Department of Homeland Security (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 for their case management systems 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 phases, each with an approximately 12- to 16-month timeframe and overlapping by 1 to 2 months. For example, Phase 2 is anticipated to begin approximately 2 months before the end of Phase 1. 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.



Source: FBI

Phase 1 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 1 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 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 hardware and software that will form the foundation of Sentinel's future service oriented architecture. Finally, the FBI will prepare the data in the Electronic Case File portion of ACS to be migrated to Sentinel in Phase 2.

Phase 2, the most ambitious and difficult of the phases, will begin the transition to paperless case records and the implementation of electronic records management. A workflow tool will support the flow of electronic documents through the review and approval cycles. A new security framework will be implemented to support access controls and electronic signatures. Additionally, the FBI will begin

migrating data from the Electronic Case File to Sentinel and preparing data from the Universal Index to be migrated to Sentinel in Phase 3.

Phase 3 will replace the Universal Index (UNI), which is used to determine if any 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 an investigative case. While the current UNI supports only a limited number of attributes, Phase 3 will expand the number of attributes within the information management system.[15] Improving the attributes will allow more precise and comprehensive searching within Sentinel and increase the ability to "connect the dots."

Phase 4 will implement Sentinel's new case management and reporting capabilities, and will consolidate the various case management components into one overall system. Shortly after 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.

Earned Value Management System

Earned Value Management (EVM) is a tool that measures the performance of a project by comparing the variance between established cost, schedule, and performance baselines and what is actually taking place. These variances are measured periodically to give project managers a timely perspective on the status of a project. EVM then can provide an early warning that a project is heading for trouble. EVM reporting is an important risk-management tool for a major IT development project such as Sentinel.

In August 2005, the OMB issued a memorandum requiring all federal agency CIOs to manage and measure all major IT projects using an EVM system. Additionally, all agencies were to develop policies for full implementation of EVM on IT projects by December 31, 2005. In response to these requirements, the FBI developed a Sentinel Program EVM Capability Implementation Plan in August 2005

[15] An attribute defines a property of an object within a case file. Examples of attributes are eye color, height, and nationality when describing an individual or address, floor, and room number when describing a specific location.

and subsequently acquired a tool to implement an EVM system for the Sentinel project.

The OMB EVM memorandum also required that Integrated Baseline Reviews (IBRs) be performed for any projects that require EVM in order to establish performance management baselines against which a project's performance can be measured.[16] Properly executed, IBRs are an essential element of a program manager's risk-management approach. IBRs are intended to provide both the government's and the contractor's program managers with a mutual understanding of the project's performance measurement baseline and agreement on a plan of action to resolve the identified risks. According to OMB guidance on IBRs, the objective of an IBR is to confirm compliance with the following business rules:

- the technical scope of work is complete and consistent with authorizing documents;
- key schedule milestones are identified;
- supporting schedules reflect a logical flow to accomplish the technical work scope;
- resources, including money, facilities, personnel, and skills, are adequate and available for the assigned tasks;
- tasks are planned and can be measured objectively, relative to technical progress;
- underlying performance measurement baseline rationales are reasonable; and
- managers have appropriately implemented required management processes.

[16] The performance measurement baseline is a total, time-phased budget plan against which program performance is measured.

Prior Reports

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

In March 2006, the OIG released the first in a series of audit reports that will monitor the FBI's development and implementation of the Sentinel project.[17] This report discussed the FBI's pre-acquisition planning for the Sentinel project, including the approach, design, cost, funding sources, time frame, contracting vehicle, and oversight structure. In reviewing the management processes and controls the FBI has applied to the pre-acquisition phase of Sentinel, the OIG found that the FBI has developed IT planning processes that, if implemented as designed, can help the FBI successfully complete Sentinel.

In particular, the OIG found that the FBI has made improvements in its ability to plan and manage a major IT project by establishing ITIM processes, developing a more mature Enterprise Architecture, and establishing a Program Management Office (PMO) dedicated to the Sentinel project.

However, at that time the OIG identified several concerns about the FBI's management of the Sentinel project: (1) the incomplete staffing of the Sentinel 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

[17] Department of Justice, Office of the Inspector General. *The Federal Bureau of Investigation's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System*, Audit Report Number 06-14, March 2006.

track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's information technology investment management processes.

In May 2006, the GAO released a report critical of the FBI's controls over costs and assets of its Trilogy project.[18] The GAO found that the FBI's review and approval process for Trilogy contractor invoices did not provide an adequate basis for verifying that goods and services billed were actually received and that the amounts billed were appropriate, leaving FBI highly vulnerable to payments of unallowable costs. These costs included first-class travel and other excessive airfare costs, incorrect charges for overtime hours, and charges for which the contractors could not document costs incurred. The GAO found about $10 million in unsupported and questionable costs. The GAO also found that the FBI failed to establish controls to maintain accountability over equipment purchased for the Trilogy project. According to the GAO, poor property management led to 1,200 missing pieces of equipment valued at $7.6 million.

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.[19] The OIG audit report concluded that the difficulties the FBI 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. The report described concerns with the cost-plus-award-fee contract as it was implemented by the FBI for Trilogy because the contract did not: require specific completion milestones, include critical decision review points, or provide for penalties if the milestones were not met.

---

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

[19] 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.

In April 2005, the House Appropriation Committee's Surveys and Investigations staff similarly concluded in its report that:[20]

- 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.[21] 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 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

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

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

GAO recommended that the FBI's CIO be provided with the responsibility and authority to effectively manage IT FBI-wide.

FINDINGS AND RECOMMENDATIONS

Foundation of the Sentinel Project

In March 2006, using a Government-Wide Acquisition Contract (GWAC), the FBI awarded Lockheed Martin Services, Incorporated a $57 million task order for Phase 1 of Sentinel, with options for $248 million more to complete three additional phases and provide the operations and maintenance of the system. In addition to a cost baseline, the project also has an overall schedule for which specific baselines are being established phase-by-phase. Over about 4 years, Lockheed Martin will be responsible for designing, developing, integrating, testing, deploying, operating, and maintaining Sentinel. In addition to the potential award of $305 million to Lockheed Martin, the FBI expects to spend $120 million for other contractor support and program management, for a total project cost of $425 million.

Based on our review of Sentinel's Statement of Work and other documents associated with the contract award, we concluded that the contracting arrangement and scope of work for Sentinel appear reasonable, particularly considering the FBI's vastly improved ITIM processes and project management capabilities. We also found that the FBI has made good progress toward addressing most of the concerns identified in our March 2006 audit report, although continued action or monitoring is needed on some of the concerns. We have also identified additional concerns in this audit. Among our overall concerns are: (1) project funding, (2) the estimate of total project costs, (3) risk management, and (4) filling PMO vacancies.

Sentinel Contract

The FBI is using a GWAC contracting vehicle, administered by the National Institutes of Health (NIH), to develop Sentinel. Such a contracting vehicle streamlines the acquisition process by allowing multiple government agencies to purchase services under one contract. Instead of awarding a specific contract to a vendor, the

awarding agency issues a task order to the selected vendor. In the case of Sentinel, the FBI administers the task order itself. In March 2006, the FBI announced that the four-phase Sentinel project would cost an estimated $425 million, with $305 million awarded to Lockheed Martin to develop the system by December 2009 and $120 million for the FBI's program management costs and other contractor support.

The FBI subsequently awarded Lockheed Martin a $57 million task order for Phase 1 of Sentinel, with options for $248 million more for the three additional phases and the operations and maintenance (O&M) of the system developed during the project. In addition to the cost baseline, the project has an overall schedule for which specific baselines are being established phase-by-phase. Over about 4 years, Lockheed Martin will be responsible for designing, developing, integrating, testing, deploying, operating, and maintaining Sentinel – which will be primarily based on commercial-off-the-shelf software – and will provide all the personnel, facilities, equipment, material, and support necessary to implement Sentinel.

Lockheed Martin is performing the work under a cost-plus-award-fee arrangement, similar to the one used during the Trilogy project.[22] However, the FBI is providing much greater control and oversight for Sentinel compared to the weak management evident in the Trilogy project. The contract is structured to reward excellent performance by Lockheed Martin. If Lockheed Martin meets the schedule and cost targets set by the FBI, the FBI can grant Lockheed Martin award fees of up to [redacted] percent of the [redacted] Sentinel development costs, or up to nearly [redacted]. Lockheed Martin's performance will also determine whether the FBI exercises options to award additional phases of the project to Lockheed Martin. If the FBI finds Lockheed Martin's performance unacceptable at any stage of the project, the FBI can order Lockheed Martin to stop work on the project. If the contractor does not meet its milestones, it will be penalized by loss of the award fee.

Estimating Sentinel's Cost

The FBI based its $425 million estimate for the total cost of the Sentinel project on: (1) an independent government cost estimate conducted on the FBI's behalf by Mitretek Systems prior to soliciting

[22] The development contract under the GWAC is cost-plus-award-fee. However, all materials are cost-plus-fixed-fee and travel is cost reimbursable only.

bids for Sentinel in April 2005, and (2) the FBI's assessment of the cost estimate contained in Lockheed Martin's proposal.[23] We reviewed the processes used to derive the $425 million estimate, noted inconsistencies in the process and the results, and concluded that the estimate is a rough approximation of Sentinel's overall costs. The estimate is, in our view, tentative given the variances in the supporting cost estimates and the inherent complexity of estimating costs for a major IT system even before the design is finalized. However, the FBI's CIO said he stands by the estimate. Further, we identified several Sentinel-related projects, the costs of which are not included in the overall Sentinel estimate.

Independent Government Cost Estimate

The independent government cost estimate concluded that project costs would range between $329 million and $493 million, with the most likely cost $438 million. According to the Chief of Sentinel's Business Management Unit, this estimate is the basis for the $120 million program management portion of the FBI's total estimate of $425 million.

The independent government cost estimate established a series of classifications to describe the work to be accomplished and the products to be acquired in the development of Sentinel. Six different techniques were used to estimate the cost of the various elements of Sentinel: parametric modeling, cost estimating relationships, analogy, engineering assessment, vendor quote, and historical data. Appendix 4 provides detailed definitions of each of these cost estimating methods. The cost-estimating method chosen for each work element depended on the availability of technical and cost data.

We reviewed the estimate and identified several concerns about its ability to provide the FBI with a reliable estimate of Sentinel's costs. The estimate was performed concurrently with development of Sentinel's requirements. While Mitretek Systems, the FBI's estimating contractor, coordinated its efforts with personnel developing Sentinel's requirements, the estimate might not accurately reflect the project's final design specifications, which are not expected to be completed

[23] Independent government cost estimates help federal agencies budget for projects, compare contractor proposals, and evaluate the reasonableness of costs in contractor proposals.

until about October 2006. Also, the estimate contains several inconsistencies. For example, some parts of the cost estimate show Sentinel's O&M phase lasting 3 years while other parts show it lasting 2 years, resulting in a likely O&M cost range of $62 million to $87 million. If the additional inconsistencies are factored into the summary cost of the O&M phase, the O&M estimate could be as low as $53 million. Finally, the overall cost estimate does not include all of the costs in the Sentinel funding plan. For example, the estimate does not include the management, or risk, reserve or a separate Independent Verification and Validation (IV&V) contract to independently assess Lockheed Martin's testing of Sentinel's software, which currently account for a total of $40 million of the PMO's $120 million estimate.[24]

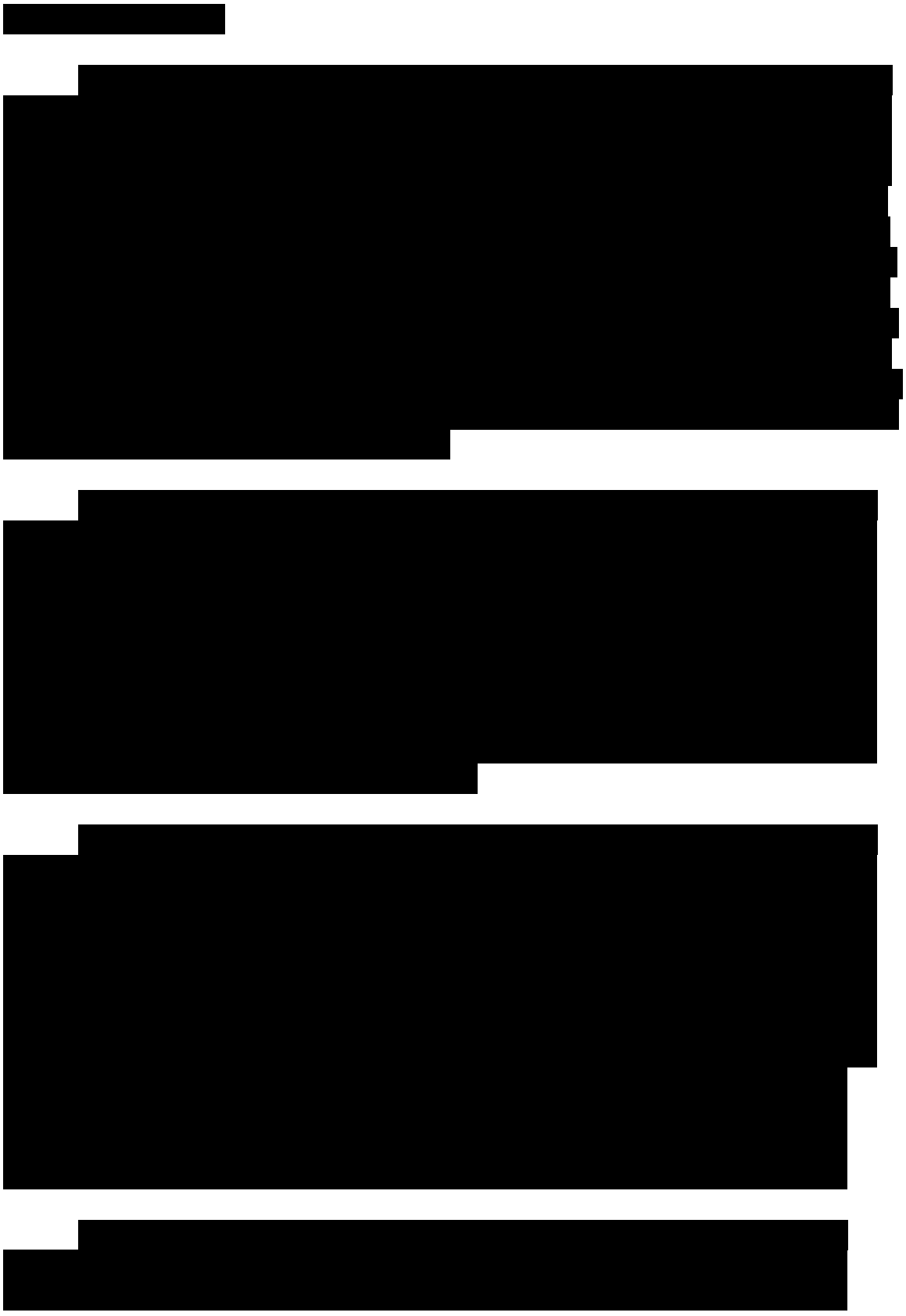
Government's Estimated Most Probable Cost

The FBI received proposals for the Sentinel project from [redacted] bidders. When the [redacted] proposals were received, the FBI reviewed them to determine whether the cost data within the proposals was complete, based on clear and accepted methodologies, and accurate. [redacted][25] Cost realism analysis results in the Government Estimate of Most Probable Cost (GEMPC) for the project. [redacted].[26] Based on the GEMPC, FBI officials concluded that Lockheed Martin's estimate was reasonable [redacted]

[24] A management reserve, also known as a risk reserve, is a budgeted contingency fund used to cover costs not anticipated at the time a project's cost estimate is developed.

[25] The Federal Acquisition Regulation (FAR) requires that cost realism analysis be performed on cost-reimbursement contracts to determine the probable cost of performance for each bidder. Cost realism analysis is the process of independently reviewing and evaluating specific elements of each proposed cost estimate to determine whether the estimated cost elements are realistic for the work performed, reflect a clear understanding of the requirements, and are consistent with the unique methods of performance and materials described in the bidder's technical proposal.

[26] [redacted]



[redacted]

[redacted]

[redacted] Despite these differences, the FBI determined that Lockheed's proposal was reasonable and did not pose a significant risk. According to FBI officials, the FBI resolved the issues identified in the GEMPC during its negotiations with Lockheed Martin.

[redacted] Due to the variability and inconsistencies of the estimates we reviewed, and the difficulty of forecasting the eventual cost of a major IT project, we could not confirm the accuracy of estimates, nor could we validate the FBI's overall estimate of $425 million for Sentinel.

[27] [redacted]

Sentinel-Related Costs

We also identified several projects and other costs, which in total exceed $25 million, that are related to Sentinel but are not considered by the FBI as direct Sentinel costs and are therefore not included in the FBI's total estimate of $425 million. Examples of these related costs include the National Name Check system, security costs, and FBI salaries. However, as discussed previously, because of the difficulties associated with accurately estimating the total cost of such a large project, we cannot state with certainty whether Sentinel's costs would exceed $425 million, only that the costs would be higher if the costs of the Sentinel-related projects were included.

The implementation of Sentinel will require changes to the FBI's National Name Check system. In response to a request from a federal, state, or local agency, the National Name Check Program queries FBI records to determine whether the person named in the request has been the subject of an FBI investigation or mentioned in an FBI investigation. The data system used by the Name Check program relies very heavily on the ACS system, which Sentinel is intended to replace. The estimated cost of updating the existing name check system to work with Sentinel is over [redacted].

The FBI is also developing security through its Information Access Technology Initiative (IATI) to support Sentinel and future FBI systems. A portion of the IATI is intended to help the FBI move from a manual security classification review of documents to a more automated review. The IATI will be developed in concert with Sentinel and should be able to integrate with Sentinel and the FBI's overall IT network as well. The purchase of any initial license for a security product used in conjunction with the IATI would be funded by the Office of the CIO (OCIO). This license will be used for testing and evaluation. If approved, Sentinel would later purchase a license for its own use of the product. While the software is critical to the security of Sentinel, the cost of the initial license is not reflected in the FBI's Sentinel costs. The FBI is uncertain as to which of the products in development would be used by Sentinel and therefore was unable to estimate the specific costs related to Sentinel.

The salary costs of FBI employees are also not tracked as a Sentinel expense. These costs include FBI employees assigned to the Sentinel PMO, the employees who will be developed to train other employees on Sentinel use, ITOD staff assigned to Sentinel,

employees who will attend Sentinel training, and the Finance Division auditors who review Sentinel invoices. While the Independent Government Cost Estimate of $438 million does not include the cost of FBI employees in the overall cost of Sentinel, other portions of the report concluded that the cost of FBI employees' involvement in the development and implementation of Sentinel would be approximately $15.8 million.

The FBI's position is that the separate projects discussed above are independent, enterprise-wide projects that will benefit the FBI's overall IT structure, including Sentinel but also many other FBI projects. The CIO and the Sentinel PMO contend that the costs of such independent projects ought not be considered as Sentinel costs. While we agree that these Sentinel-related projects may not be direct Sentinel costs, in our view the scope of the Sentinel project would be larger if it was not supported by these other investments. When decision makers are considering the full cost of the Sentinel project, they should keep in mind both the direct project costs as well as the additional related costs.

Spending Plan and Management Reserve

In the FBI's spending plan for Sentinel, developed shortly after it awarded the contract, the $425 million total project cost estimate covers the four phases of Sentinel plus 2 years of O&M after the completion of the system. Based on Lockheed Martin's proposal, the FBI plans to pay Lockheed Martin $305 million for the development of Sentinel and its O&M expenses. The spending plan shows that the FBI will use the remaining $120 million for program management, the IV&V of the software, and management reserve. The FBI estimates that Phase [redacted], with a cost of [redacted] over [redacted] years, will be the most expensive phase as well as the most challenging. The chart below summarizes the FBI cost estimates by type of expense and project phase.

Sentinel Spending Plan by Phase

CHART REDACTED

Source: The FBI

According to a May 2006 Lockheed Martin plan, material and equipment will be the largest cost of Lockheed Martin's contract to develop and deploy Sentinel. As shown in the following chart, labor to develop the system and O&M of the system are the other two major cost categories; together, they represent over 50 percent of the value of Lockheed Martin's contract.

Lockheed Martin Spending Plan
By Cost Category

CHART REDACTED

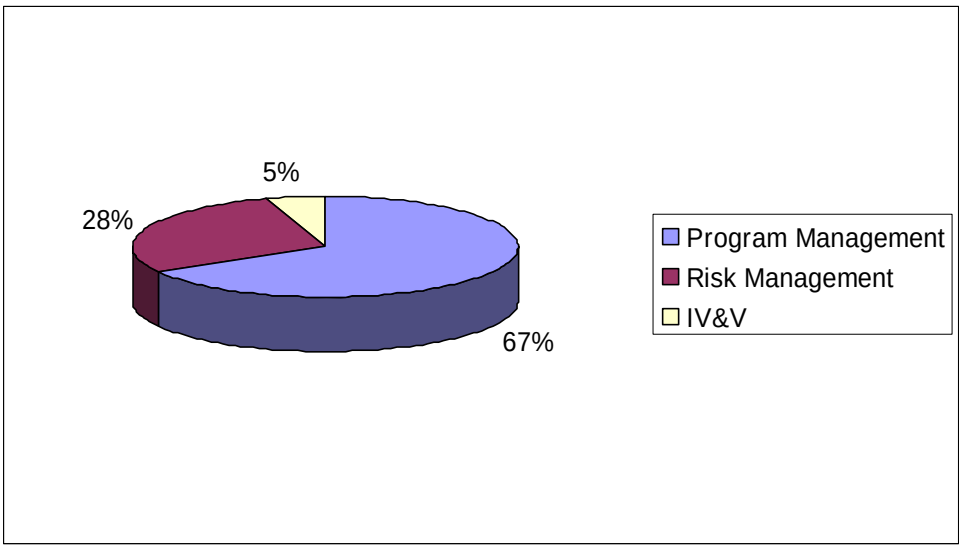
Source: Lockheed Martin Services, Incorporated

The Sentinel PMO is responsible for ensuring that the Sentinel project is properly executed, including: (1) oversight of the program's cost, schedule and performance, (2) Life Cycle Management Directive (LCMD) reviews; (3) award fee evaluations; (4) review and acceptance of Lockheed Martin's documents; (5) requirements and risk management; and (6) budget and financial management.[28] As shown in the following chart, the FBI estimates that the majority of the PMO's expenses will be for the operation of the PMO itself. The primary expense of the PMO is contractors, which accounts for about 74 percent of the PMO's 73 planned positions. The PMO's budget is based on the requirement that all positions be filled throughout the four phases of development. However, the Chief of the Business Management Unit told us that there is no reason to fill six positions until the project approaches Phase 2, which begins in early 2007 (PMO staffing is discussed later in this report). Twenty-eight percent of the PMO's $120 million budget is for a management, or risk, reserve. (As discussed in the EVM section of this report, Lockheed Martin also has a management reserve for Phase 1.) The management reserve is an

[28] The LCMD, which is a set of policies applicable to all FBI IT programs and projects, contains a framework for standardized, repeatable, and sustainable processes for developing IT systems. The LCMD covers the entire IT system life cycle, including planning, acquisition, development, testing, and operations and maintenance. See Appendix 6 for a detailed description of the LCMD.

OMB-required contingency fund used to cover the costs not known at the time a project's cost estimate is developed. Depending on the confidence level the agency has in a project's cost estimate, the OMB calls for management reserve of 10 to 30 percent.

Project Management Office Spending Plan
By Cost Category



Source: OIG Analysis of FBI data

According to the Sentinel Program Manager, Sentinel's management reserve should be 11 percent of the estimated $232.4 million development cost of the project, or about $25.6 million. The PMO determined the percentage of the management reserve based on a review of the known risks and the System Requirements Specification.[29] We found that the total Sentinel management reserve of $34.1 million is about 15 percent of the development cost of the project. As shown in the following chart, the FBI's management reserve varies by program phase from 11 percent of the development cost for Phase 2 to 32 percent for Phase 4.

[29] A System Requirements Specification defines a system's technical requirements in quantifiable and verifiable terms and the methods to be used to ensure that each requirement has been met.

Management Reserve as a Percentage of Development Cost by Project Phase

CHART REDACTED

Source: OIG Analysis of FBI data

The Sentinel Program Manager said he did not advocate a management reserve greater than 11 percent of development, and he expects the Phase 1 management reserve to be reduced from 15 percent to 11 percent.[30] The FBI's Deputy Assistant Director of Finance agreed that an 11 percent management reserve was sufficient for Phase 1. However, he said the Finance Division had not transferred the excess management reserve to another account because there was no current operational need for the money. Both the Chief of the Sentinel PMO's Business Management Unit and the Deputy Assistant Director of Finance said that the amount of the management reserve for each phase was determined based on preliminary estimates of Sentinel's cost and had not been adjusted to reflect the FBI's contract with Lockheed Martin. The FBI's current spending plan for Sentinel overstates the total anticipated cost of the project by $8.6 million, the difference between a management reserve of 15 percent of development costs and the 11 percent. However, FBI officials told us that over the course of the project, the management reserve will be adjusted to 11 percent of Sentinel's development cost.

[30] The FBI's Finance Division, not the Sentinel PMO, controls the management reserve.

Funding Sentinel

Our March 2006 report stated that 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. According to the PMO's most recent cost estimates, Phase 1 will cost $108.5 million and require funds over four fiscal years (FY) starting in FY 2006. However, Phase 1 will only require $93.4 million in FY 2006 and 2007 funds, potentially making $3.6 million of the $97 million in reprogrammed funds available to help fund Phase 2.

The President's FY 2007 budget request includes $100 million for Phase 2 of the Sentinel project. However, whether the FBI will receive the full requested amount is uncertain because the FY 2007 appropriation has not been finalized by Congress. [redacted] If the FBI receives the full $100 million requested in the FY 2007 budget, the FBI would need to identify an additional [redacted] to meet Sentinel's FY 2007 funding requirements. [redacted] However, the FBI's CIO recently told us that an FY 2007 appropriation of less than $100 million would be cause for concern and could result in an unanticipated level of reprogramming of FBI resources to fund the Sentinel project.

The FBI plans to seek additional appropriations to fund the third and fourth phases of Sentinel. [redacted]

[redacted] The table below shows the spending plan for Sentinel by fiscal year over the life of the project.

Sentinel Spending Plan (Millions of Dollars)

CHART REDACTED

Source: FBI

In our first report on Sentinel, we noted that more than $14 million of the FBI's $97 million November 2005 reprogramming would come from the Counterterrorism Division budget, $13 million from intelligence-related activities, and $2 million from the Cyber Division. During our first audit, most FBI divisions and offices seemed confident about their ability to absorb the initial reprogramming of funds to Sentinel for Phase 1. However, the officials stated that a second reprogramming of the same magnitude would damage their ability to fulfill their mission.

During this audit, we also interviewed officials at FBI headquarters to assess the impact of the $97 million reprogramming and any future reprogrammings for Sentinel. Generally, these officials confirmed that their divisions and offices can withstand the diversion of funds to Sentinel for the first reprogramming and that the successful implementation of a modern case management system would offset the operational impact of the reprogramming. These officials also said they had not received notice of the need for or amount of any future reprogrammings and therefore could not assess its potential impact. In our judgment, any reprogramming significantly above $50 million will require the FBI to carefully consider which programs and activities will be affected and how to monitor the overall impact on the FBI's mission.

Cost Tracking and Control

For 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 stated our continuing concern in our March 2006 report on Sentinel. Also, in its February 2006 report the GAO stated that the FBI's poor cost controls resulted in the payment of about $10 million in questionable contractor costs, and poor property management led to missing equipment valued at $7.6 million.

The FBI has now established several layers of control to help ensure that costs are authorized in advance, verified when delivered, and validated when invoiced. The overlapping responsibilities for oversight of Sentinel's costs include: the FBI's Finance Division – which performs accounting, auditing, and budget monitoring; the Office of the Chief Information Officer's (OCIO) IT Financial Management Unit – which tracks Sentinel's costs in detail; and the Sentinel PMO's Program Integration Unit – which tracks program and development costs and has developed policies and procedures for processing invoices, requisitioning and procuring equipment, reviewing contractor time charges, and resolving discrepancies. The Sentinel PMO's Business Management Unit has also implemented a "change management process" to help prevent "requirements creep" that can increase project costs or schedule delays. The tracking systems and controls the FBI has implemented provide greater assurance that the FBI will be better able to monitor and control project costs for Sentinel than was the case under Trilogy.

Oversight and Control

The Finance Division's Audit Unit has dedicated two of its six auditors to work part time on Sentinel. According to Finance Division staff, auditors periodically review a sample of invoices for Sentinel goods and services to verify that applicable procedures are being followed. The Audit Unit produces a monthly audit report, which is distributed to the Contracting Officer's Technical Representative (COTR), the Finance Division, and FBI management, including the Deputy Director.

The Finance Division tracks Sentinel spending through the FBI's Financial Management System (FMS). The FMS uses four categories – development contract, O&M, program management, and risk

management – to track Sentinel costs. In addition, the Chief Financial Officer (CFO) has established a separate, dedicated cost code for Sentinel that allows the Sentinel PMO, OCIO, and CFO teams to jointly track and control Sentinel costs through the Budget Execution and Analysis Reporting System (BEARS), a database used to track budget information within the OCIO. BEARS tracks Sentinel equipment purchases and other expenditures by project phase based on 20 specific spending plans. BEARS extracts purchase order information from the FMS and generates reports on funds requested, amounts approved, and obligations that have not yet entered the FMS. BEARS data is used for the FBI's EVM analyses, discussed below.

Requisitions require the approval of the Sentinel PMO, Business Management Unit Chief, the COTR, and the Office of IT Program Management's Program Management Executive. The PMO budget analyst and the IT Financial Management Unit verify availability of funds according to the spending plans. The Office of IT Policy and Planning validates and approves the requisition requirements, and the IT Financial Management Unit enters the requisition information into BEARS.

The IT Financial Management Unit only tracks funds that have been entered into the Sentinel spending plans in BEARS. It loses visibility over Sentinel funds any time funds are transferred from Sentinel to another FBI program. For example, the Sentinel PMO had to pay for its portion of the FBI's wireless service that supports its handheld e-mail devices. The IT Financial Management Unit transferred funds from the Sentinel account to the appropriate account. Once this transfer occurred, the Unit no longer had the capability through BEARS to determine whether the money was actually spent for the use intended**.** The IT Financial Management Unit has not devised a practical alternative method to track Sentinel costs not entered into the BEARS database managed by the unit.

Invoice Processing Overview

We reviewed Sentinel's requisitioning and invoice processing procedures and found that they appeared reasonable. The contractor submits invoices to the COTR for review. The COTR verifies the invoices with the Sentinel Unit Chiefs, such as the chief of the System Development Unit, to ensure that the billed work has been performed, is within the scope of work, and is funded. The COTR returns any

incorrect invoices to the vendor with comments detailing the discrepancies or the additional information required.

The Chief of Sentinel's Business Management Unit records and tracks invoices against purchase orders; analyzes actual expenditures against planned spending by month; prepares regular reports for the COTR, Unit Chiefs, and the Program Manager regarding the availability of funds; notifies the COTR and Program Manager of any deviation greater than 5 percent from planned expenditures; revises spending plans at least quarterly; and coordinates invoices with EVM estimates.

The Program Manager or Deputy Program Manager reviews final invoices after the reviews by the COTR and unit chiefs, and is responsible for approving invoices for payment. The Contracting Officer then gives final approval and forwards the invoice to the FBI's Commercial Payments Unit for payment.

Based on our review, the Sentinel's policies and procedures for processing invoices, requisitioning and procuring equipment, reviewing contractor time card, and handling deviations in bills of materials should help prevent the FBI from incurring and paying for unauthorized services and materials.

Earned Value Management

Our March 2006 report on Sentinel pointed out the need for the FBI to establish an EVM process for Sentinel, which it has since done. EVM helps manage project risks by achieving reliable cost estimates, evaluating progress, and allowing the analysis of project cost and schedule performance trends. EVM compares the current status of a project, in terms of both cost and schedule, to the established cost and schedule baselines. Deviations between the baselines and the current status demonstrate the project's progress and the overall level of performance, thereby enabling a level of accountability to be imposed on the project. When properly utilized, EVM allows project management to pinpoint potential problems and address them before they escalate. Based on our review of early EVM reporting from April to August 2006, we identified no immediate concerns with Sentinel's cost or schedule in the first phase of the project, although Lockheed Martin was still grappling with some estimating errors that may have a future impact on the EVM results.

According to the FBI's EVM plan, the Sentinel PMO will use the plan to measure its and the contractor's earned value performance and report the result to oversight entities. The Sentinel project's Statement of Work requires vendors and contractors to fully implement EVM in accordance with the plan, including having an EVM system of its own that complies with American National Standards Institute (ANSI)/Electronic Industries Association (EIA) Standard 748-A.[31] This allows the FBI to gather EVM data on the development portion of the project from Lockheed Martin through monthly electronic data transfers from Lockheed Martin. The Sentinel PMO collects EVM data for the PMO portion of the Sentinel from invoices from support services contractors and BEARS, an FBI reporting system discussed previously.

The Statement of Work also included the requirement that the vendor perform an Integrated Baseline Review (IBR), where the cost and schedule baselines would be established for the project. Properly executed, IBRs are an essential element of a Program Manager's risk-management approach. IBRs are intended to provide both the government's and the contractor's program managers with a mutual understanding of the project's performance measurement baseline and agreement on a plan of action to resolve any identified risks.

The Sentinel IBR started on schedule, but took somewhat longer than scheduled to complete. According to the report documenting the results of the IBR, the FBI and Lockheed Martin achieved the objectives of the IBR, and the Project Management Baseline was set for Phase 1. The IBR set the baseline budget at [redacted], not including the [redacted] (about [redacted] percent of the baseline budget) management reserve established for Lockheed Martin at the IBR. Including the management reserve, the baseline budget is $2.9 million less than the $57.2 million contracted for Phase 1. Lockheed Martin's management reserve, which was established with the FBI's agreement, is intended to provide Lockheed Martin with the flexibility to respond to any cost estimating errors it may have made and still stay within the contracted amount. The Sentinel Statement of Work also required that Lockheed Martin submit its EVM system to the

[31] ANSI/EIA Standard 748-A is the criteria selected by the OMB for EVM systems. The standard includes 32 specific criteria in five process areas necessary for a sufficient EVM system: (1) organization; (2) planning, scheduling and budgeting; (3) accounting; (4) analysis and management reports; and (5) revisions and data maintenance.

contracting officer for review. In June 2006, the PMO's EVM analyst reviewed Lockheed Martin's EVM system and determined that the system complies with ANSI/EIA Standard 748, and the FBI's contracting officer concurred.

At the time of our audit, the FBI had begun using "Winsight" software to maintain and report Sentinel's EVM performance metrics. Sentinel's EVM analyst prepares three EVM reports each month: one analyzing the whole program's EVM data, one analyzing Lockheed Martin's EVM data, and one analyzing the PMO's EVM data.

We reviewed the EVM reports for April to August 2006. The August 2006 EVM reports show that since the schedule and costs of Lockheed Martin's work were determined, the actual cost of work performed by Lockheed Martin exceeded the planned cost. During June, July, and August, the Lockheed Martin portion of the program was [redacted] percent, [redacted] percent, and [redacted] percent over budget respectively.

According to the June report, Lockheed Martin made an estimating error in the EVM baseline approved at the IBR. [redacted] However, according to the EVM report, Lockheed Martin officials said another estimating error should offset the excess costs accrued in June. [redacted]

However, if Lockheed Martin continues to accrue costs at the rate it did in June, the EVM report projects that Lockheed Martin's cost for Phase 1 will be about [redacted], or approximately [redacted] more than the baseline budget of $[redacted] (excluding Lockheed Martin's [redacted] management reserve). Still, the projected cost is less than the $57.2 million contracted amount for Phase 1 of Sentinel. The report concluded that Lockheed Martin's EVM data is not likely to show "a rapid and large improvement," [redacted]

[redacted] FBI officials recently told us that Lockheed Martin has developed a plan showing how the variance in [redacted] will not have a negative impact on the cost of Phase 1.

The July 2006 EVM report also showed that the actual costs incurred by the PMO were about $1.1 million less than planned at this stage of the project. The EVM report attributes the spending variation primarily to vacancies in the PMO. The report concluded that the variance should not prevent the program from meeting its schedule or performance goals and recommended that PMO management continue to focus on filling the PMO's vacancies (see discussion of PMO vacancies later in this report). As a result of joint Lockheed Martin-FBI decision to delay some purchases, Lockheed Martin did not receive hardware and software on the dates envisioned by the baseline schedule, causing the July EVM report on Lockheed Martin's activities to show it being behind schedule by 10.1 percent.

The OMB requires agencies to report to it EVM variances greater than 10 percent, including what corrective actions the agency will take to remedy the variances. While the development of Sentinel depends heavily on Lockheed Martin's performance, the Lockheed Martin EVM data is only part of the Sentinel EVM data. In July, the net schedule variance for the Sentinel program as a whole – the basis for whether it is required to report variances to the OMB – was 8.1 percent. Sentinel is on the OMB government-wide list of high-risk IT projects, meaning that Sentinel is a high-priority project, not that it is a troubled project. FBI officials said that because Sentinel is on the high-risk list, the FBI provides the OMB with monthly EVM data on the PMO's performance and Lockheed Martin's performance, regardless of whether or not there are any significant variances.

In our judgment, reporting from June to August 2006 shows that Sentinel's EVM system is functioning as intended and providing FBI managers with warnings of issues that may affect Sentinel's cost or schedule, including Lockheed Martin's estimating errors and vacancies in the PMO. We also believe it was prudent for the FBI to allow

Lockheed Martin to establish a management reserve to compensate for estimating errors. While we identified no significant immediate concerns, we are concerned about the future implications of the cost variances experienced by Lockheed Martin, especially the higher-than-expected labor rates. We will continue to monitor Sentinel's EVM reporting to identify any concerns affecting the project baselines.

Risk Management

The FBI has instituted a risk management process to identify and mitigate the risks associated with the Sentinel project. The risk process is managed by the Sentinel Project Manager and a Risk Review Board, which meets biweekly. 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 FBI's LCMD.[32]

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 the Sentinel Program Manager, PMO personnel attend and participate in Lockheed Martin's risk management meetings. These weekly meetings are the

[32] In addition to the risk management processes cited above, the following receive briefings that include information about Sentinel risks: the FBI Director (weekly); a review team with senior representatives from the Department of Justice, OMB, and Director of National Intelligence (monthly); the FBI CIO's Advisory Council (bi-monthly); the FBI Director's Advisory Board (as requested); and congressional oversight committees (quarterly).

primary reason that the Sentinel Risk Review Board continues to meet biweekly rather than weekly, as planned in the pre-acquisition phase.

According to the Sentinel Risk Management Plan, risks are to be identified, assessed, and tracked throughout the life of the project. When a proposed risk is brought before the Risk Review Board, the board's voting members decide whether or not to accept the risk as an "open" risk and, if accepted, vote on the severity the risk will have on the project's cost, schedule, and performance and the probability the risk will occur. Risks brought before the Risk Review Board are documented in a risk register, which includes the following:

- description of the risk,
- impact on the program should the risk occur,
- phase of Sentinel affected by the risk,
- person responsible for managing the risk,
- OMB risk category,
- severity of the risk as voted by the Risk Review Board,
- probability the risk will occur as voted by the Risk Review Board,
- strategy to mitigate the risk,
- risk status,
- contingency trigger, and
- contingency plan

The risk register lists open risks in rank order based on the risks' probability and severity ratings. The PMO is responsible for tracking and periodically reviewing risks that are closed or resolved to prevent recurrence and to document the effectiveness and any unintended consequences of the mitigation strategy employed. Generally, Sentinel's mitigation strategy has been to develop a series of actions that will decrease the probability a risk will occur or the severity of a risk's impact on Sentinel.

As of August 2006, the FBI had identified, and was managing, 20 open risks to the Sentinel program, including the five top-ranked risks:

- new model for data access and control (access rules) may impact project schedule and budget;

- user requirements may change significantly as a result of the business process reengineering initiative and impact Sentinel's schedule and budget;

- absent an authoritative source of identity attributes, Sentinel must internally develop identity attributes for Role Based Access Control, and impact on FBI Enterprise Directory Service requirements is unknown;

- development contractor hiring is lagging in providing the resources needed to complete design work; and

- lack of attendance or participation by users in training.

The severity of 9 of the 20 risks was classified as high, meaning that if the risks occurred they would have a major impact on Sentinel's schedule, cost, or performance. One risk was classified as having a high probability of occurring. However, no high-impact risk was judged to have a high probability of occurrence. Many of these risks addressed subjects raised in our interviews of FBI personnel working on Sentinel, including successfully migrating data from ACS to Sentinel.

We view the FBI's ability to successfully migrate data from the antiquated ACS system to Sentinel as a potentially significant challenge. If the migration were to fail or be seriously delayed, the FBI would need to try maintaining its legacy ACS system with all of its flaws. An inability to migrate the ACS data would also result in a Sentinel system that builds its data from the present day forward, without the benefit of years of investigative data compiled in the old system. Further, should ACS cease to be maintainable, that data could effectively be lost. The Sentinel Program Manager told us that the task of "cleaning" and reconciling the ACS data for migration into Sentinel is not technically difficult, and the FBI plans to use an available COTS software tool for that purpose. However, he pointed out that it will take a significant amount of work to accomplish. He also said that as a preventative measure intended to eliminate any delays in the overall project due to data cleansing, the FBI plans to cleanse data in the phase preceding the phase in which the data will be transferred to Sentinel.

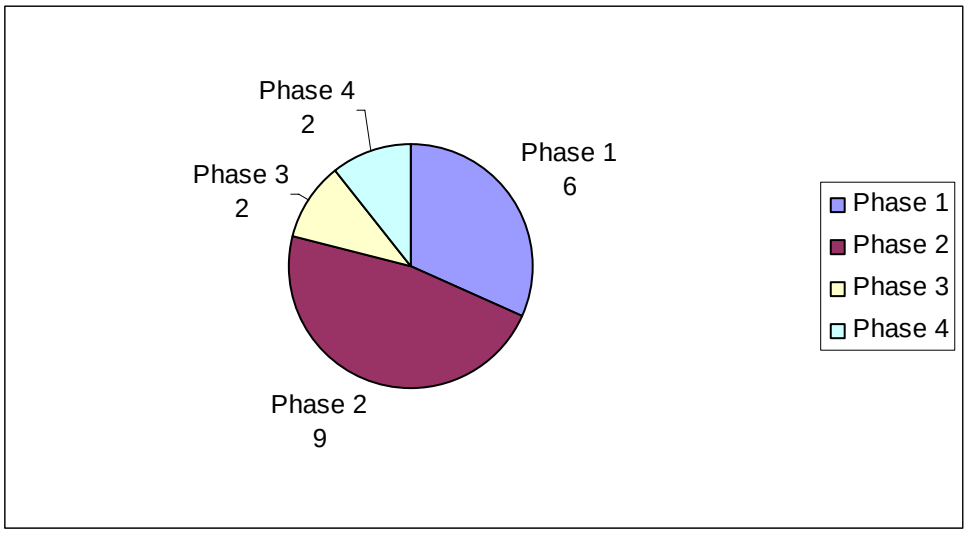
Another potential risk in our opinion is the extent to which Sentinel will actually use commercial-off-the-shelf software modules as intended. A high degree of customization of the software could result in increased costs and schedule delays. The Sentinel Program Manager told us that the components for Sentinel are all off-the-shelf and little or no customization is anticipated. However, the key task

will be configuring Sentinel's various applications – such as the workflow, document management, searching and reporting, and electronic signatures – to all work together. The Program Manager noted that Lockheed Martin has successfully configured similar systems in other major projects, using some of the same software modules, including one at the Social Security Administration.

The August 2006 risk register also included 43 closed risks. Most of these risks had been closed for the following four reasons: the time for the risk to occur had passed; all the steps in the mitigation strategy had been completed; the risk was divided into multiple risks; or the risk was consolidated with another risk.

Our review of the risk register showed that the majority of the 20 open risks are most likely to affect the first two phases of the Sentinel project. As shown in the following chart, the Risk Review Board classified 15 of the 20 (75 percent) risks as having a potential impact on Phases 1 and 2.[33] Of the 6 risks identified as having a potential impact on Phase 1, all but 2 were ranked within the top 10 highest priority risks. Appendix 5 lists the 20 risks in order of priority as well as the phase of Sentinel they could affect.

Open Risks by Sentinel Phase

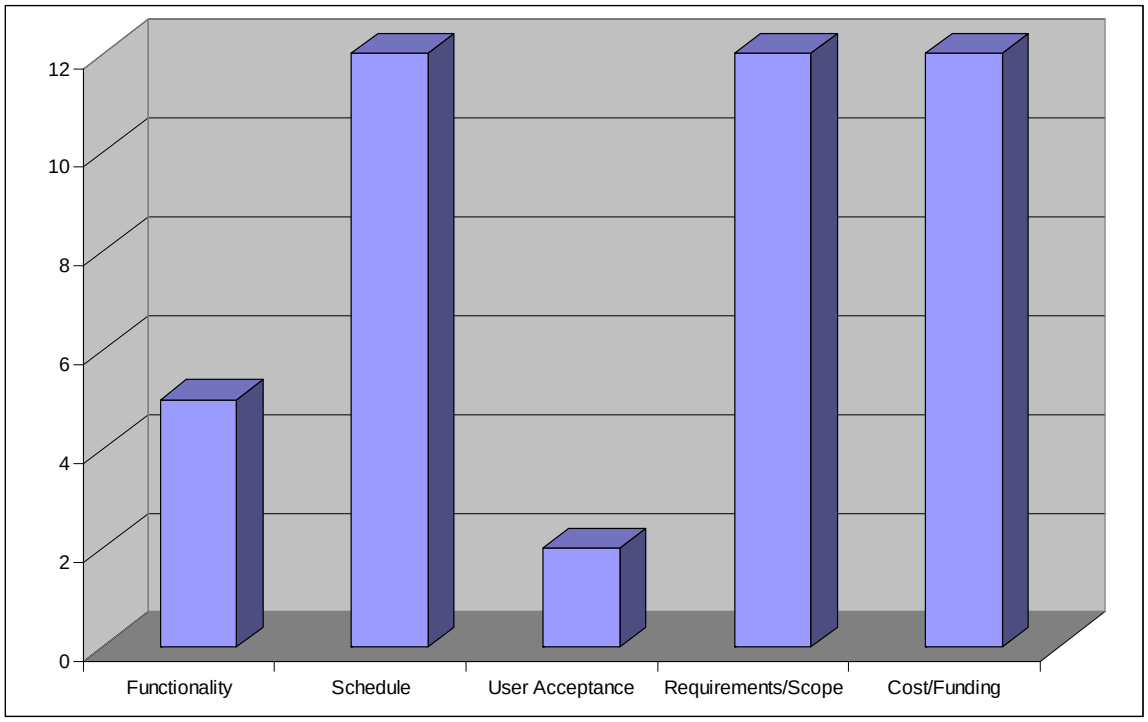


Source: OIG analysis of FBI data

[33] One risk was not assigned a phase in the risk register; as a result, the chart includes a total of 19 risks rather than 20.

The register also includes a statement describing the impact each risk would have on the project should it go unmitigated. We reviewed these statements and found that the consequences of the risks may affect the following aspects of Sentinel: the project's cost and the need for additional funds, the scope of the work to be performed and the project's requirements, the project's schedule, the system's functionality, and user acceptance of the system. As shown in the following chart, schedule, requirements or scope, and cost or funding are the most frequent consequence of the risks the FBI is currently managing.

Consequences of the Risks Currently Being Managed by the Sentinel PMO



Source: OIG analysis of FBI data

According to the FBI's risk management plan, the Sentinel PMO should develop a "contingency trigger" and a contingency plan for each risk it is managing that has a probability or severity rated as medium or higher by the Risk Review Board. A contingency trigger is an event that would convert a risk into an operational issue and cause the FBI to implement a risk's contingency plan. However, we found that the risk register includes a contingency trigger and contingency plan for

only 3 of the 18 risks required to have a contingency plan.[34] In addition, only one of the five highest-ranked risks had a contingency trigger or plan. The Sentinel Program Manager told us that in some cases it is difficult to develop a contingency plan before the FBI's preventive actions mitigate the likelihood or severity of the risk. Instead, he said the PMO is focusing on taking action to prevent risks from occurring and reducing the impact risks could have on the program. He also told us that many risks are temporary and as a project phase progresses the risk may become moot, at which point it is closed. If a risk occurs, the PMO said the FBI will develop corrective actions. We believe there should be a contingency plan developed for each major risk having the potential to result in a significant cost, schedule, or performance deviation from the project baselines.

Staffing of the Program Management Office

Due to the importance of the PMO in project oversight, our previous Sentinel audit raised concerns about the progress in staffing the Sentinel PMO. 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 our March 2006 audit: the planned size of the PMO has decreased from 76 positions to 73 positions primarily because of less overlap in the project phases than initially anticipated; the PMO has reallocated positions among PMO units; and the PMO has filled 14 additional positions.[35] As of October, 2006, the PMO consisted of 65 of the 73 personnel identified in the FBI's Sentinel Staffing Plan (89 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

[34] The remaining two risks did not have probability or severity ratings, so we could not determine whether they required contingency plans.

[35] Three hires are in the process of coming on board.

assistance contractors to maximize program expertise.[36] The following table summarizes the PMO's staffing level as of October 18, 2006, and shows the progress the FBI has made in staffing the office since January 2006.

SENTINEL PMO STAFFING REQUIREMENTS

Organizational Units	Planned Staff (a)	Staff on Board, January 2006	Staff on Board October 2006 (b)
Program Leadership	2	2	2
Direct Reporting Staff	8	6	8
Organization Change Management Team	4	2	3
Business Management	14	9	13
Program Integration	10	10	10
System Development	25	21	25
Transition	5	1	4
Operations & Maintenance	5	0	0
Total	**73**	**51**	**65**

Source: The FBI

Notes: (a) Since January 2006, the Sentinel PMO has revised the total planned staff from 76 to 73. Also, the plan does not include individuals who are on temporary duty assignment to the project.

(b) The number of staff on board includes three positions for which the FBI has selected candidates and is in the process of hiring.

For a more complete description of PMO staff and their duties, see Appendix 7.

The Sentinel Program Manager told us he did not intend to fill all of the PMO's eight vacancies immediately because six positions are not

[36] 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.

needed until the project approaches Phase 2, which begins in early 2007. We agree that not filling positions until required is prudent. However, recruitment efforts need to be timed so that the six positions are filled when needed, allowing time for processing the new hires, including conducting background investigations. The FBI plans to begin recruiting for the Phase 2 positions by the end of October 2006. Moreover, even if some hiring is delayed, two current vacancies exist. Of the current vacancies, one is a government position — an intelligence analyst – and one is a contractor position – a planner. The Chief of the Business Management Unit said that government positions were the most difficult to fill because of the FBI's hiring and background investigation processes. However, he said the steps the PMO had taken steps to expedite hiring, including interviewing applicants who had applied to an open FBI-wide job announcement for computer scientists, had been successful.

The Sentinel Program Manager said that he has gained more insight into the personnel requirements of the PMO and that these insights led him to decrease the number of planned staff by three and reallocate the planned staff among the PMO's units. He said he made the most significant reduction, the elimination of four positions from the Transition Unit, because the current schedule has phases of the project overlapping less than originally anticipated. The following table shows the changes in the number of planned staff from January 2006 to October 2006.

Changes in Sentinel PMO Staffing Requirements, January 2006 to October 2006

Organizational Unit	Change in Planned Staff
Organization Change Management Team	-1
Business Management	-2
System Development	+2
Transition	-4
Operations & Maintenance	+2
Total	**-3**

Source: The FBI

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. As of August 2006, three staff from the Sentinel PMO (five percent) had left the PMO since the project's inception in March 2005. While the PMO has replaced all three staff, we will continue to monitor turnover of Sentinel PMO staff in future audits.

Improved Management Processes and Controls

In the early stages of the Trilogy project, the OIG and GAO recommended that the FBI establish Information Technology Investment Management (ITIM) processes to guide the development of its IT projects. In response, the FBI issued its Life Cycle Management Directive (LCMD) in 2004 after Trilogy was well underway. The LCMD established policies and guidance applicable to all FBI IT programs and projects, including Sentinel. As we reported in our March 2006 report on Sentinel, we believe the structure and controls imposed by the LCMD can help prevent many of the problems encountered in the VCF effort. Since our March 2006 report on Sentinel, the FBI has further refined its LCMD and is applying the revised directive to Sentinel.

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 and a description of the life cycle phases, control gates, and project level reviews is found in Appendix 6.

LCMD Phases and Control Gates

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 August 2006, the Sentinel project had passed through the first four life cycle phases and is currently in the fifth phase – Design.

FBI LCMD 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

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.

At the time of our previous Sentinel audit, the Sentinel project had received approval for the first two of the LCMD control gates: the System Concept on July 15, 2005, and the Acquisition Plan on July 29, 2005. As of August 2006, the Sentinel program had not requested or received approval for the third control gate. According to the Sentinel program manager, Phase 1 of Sentinel is scheduled to pass through Control Gate 3, Final Design Review, in late October 2006. 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.

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. 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. Appendix 6 lists the five executive-level review boards that serve as the decision authority for the control gate reviews.

The Gate 2 approval for Sentinel in July 2005 signified that the IMPRB accepted the overall project approach and cost estimate for acquiring the Sentinel system. Our previous audit showed that the FBI generally complied with the requirements of the then-current LCMD in performing the control gate reviews for Sentinel. However, two documents had not been completed at the time the control gate review

was conducted: (1) the system security plan could not be developed at that time because the vendor needed 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 Independent Verification and Validation (IV&V) plan, to be implemented by a separate contractor to independently assess the implementation of the system according to technical and performance baselines, required a separate contract.

In August 2006, the Department awarded eight IV&V contracts for use throughout the FBI and parts of the Department of Justice. In September 2006, the FBI awarded a task order to Booz Allen Hamilton under one of those contracts for the IV&V of Phase 1 of Sentinel, with options for the remaining phases.[37] According to the FBI, the independent contractor will monitor Lockheed Martin's testing of the system software to ensure the software performs as intended. As an interim measure prior to the award of the FBI-wide IV&V contract, the FBI used one of the contractors supporting the PMO, Keane, Inc., to provide those services pending the availability of the independent contractors. To minimize any conflict of interest with its FBI PMO responsibilities, Keane's activities have been limited to examining Lockheed Martin's performance and not the FBI's. We believe Keane is providing a useful service in helping the FBI monitor Lockheed Martin's performance to date. However, the FBI and its oversight bodies need the assurance of a fully implemented IV&V process throughout the development of Sentinel. We believe this process should begin as soon as possible, and we intend to review the scope and results of the IV&V in our upcoming Sentinel audits.

The system security plan will provide the detail necessary for the completion of the critical certification and accreditation of the applications being created for Sentinel. Unless certification and accreditation is accomplished, Sentinel will not be allowed to operate due to security risks. According to FBI officials, it was not feasible to develop Sentinel's system security plan prior to Sentinel's final design, because the security plan is dependent on the design. However, as of August 2006, Lockheed Martin and the FBI had largely agreed on the design for Phase 1 of the Sentinel project, and Lockheed Martin provided the FBI with a draft of the system security plan for that phase. The Sentinel Program Manager said the plan should be

[37] At the time our audit, all of the specific IV&V activities for Sentinel had not been determined. However, IV&V may include oversight of program management processes and assessments related to the development contractor's performance.

completed by October 2006 when Lockheed Martin and the FBI are scheduled to finalize the design of Phase 1.

The plans for IV&V and system security are, in our opinion, crucial to ensuring the success of the Sentinel project. We will monitor the implementation of both plans in our subsequent audit work.

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. Appendix 6 includes a list of the project-level reviews called for in the LCMD from the beginning of the Concept Exploration Phase to the end of the Design Phase.

In the Sentinel Program Management Plan, approved in August 2005, the FBI stated its intention to combine the Design Concept Review and Preliminary Design Review into a single review as part of the project's LCMD tailoring approach. The LCMD provides for the tailoring of its requirements to meet a specific project's needs, allowing a project to combine, streamline or eliminate events, and modify reports, documents, or deliverables. All tailoring decisions must be reviewed and approved at the Acquisition Plan Review Control Gate before finalizing them as part of the Program Management Plan. A review of the minutes from the Acquisition Plan Review indicates that the IMPRB was briefed on Sentinel's LCMD tailoring approach.

To date, the FBI has conducted the Mission Needs Review, System Specification Review, Source Selection Acquisition Review, Contract Implementation Review, Requirements Clarification Review, combined Design Concept/Preliminary Design Review, and Critical Design Review. The FBI planned to conduct the Final Design Review in October 2006.

Based on our review of meeting minutes and documentation resulting from these reviews, it appears that the FBI is adhering to LCMD requirements in conducting these reviews and is following the schedule for producing the requisite deliverables established in the Program Management Plan.

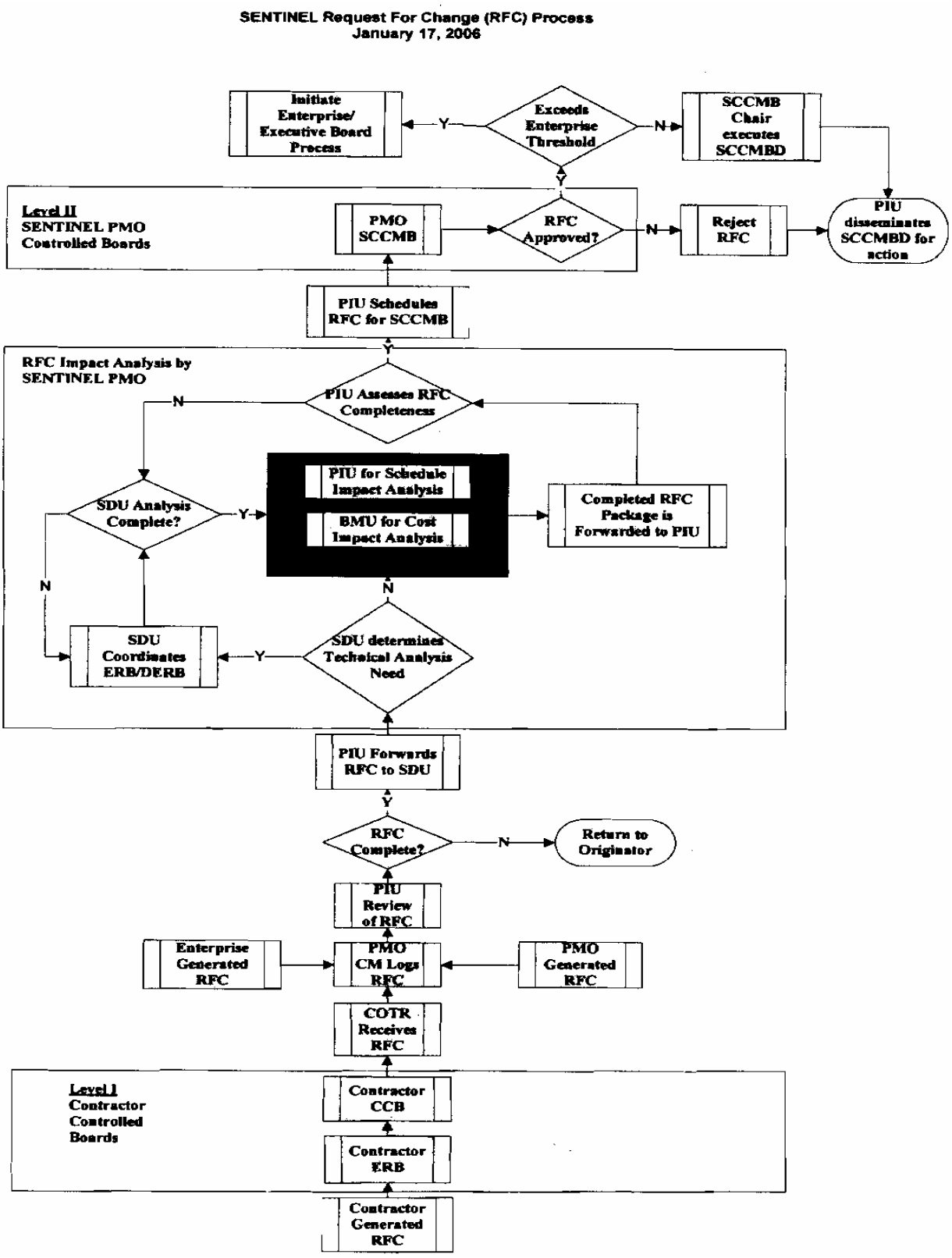
Department Investment Review Board

In addition to the FBI's management reviews, Sentinel has also been required to make periodic presentations to the Department Investment Review Board (DIRB). As part of the Department's IT investment management process, the Department Investment Review Board oversees 10 to 15 of the Department's IT investments with the greatest strategic and financial value. Periodic presentations to the Board, which includes the Deputy Attorney General and the Department's CIO, should demonstrate adequate financial and risk management, alignment with the Department's mission, and a sufficient return on investment. Each time Sentinel has appeared before the DIRB, the DIRB has approved the continued development of Sentinel. The Office of Management and Budget provides additional monitoring of Sentinel. For example, Sentinel is on the OMB government-wide list of high-risk IT projects, meaning that Sentinel is a high-priority project, not that it is a troubled project. Were the Sentinel project to encounter serious problems, it could be placed on the OMB watch list.

Change Management Process

The FBI has implemented a change management process to aid in controlling changes in Sentinel's requirements that could result in cost growth, schedule delays, or performance problems. As shown in the following flowchart, the FBI evaluates the potential effect of each request for change (RFC) on project baselines. Changes that affect the cost or schedule must be approved by the System Configuration and Change Management Board and senior FBI management, up to and including the Deputy Director. According to FBI officials, the FBI Director has made it clear that the FBI's requirements should not necessitate the customization of the commercial software being used in Sentinel. If the FBI's business processes conflict with the capabilities of the software, the FBI is committed to changing its processes rather than the software. We reviewed five of the six RFCs and found they were approved in accordance with the FBI's procedures.[38]

[38] One RFC was approved after we completed audit fieldwork.



Source: The FBI's Sentinel Configuration Management Plan

However, while the FBI has established a reasonable system for limiting changes to the system's requirements, the Sentinel PMO does not control all events that could affect Sentinel's requirements. For example, the Sentinel PMO does not control the FBI's legacy systems or policy changes affecting the FBI. The FBI continues to improve several IT systems that will either interface with Sentinel or be subsumed by Sentinel. These upgrades could add to the scope of Sentinel's requirements by making more difficult the required interfaces. For example, the FBI continues to improve Guardian, an incident tracking system that Sentinel is expected to replace. According to Sentinel's risk register, changes to Guardian may lead to changes in Sentinel's functional or interface requirements, causing delays or cost increases. Also, changes in the FBI's policies governing access to FBI computer systems could affect Sentinel's requirements.

Information Sharing

Executive Order 13356 requires that federal agencies design information systems with priority given to the interchange of terrorism information among agencies and between agencies and appropriate authorities of state, local, and tribal governments. According to FBI officials, the FBI will build Sentinel to share information based on the National Information Exchange Model (NIEM), a joint project of the Departments of Justice and Homeland Security.[39] The NIEM also has the support of the Director of National Intelligence. When finalized, the model will essentially become the new government-wide law enforcement and intelligence agency standard and will serve as the vehicle for future information exchange. However, because the NIEM standards have not been finalized, the FBI has not modified Sentinel's information sharing requirements to meet the draft NIEM standards currently available. FBI officials said that Sentinel will be modified to meet final NIEM standards.

[39] The Sentinel statement of work, which was developed prior to the release of the draft National Information Exchange Model, requires Sentinel to be built to the Global Justice XML Model.

The National Information Exchange Model

Agencies are not able to exchange information if they maintain legacy systems that were not designed for information exchange. The NIEM information sharing standard, which FBI officials said should be finalized in January 2007, is intended to create a national enterprise-wide framework to facilitate information sharing across all levels of government by developing common information exchange standards.

Previously, many agencies shared information with other agencies on a strict "need-to-know" basis and therefore provided little or no access to their systems. In addition, many agencies maintained databases with applications residing on networks that could not communicate with other agencies' networks. As a result of the September 11, 2001, terrorist attacks, information sharing became a high priority. Agencies found that they did not have enough time or resources to modify their systems fast enough to allow for real time information exchange. In an attempt to remedy the immediate problem, agencies built "bridges" to facilitate information exchange, such as Law Enforcement Information Exchange (LInX) and the Regional Data Exchange (R-DEx).[40] R-DEx permits data to be accessed from another computer system and, based on security clearance and the need to know the information, the requester is permitted access to information up to the security level deemed necessary. Standards had to be developed so that information is characterized the same way, no matter what agency originates it, to facilitate the information exchange. NIEM is the effort to standardize the data.

[40] The LInX initiative is a project designed to enhance information sharing between local, state, and federal law enforcement by providing participating law enforcement agencies with secure access to regional crime and incident data, enabling investigators to search across jurisdictional boundaries to help solve crimes and resolve suspicious events. R-DEx gives state, local, and tribal law enforcement access to federal investigative and intelligence information. R-DEx provides detectives, investigators, and analysts the ability to view the linkage across multiple cases and their jurisdictions. These links include individuals, vehicles, weapons, addresses, phone numbers or other types of links. It also allows cases to be plotted on maps in order to identify geographical patterns or links.

Interagency Coordination on Sentinel

We interviewed representatives from the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the Department of Homeland Security (DHS) to determine the extent of each agency's involvement with Sentinel and the need to retrofit their case management systems to communicate with Sentinel.

According to the DEA, two staff members participated in Sentinel coordination meetings and used these meetings to identify changes to Sentinel that would require the DEA to retrofit its case management system, Impact. The DEA is also involved with the development and usage of the NIEM information sharing standard.

The ATF told us it has had limited involvement with Sentinel. The ATF has a representative on the DIRB as a non-voting member and has another staff member who serves as the liaison with the FBI for Sentinel. The ATF is trying to avoid investing large amounts of money in its case management system until after Sentinel is developed because the ATF representative believes that modifications will be needed to its case management system, N-Force. The ATF representative said that if the FBI builds a generic system that other agencies can use, it will be good for everyone; if not, it will not be very helpful to the ATF. In response, FBI officials said Sentinel will be a flexible system that other agencies can configure to meet their needs.

According to a DHS official, a DHS representative will participate with the FBI on the FBI Change Control Board. The DHS representative stated that during the early stages of the Sentinel project, the DHS provided four of its employees and two contractors to support the Sentinel PMO in the areas of case management, system analysis, biometrics, immigration enforcement, strategic planning, and technical architecture. Similar to concerns expressed by the ATF, the DHS hopes Sentinel will not be too FBI-specific so that it will be usable by other agencies. The DHS is developing its own case management system, the Consolidated Enforcement Environment, and expects to use some of the knowledge and reusable components from Sentinel to reduce the costs of DHS's own case management system.

Lockheed Martin's Observations on Sentinel

During our audit, we met with Lockheed Martin's project manager for Sentinel to obtain his perspective on how the project is progressing. The project manager stated that he is confident the project would meet its targeted budget and schedule, but that there were project risks that need ongoing attention. In his opinion, user acceptance and utilization was the most significant risk to the project. He explained that this risk is being addressed in several ways during the implementation of Sentinel. First, a prototype of the Phase 1 products were provided to agents in three field offices to obtain input on what should be added, removed, or changed. Similar assessments would be made in the future phases of Sentinel. Second, organizational change management strategies were being implemented within the FBI so that the transition from current workflows and IT systems used by agents and analysts to the new Sentinel workflow and systems would be facilitated. For example, Sentinel users will be trained as the system is brought online. This would allow users to immediately utilize the training on how to operate the system. System trainers will remain after the system is brought online in order to assist any users requiring further training or help. Finally, the project manager said that Lockheed Martin is taking steps to ensure that all of the significant workflows that will be affected by Sentinel will be addressed in planning the system. This will ensure that users will readily use the system to perform their day-to-day activities.

While the project manager viewed user acceptance and utilization as a significant risk, and Lockheed Martin is taking steps to ensure that the processes that need to be included within Sentinel are covered, we believe other risks are more significant, as discussed earlier in this report. In our view, because Sentinel will be the only FBI case file system and employees will have to use the system in order to perform their jobs, we do not believe user acceptance and utilization is a significant concern. However, a related risk, that all of the processes used by the FBI are included within the functionality of Sentinel, is a greater concern. We believe that the steps being taken by the FBI and Lockheed Martin should ensure that all of the necessary workflow processes are included within Sentinel. In future audits we will monitor whether agents and analysts are finding the new Sentinel applications to be user-friendly and include all of the required functionality necessary to perform their jobs.

Other risks the Lockheed Martin project manager identified include the control over system requirements, the migration of data from the antiquated ACS system to Sentinel, and the connectivity of all of the field offices to the Sentinel databases. He noted that the FBI is paying particular attention to the requirements of the system and making efforts to eliminate "requirements creep." The project manager pointed out that to date the FBI has only made six requests for change. Of those requests, one involved a security item that Lockheed Martin was implementing differently than the FBI anticipated. Lockheed Martin agreed to change the way the security issue was implemented and funded the changes through its management reserve. Four of the requests for change amounted to issues that were implemented at no cost and did not affect the project schedule. Lockheed Martin is considering the sixth request, which deals with the project's cost classification system.

The project manager told us that Lockheed Martin and the FBI are dealing with the risks involved in migrating ACS data to Sentinel. He explained that a software tool had been purchased to take the data from the ACS and "cleanse" it by determining the attributes of the data, placing the data into defined categories, and then placing the data into the correct locations in Sentinel. The significant risks of this process include the creation of rules to properly categorize the data within ACS and place it in Sentinel, and also what occurs when data is not properly cleansed. To address this risk, the software has been tested using sample case files. However, according to the project manager, until actual case file information is used, it will not be known how many of the case files will not be able to be cleansed and uploaded into Sentinel. For those case files that cannot be cleansed, a review board of Lockheed Martin and FBI personnel has been established to manually review the data and determine where it should be placed within the Sentinel system. Because no one knows how many case files will not be able to be cleansed, the time required to cleanse or review all of the ACS case file data cannot be estimated. As discussed earlier in this report, we consider the migration of data from ACS into Sentinel as a significant risk that could affect both the cost and schedule of bringing Sentinel fully online.

The last risk the Lockheed Martin project manager cited was that of the FBI's IT infrastructure being able to adequately handle the signal traffic over its networks. With the creation of a true electronic case file system that will be used by about 15,000 agents and analysts on a continuing basis, a substantial network is required so

that the information can be passed quickly within the system. According to the project manager, Lockheed Martin is not responsible within the Sentinel contract to ensure that the FBI's entire network operates efficiently. Instead, Lockheed Martin is responsible for building the hardware and software portions of Sentinel that will be located at two sites, one as the primary site and the second as a backup site. The FBI is responsible for networking the system. We agree with Lockheed Martin that the connectivity of Sentinel is a major concern, and we will be following up on this concern in future audit work.

The project manager said that from his perspective Lockheed Martin and the FBI are working well together. Specifically, there has been significant interaction between the two groups in management meetings, including the risk boards that have been established both by the FBI and by Lockheed Martin. Working groups have also been established between the two organizations where Lockheed Martin's teams responsible for drafting products are working with FBI staff responsible for reviewing the products, thereby providing clear communications on what is expected for each product. Overall, the project manager believed that the FBI is performing well its role as a good customer in providing direct feedback and maintaining the original requirements for the Sentinel project.

Regarding the Sentinel budget, the project manager stated that Lockheed Martin's costs possibly could be held to under the $305 million contract amount because of two changes in the implementation of the project. First, since the time of Lockheed Martin's proposal for the project, new hardware to house database files has come on the market that will lessen the cost of some aspects of the project. Second, the FBI reduced the requirement for the number of trainers needed by performing the training at fewer locations. The training plan originally called for about 120 trainers, but now requires only about 50 over the 6 to 7 weeks of implementation in the field for Phase 1.

Conclusion

By establishing stronger ITIM processes and an array of monitoring and control mechanisms, the FBI has positioned itself to better manage the Sentinel project and avoid the problems that occurred in the Trilogy and VCF projects. However, FBI officials agreed this does not mean that Sentinel is risk free. While the FBI has

corrected or alleviated many of the concerns we raised in our March 2006 report, several areas warrant continued attention to avoid potentially serious problems as the project progresses.

As a result of management improvements and the FBI's structuring of Sentinel into four phases, Sentinel poses much less risk to the FBI than the failed VCF project. Management improvements that reduce the risks include rigorous reviews and control gates required by the FBI's LCMD; new procedures to track and control costs; the use of an EVM system to detect deviations from cost, schedule, or performance baselines; a change management control process; and a risk management process. Risks are also minimized by the way the FBI structured the Sentinel program, such as the use of off-the-shelf components, conducting the project in a phased approach with specific deliverables, and the establishment of firm baselines and design requirements for each project phase. Further, the FBI will adopt the new information sharing standards required by the Department, has made progress toward completing and implementing plans for system security and the IV&V of the system, and has added staff to the Sentinel PMO.

However, some of the concerns from our March 2006 report remain. These concerns include: (1) uncertainty over the funding for the project and the effect on the FBI's operations should an unexpected level of reprogramming of FBI funds be required to continue Sentinel, and (2) the need to fill remaining vacancies in the Sentinel PMO to ensure proper FBI oversight of the project. In addition, our current review identified concerns over: (1) the uncertainty of total project cost estimates, and (2) the need for contingency plans for the risks the PMO is currently monitoring. Because the FBI has, in our judgment, only a tentative estimate of project costs, we believe the FBI needs to periodically update its cost estimate for the Sentinel project based on actual cost experience and inform Congress and the Department of any revisions to its estimate. We also believe the FBI should establish contingency plans for risks that could seriously affect the cost, schedule, or performance of the Sentinel project.

We believe the FBI's approach to the Sentinel project and the processes and controls it has developed, if implemented and followed, provide reasonable assurance that Sentinel can be developed and deployed successfully. However, there are serious project risks such as the ability to configure all of Sentinel's components into a seamless

system and to migrate ACS data into Sentinel. Project costs and funding are also somewhat uncertain. The OIG will continue to monitor and periodically issue audit reports throughout the four overlapping phases of the FBI's Sentinel project in an effort to track the FBI's progress and identify any emerging concerns.

Recommendations

We recommend that the FBI:

1. Ensure the management reserve is based on an assessment of project risks for each phase and for the project overall.

2. Periodically update the estimate of total project costs as actual cost data is available.

3. Complete contingency plans as required by the Sentinel Risk Management Plan.

4. Ensure that the IV&V process is conducted through project completion.

5. Complete hiring as soon as possible for the vacant PMO positions needed during the current phase of the project.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

This audit assessed the FBI's implementation of the contract 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:

- OMB Circular A-11 and Memorandum M-05-23,
- Executive Order 13356 (superseded by "Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect Americans," dated October 25, 2005),
- DOJ Order 2880.1b,
- Federal Acquisition Regulations,
- FBI Life Cycle Management Directive,
- Department of Defense Programmer's Guide to the Integrated Baseline Review,
- American National Standards Institute/Electronic Industries Alliance Standard 748A: Earned Value Management Systems, and
- National Defense Industrial Association Earned Value Management System Intent Guide and Surveillance Guide.

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 contract 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.

- Funding for Sentinel Phase 2 not completely identified.
- Contingency plans for project risks need to be developed.
- The FBI's Program Management Office for Sentinel is not yet fully staffed.

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 contracting 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 objectives of this audit were to determine: (1) the progress the FBI has made in resolving the concerns identified in our first report on the planning for Sentinel, and (2) if the contract with Lockheed Martin and the FBI's ITIM processes and project management are likely to contribute to the successful implementation of Sentinel.

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, DC, and at the FBI Sentinel Program Management Office in McLean, VA.

To perform our audit, we interviewed officials from the FBI, DEA, ATF, DHS, and the Department of Justice. We also interviewed officials from Lockheed Martin and other contractors supporting the PMO. We reviewed documents related to the Sentinel contract; cost and budget documentation; Sentinel plans, processes and guidelines; and the prior OIG Sentinel report.

To evaluate the FBI's implementation of the Sentinel contract, we examined the contract as well as associated amendments and documentation, underlying cost estimates, and methodologies for contract modifications. We interviewed officials responsible for cost estimates, source selection, and contract award and implementation.

To update issues identified in the OIG's March 2006 Sentinel audit report, we interviewed responsible FBI and contractor officials and reviewed plans and procedures for IV&V, EVM, cost tracking, information sharing, and training. We also interviewed FBI officials and obtained updated status on issues related to financial reprogramming and PMO staffing.

APPENDIX 2

ACRONYMS

ACS	Automated Case Support
ANSI	American National Standards Institute
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BEARS	Budget Execution and Analysis Reporting System
CFO	Chief Financial Officer
CIO	Chief Information Officer
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIRB	Department Investment Review Board
EIA	Electronic Industries Alliance
EVM	Earned Value Management
FBI	Federal Bureau of Investigation
FICMS	Federal Investigative Case Management System
FMS	Financial Management System
FY	Fiscal Year
GAO	Government Accountability Office
GEMPC	Government's Estimated Most Probable Cost
GOTS	Government Off-the-Shelf
IBR	Integrated Baseline Review
IOC	Initial Operational Capability
IMPRB	Investment Management Project Review Board
ITIM	Information Technology Investment Management
IT	Information Technology
IV&V	Independent Verification & Validation
LCMD	Life Cycle Management Directive
LInX	Law Enforcement Information Exchange
MOU	Memorandum of Understanding
NIEM	National Information Exchange Model
O&M	Operations and Maintenance
OCIO	Office of the Chief Information Officer
OCM	Organization Change Management
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PMO	Program Management Office
R-DEx	Regional Data Exchange

RFC	Request For Change
UNI	Universal Index
VCF	Virtual Case File

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.

Prior OIG Reports on FBI Case Management Efforts

In March 2006, the OIG issued a report entitled *The Federal Bureau of Investigation's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System.* The report found that the FBI had taken important steps to address its past mistakes in planning for the development of Sentinel. The report identified the following areas of concern:

- the incomplete staffing of the PMO,
- the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations,
- Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems,
- the lack of an established EVM process,
- the FBI's ability to track and control Sentinel's costs, and
- the lack of complete documentation required by the FBI's ITIM processes.

The OIG concluded that these areas of concern required action and continued monitoring by the FBI, the OIG, and other interested parties.

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.

External Reports on FBI Case Management Efforts

In May 2006, the GAO released a report titled *Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets* that was critical of the FBI's controls over costs and assets of its Trilogy project. The GAO found that the FBI's review and approval process for Trilogy contractor invoices did not provide an adequate basis for verifying that goods and services billed were actually received and that the amounts billed were appropriate, leaving the FBI highly vulnerable to payments of unallowable costs. These costs included first-class travel and other excessive airfare costs, incorrect charges for overtime hours, and charges for which the contractors could not document costs incurred. The GAO found unsupported and questionable costs in the amount of $10 million. The GAO also found that the FBI failed to establish controls to maintain accountability over equipment purchased for the Trilogy project. According to the GAO, poor property management led to 1,200 missing pieces of equipment valued at $7.6 million.

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 that:.

- 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. For example, 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*, reported that FBI personnel were not well-versed in the ACS system and other databases.

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.

APPENDIX 4

COST ESTIMATING METHODOLOGIES USED IN THE INDEPENDENT GOVERNMENT COST ESTIMATE

The Independent Government Cost Estimate methodology involves the use of six cost estimating techniques, detailed below. The method chosen to estimate each element of the project was based on the availability of technical and cost data.

Parametric Modeling - The parametric technique uses a compilation of historical data to formulate functional relationships (or models). These relationships are then used to predict the cost of the new system. The costs for custom-developed software were estimated using a commercial parametric modeling tool, CostXpert. Cost Estimating Relationships are a form of parametric estimation, but are separately defined for clarification.

Cost Estimating Relationships – Cost Estimating Relationships are factors that are applied against the known costs of a portion of the system under consideration to estimate the costs of an unknown portion of the system.

Analogy - Analogy estimation involves drawing parallels between the system under consideration and other systems for which technical and cost information is known.

Engineering Assessment - The engineering or "bottom-up" technique aggregates a cost estimate from resource estimates made at the lowest level possible. Often the estimate is compiled by determining the unit cost of each system component, multiplying by the quantity, and aggregating the results to product total system costs.

Vendor Quote - The vendor quote technique consists of gathering cost information directly from specific vendors, contract vehicles, and catalog resources.

Historical - The historical technique consists of using relevant past cost data from similar items to estimate the cost of the current item.

APPENDIX 5

RISK REGISTER

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
1	New model for data access and control (access rules) may impact Sentinel's schedule and budget.	Regarding APG, parallel development efforts may result in changes to Sentinel functional content or interface requirements and consume significant resources.	1	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces and funding strategy; incorporate into Sentinel plans as appropriate. M2. Identify critical interfaces and the phase they may impact Sentinel. M3. Establish WG to help establish ICDs with other projects (ICWG). M4. Establish MOUs with other projects as applicable. M5. Identify source of additional funding if required. M6. Document external systems and interface requirements for inclusion in the solicitation. M7. Establish a working partnership and collaborate with the legacy systems' owning organization (ITOD).
2	User requirements may change significantly as a result of the BPR initiative and impact Sentinel's schedule and budget.	Funding and schedule will not support project completion.	2	M1. Place the 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/needs. M4. Ensure contractors are aware and adhere to change process, including communication with user community. M5. Ensure core 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.

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
3	Absent an authoritative source of identity attributes, Sentinel must internally develop identity attributes for Role Based Access Control, and impact to be consistent with FBI Enterprise Service Directory Service requirements is unknown.	Time spent on creating Role Based Access Control may impact schedule.	2	M1 Seek FBI definition of authoritative identify attributes and authoritative sources M2 Establish identity attribute standards for Sentinel and FBI use M3 Seek FBI clarification of target directory architecture to support centralized management of authoritative identity attributes
4	Development contractor hiring is lagging resource need to complete design work.	Project plans, schedules and scope will require modification; Sentinel vision prolonged/ not achieved.	2	PM1. Identify the Government and support contractor resources, (and associated timeline, skills, et al.) in the Sentinel Project Plan. PM2. Assess the realism of Contractor staffing during Source Selection. PM3. Define security clearance requirements consistent with the access required by Development contractor personnel, likely reducing the number of TS security clearances required. M4. Require staffing plan submission, with clearance status, in project review reporting M5. Ensure active govt involvement in VAR resolution M6. LM has opened up hiring to all corporate divisions and Sentinel subcontractors and Corporate HR is assisting with surge support.
5	Lack of attendance or participation by users in training.	Poor or slow user acceptance of Sentinel.	1	M1-- Review the prime contractor's approach to market and provide outreach for each Sentinel phase. M2-- Validate training approach with pilot user group to be followed by Bureau executive endorsement. M3--Identify method to achieve or require sufficient level of training participation.

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
6	Activities related to data cleansing of data from phased out legacy systems may have been underestimated.	1. Requires GFE Data Staging partition by 11/1/06 (in FBI facility with C&A complete and Oracle 10g with RAC installed). 2a. Cleansed data will not be placed back into ACS which can result in a long term data synchronization problem. 2b. Placing cleansed data back into the legacy data base may impact those continuing to use legacy applications. 3. Need to maintain security control of data in staging area (Data will not be protected by ACS or Sentinel access controls) 4. Data cleansing is a Phase 2 risk mitigation activity and should not delay Phase 1 critical path activities.	1	<u>Consequence 1.</u> M1 Use new staging or SIT hardware to perform data cleansing. Delay data cleaning until receipt of hardware. <u>Consequence 2a.</u> M1 Data Migration alternative trade studies (IMS UID 2070 &3955) <u>Consequence 2b.</u> M1 Data Migration alternative trade studies (IMS UID 2070 &3955) <u>Consequence 3.</u> M1 Cleansing to be done only in FBI Facility M2 Access limited to select group read into "process". FBI only? <u>Consequence 4.</u> M1 Remove IMS dependencies between Data Cleansing and DCR/PDR/CDR

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
7	The evolving Enterprise Architecture can present new design constraints to Sentinel	To preclude non-compliance with Enterprise Standards, incorporation of changes, deviations, and/or corrective actions will impact cost, schedule and scope.	1	√M1. Monitor evolving standards; perform impact assessments; present assessments to TRB; file deviation request or incorporate as appropriate √M2. Participate in TRB and EAB and evaluation of technical inputs. EC submitted √M3. Develop method to influence EA, standards list, and monitor enterprise mandates (sys arch Mike Reed) √M4. Establish ICWG √M5. Ensure EA changes are forwarded to Sentinel for review and impact, with RFC developed if appropriate √M6. System Architect hired and has direct liaison with Enterprise Architect chief.
8	Data migration from phased-out legacy systems may have been underestimated	Some data may be lost or compromised, or ACS may not be able to be replaced	2	PM1. Identify all required data elements PM2. Develop mapping of ACS elements to Sentinel data requirements M3. Develop migration plan to support data conversion to new environment M4. Develop test plan to validate migration strategy √M5. Ensure management funds adequate to provide analysis if required. M6. Work with ITOD to determine scope of effort M7. Review results of previous data cleansing efforts for issues, provide lessons learned to LM M8. Ensure system design provides for migration. M9. Integration of data, design and migration IPTs

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
9	Use of PKI requires the user to change their logon routine from a UID/Password approach to using tokens, readers, and pin numbers. The transition to this mode of logon will inevitably antagonize many users, although, once they get used to it they most likely will not find it problematic.	The risk here is fundamentally one of having users fail to accept Sentinel because of, or in association with, their negative reaction to their initial use of PKI-enabled logon	2	M3 - Transfer Bureau roll-out and use of PKI enabled infrastructure to Trilogy prior to the Sentinel use so that the issue is addressed for most users independent of Sentinel. M4 - Decision will have to be made as to whether to use non-PKI enabled authentication for Phase 1. (Contractor must implement some form of authentication for "non-general" users) M5 - Add PKI to communications strategy (get the word out in training and all communications, etc.)
10	Proposed Controlled Interface solution does not meet the requirements for information sharing with systems classified higher than Collateral Secret (e.g., with Intelligence Community) and with systems at a lower classification level (e.g., state and local law enforcement).	Imprecise requirements could lead to scope creep.	2	M1 Investigate Intelligence Community certified products. M2 Evaluate cross domain design and present a design at Program Design Review (PDR) that most effectively meets required functionality and cross domain security requirements. M3 Evaluate product and design recommendations and adjudicate via Engineering Review Board (ERB) and Sentinel Configuration and Change Management Board (SCCMB).

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
11	LCMS is an interface to Sentinel, but the legacy program continues to modify the application, thereby adding to Sentinel's risk for uncontrolled scope, schedule, and cost.	Parallel development efforts may result in changes to Sentinel's functional or interface requirements that may cause delays or increase cost.	1	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into SENTINEL plans as appropriate √M2. Identify critical interfaces and the phase that they may impact Sentinel √M3. Establish WG to help establish ICDs with other projects (ICWG) M4. Establish MOUs with other projects as applicable M5. Identify source of additional funding if required PM6. Document external systems and interface requirements for inclusion in the solicitation. PM7. Establish a working partnership and collaborate with the legacy systems' owning organization (ITOD).
12	Privacy Impact Assessment (PIA) requirements impact cost and schedule	Cost and schedule could expand to accommodate new requirements	2	M1-- Work with OGC to define the hard system requirements and verify against the SRS, include OGC (PIA centric) personnel in our high level design meetings, so they can understand what and how various data elements are being used. M2-- Work with OGC and DNI to accommodate 'interim, best guess' requirements; comply with RFC process as requirements firm up M3-- Document DNI/OGC guidance through use of ECs

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
13	N-Dex is an interface to SENTINEL, but the program continues to modify the application, thereby adding to Sentinel's risk for uncontrolled scope, schedule, and cost.	Parallel development efforts may result in changes to Sentinel's functional or interface requirements that may cause delays or increase cost.	2	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into Sentinel plans as appropriate √M2. Identify critical interfaces and the phase that they may impact Sentinel √M3. Establish WG to help establish ICDs with other projects (ICWG) M4. Establish MOs with other projects as applicable M5. Identify source of additional funding if required PM6. Document external systems and interface requirements for inclusion in the solicitation. PM7. Establish a working partnership and collaborate with the legacy systems' owning organization (ITOD). M8. RFP to extend program has been published.
14	Audit Services (ESOC) is an interface to Sentinel, but the legacy program continues to modify the application, thereby adding to Sentinel's risk for uncontrolled scope, schedule, and cost. ESOC plans to use ArcSight, a COTS application LMSI also plans to use in Sentinel.	Parallel development efforts may result in changes to Sentinel's functional or interface requirements that may cause delays or increase cost. ArcSight client may impact Sentinel network connectivity, bandwidth and loads from passing data.	2	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into Sentinel plans as appropriate √M2. Identify critical interfaces and the phase that they may impact Sentinel √M3. Establish WG to help establish ICDs with other projects (ICWG) M4. Establish MOUs with other projects as applicable M5. Identify source of additional funding if required PM6. Document external systems and interface requirements for inclusion in the solicitation. PM7. Establish a working partnership (an IPT) and collaborate with the legacy systems' owning organization (ITOD).

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
15	DEEP is to be replaced by Sentinel, but the legacy program continues to modify the application, thereby adding to Sentinel's risk for uncontrolled scope, schedule, and cost.	Parallel development efforts may result in changes to Sentinel's functional or interface requirements that may cause delays or increase cost	3	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into Sentinel plans as appropriate √M2. Identify critical interfaces and the phase that they may impact Sentinel √M3. Establish WG to help establish ICDs with other projects (ICWG) M4. Establish MOUs with other projects as applicable M5. Identify source of additional funding if required PM6. Document external systems and interface requirements for inclusion in the solicitation. PM7. Establish a working partnership and collaborate with the legacy systems' owning organization (ITOD).
16	Requirement definitions necessitate inordinate customization of selected COTS/GOTS products (custom code)	Integrated solution will not facilitate expansion of services throughout the enterprise as envisioned	3	M1. Ensure min. functionality requirements can be identified M2. Conduct analysis of minimum requirements vs. proposed technical solution M3. Ensure at each phase and design review that solution is extendible to the enterprise M4. Tag milestones by phase to program schedule for monitoring

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
17	EDMS is an interface to Sentinel, but the legacy program continues to modify the application, thereby adding to Sentinel's risk for uncontrolled scope, schedule, and cost.	Parallel development efforts may result in changes to Sentinel's functional or interface requirements that may cause delays or increase cost.	4	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into Sentinel plans as appropriate √M2. Identify critical interfaces and the phase that they may impact Sentinel √M3. Establish WG to help establish ICDs with other projects (ICWG) M4. Establish MOUs with other projects as applicable M5. Identify source of additional funding if required PM6. Document external systems and interface requirements for inclusion in the solicitation. PM7. Establish a working partnership and collaborate with the legacy systems' owning organization (ITOD).
18	GUARDIAN is to be replaced by Sentinel, but the legacy program continues to modify the application, thereby adding to Sentinel's risk for uncontrolled scope, schedule, and cost.	Parallel development efforts may result in changes to Sentinel's functional or interface requirements that may cause delays or increase cost	4	M1. Actively engage parallel development efforts; develop MOUs for content, interfaces, and funding strategy; incorporate into Sentinel plans as appropriate √M2. Identify critical interfaces and the phase that they may impact Sentinel √M3. Establish WG to help establish ICDs with other projects (ICWG) M4. Establish MOUs with other projects as applicable M5. Identify source of additional funding if required PM6. Document external systems and interface requirements for inclusion in the solicitation. PM7. Establish a working partnership and collaborate with the legacy systems' owning organization (ITOD).

Rank	Risk Condition	Risk Consequence	Impact Phase	Mitigation Strategy
19	Policy does not currently exist to support the sharing of Sentinel information with external agencies.	The lack of policy could delay the implementation of information sharing capabilities.	1	M1 There is a requirement to have a data model that is compliant with the latest version of the Global Justice XML standard. This should accommodate the appropriate data elements. The program will track with the appropriate FBI divisions and the Global Justice XML standards groups to ensure that as updates occur; this information can be passed back to the appropriate Sentinel committees for action.
20	Development environment data is lost or corrupted.	Disaster event causes loss of SEI/ Development data resulting in key milestone/ schedule slippages.		M1 Develop a well defined Disaster Recovery Plan with contingencies for all types of anticipated disasters.

APPENDIX 6

THE FBI'S LIFE CYCLE MANAGEMENT DIRECTIVE

The FBI's IT Systems Life Cycle Management Directive (LCMD) is comprised of interrelated components. They include Life Cycle Phases, Control Gate Reviews & Boards, and Project Level Reviews. Sentinel is currently in the Design phase of the LCMD.

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.

Control Gate Reviews & Boards

The approvals to proceed from one phase to the next occur through seven control gates, where management boards meet to discuss and approve or disapprove a project's progression to future phases of development and implementation. 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.

Project-Level Reviews

Project-level Reviews support the IT Systems Life Cycle process. Project Level Reviews determine program or project readiness to proceed to the next activities of the project life cycle. Each Project Level Review feeds information up to the Executive-level Control Gates, as data is developed and milestones are completed.

FBI LCMD 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

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.

EXECUTIVE REVIEW BOARDS RESPONSIBLE FOR 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.

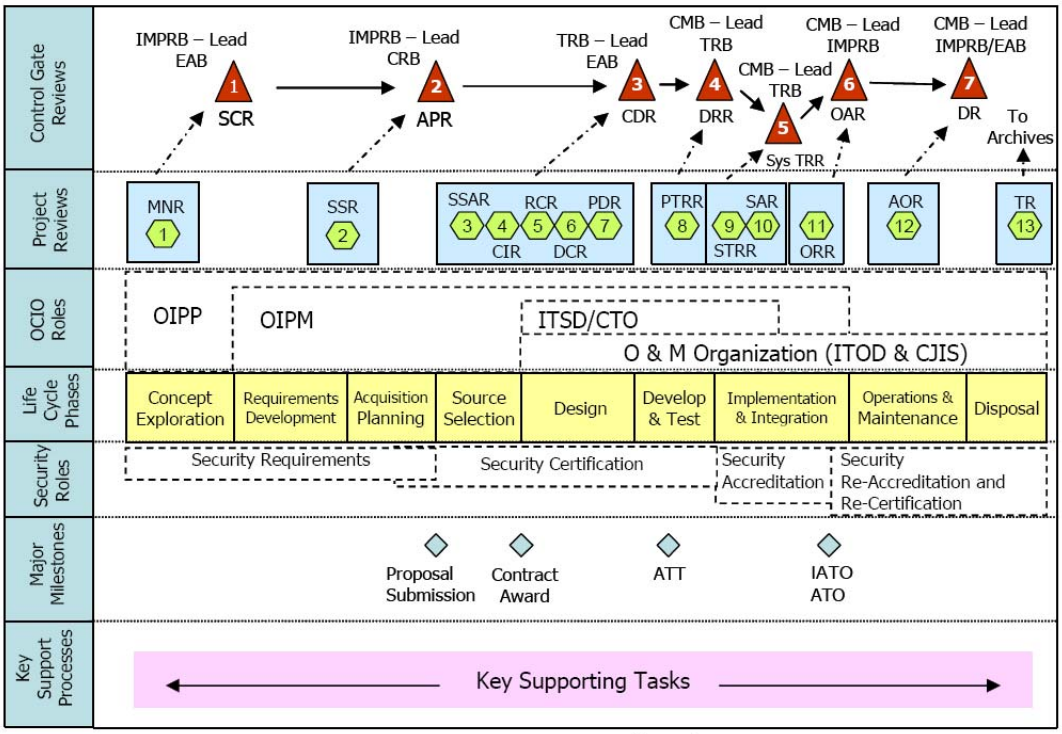
- The Enterprise Architecture Board ensures that IT systems comply with Enterprise Architecture requirements.

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

PROJECT LEVEL REVIEWS: CONCEPT EXPLORATION PHASE THROUGH DESIGN PHASE

REVIEW NAME	DESCRIPTION
1. Mission Needs Review	Examines the user need or technological opportunity, the deficiencies in the current set of systems, alternative and the proposed solution, and a business case or rationale for further investigating changes to the FBI's information systems.
2. System Specification Review	The decision point to proceed with the development of an Acquisition Plan, the allocation of high level system requirements to segment specifications, and the development of Project Plans that will manage the acquisition.
3. Source Selection Acquisition Review	Approves source selection results and authorizes contract negotiations.
4. Contract Implementation Review	The first Review between the customer and the solution provider following a contract award.
5. Requirements Clarification Review	Ensures the solution provider has a full understanding of the requirements for the system or segment and can articulate this understanding through proposed implementations of the requirement.
6. Design Concept Review	A review of the decomposition of the system or product (hardware, software, and manual operations).
7. Preliminary Design Review	Can be a single event or can be spaced out over time during the Design Phase to cover logical groupings of configuration items.

FBI'S LCMD IT SYSTEMS LIFE CYCLE



LEGEND

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

APPENDIX 7

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

Organizational Change Management (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 status.

Administrative Support

The Administrative Support staff directs the administrative and support services required by the Program Management Office.

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 8

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

November 7, 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--SENTINEL AUDIT II: STATUS OF THE FEDERAL BUREAU OF INVESTIGATION'S 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 "SENTINEL Audit II: Status of the Federal Bureau of Investigation's 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 me, on 202-324-2307, or Mr. Mio Lazarevich, SENTINEL Program Manager, should you have any questions. Mr. Lazarevich may be reached on 703-983-9610.

Sincerely,

Dean E. Hall
Project Management Executive

Enclosures

FBI Response to the DOJ/OIG Draft Audit Report
SENTINEL Audit II: Status of the Federal Bureau of Investigation's
Case Management System

Recommendation # 1: Ensure the management reserve is based on an assessment of project risks for each phase and for the project overall.

FBI Response: Agree. The FBI's Deputy Director governs the use of the management reserve through the Finance Division (FD). The SENTINEL Program Management Office (PMO) will work with FD and senior FBI management to determine the appropriate management reserve for each phase. The PMO asserts that 11 percent is an appropriate overall reserve amount and may be adjusted per phase depending on a comprehensive assessment of risk.

Recommendation # 2: Periodically update the estimate of total project costs as actual cost data is available.

FBI Response: Agree. Since contract award, the PMO, in conjunction with Lockheed Martin (Lockheed) and FD, has worked to revise projected program costs as appropriate, and will continue to do so over the life of the project. These changes will be communicated through budget requests and the OMB Exhibit 300 process.

Recommendation # 3: Complete contingency plans as required by the SENTINEL Risk Management Plan.

FBI Response: Agree. During the course of this audit, the Office of IT Policy and Planning (OIPP) released Version 2 of the FBI's Risk Management Plan. The most recent version only requires "contingency triggers" and plans for high risks. The SENTINEL Risk Management Plan is being revised so that it complies with the new OIPP risk policy. That being said, the first high risk was identified in mid-October. This risk was associated with schedule compression. The PMO is evaluating Lockheed's re-plan strategy and is developing contingency plans for this high risk.

Recommendation # 4: Ensure that the independent verification and validation process is conducted through project completion.

FBI Response: Agree. The FBI, as stated in the audit, will be providing experienced contractors to perform this service. Along those lines, the Independent Verification and Validation (IV&V) services will report to the CIO on both the PMO and Lockheed's performance as mandated by the program plan.

Recommendation # 5: Complete hiring as soon as possible for the vacant PMO positions needed during the current project phase.

FBI Response: Agree. The PMO continues to aggressively fill government and contractor positions. The two vacancies represent less than 5 percent of the total PMO staffing. The PMO believes that this is significantly less than government and industry levels, and will continue to actively recruit for positions before vacancies occur. Since the PMO requires contractors to have existing security clearances, contractor replacements have tended to be

very quick, generally less than 30 days. The six O&M vacancies that had been deferred are currently being finalized for recruitment.

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

Pursuant to the OIG's standard audit process, the OIG provided a draft of this audit report to the FBI on October 27, 2006, for its review and comment. The FBI's November 7, 2006, response is included as Appendix 8 of this final report. The FBI concurred with the five recommendations in the audit report. Our analysis of the FBI's response to the five recommendations is provided below.

The OIG also provided a draft of this report to Lockheed Martin for its review and comment. The comments Lockheed Martin provided were incorporated into this final report as appropriate.

Response to Recommendations

1. **Resolved.** In response to this recommendation, the FBI stated that the Sentinel PMO will work with the Finance Division and senior FBI management to determine the appropriate amount of the management reserve for each phase. The PMO believes that 11 percent is an appropriate overall reserve amount and that the amount of each phase's reserve may be adjusted based on a comprehensive assessment of risk. The FBI also noted that, through its Finance Division, the FBI's Deputy Director governs the use of the management reserve. This recommendation can be closed when we receive documentation showing the management reserve is based on an assessment of the project risks for each phase and for the project overall.

2. **Resolved.** This recommendation is resolved based on the FBI's agreement to periodically update its estimate of total project costs as actual cost data is available. The FBI said that since the award of the Sentinel contract, the PMO has worked in conjunction with Lockheed Martin and the Finance Division to revise projected program costs as appropriate. The FBI said it will communicate any changes to program costs through budget requests and the OMB Exhibit 300 process. This recommendation can be closed when we receive documentation showing the FBI has periodically updated the estimate of total project costs as actual cost data becomes available.

3. **Resolved.** This recommendation is resolved based on the FBI's agreement to complete contingency plans as required by the Sentinel Risk Management Plan. The FBI noted that Version 2 of the FBI's Risk Management Plan, recently released by its Office of IT Policy and Planning, requires contingency triggers and contingency plans only for high risks. The FBI said the Sentinel Risk Management Plan is being revised to comply with this new policy. However, the FBI advised us that Sentinel had identified its first high risk in mid-October and was developing a contingency plan to address it. This recommendation can be closed when we receive documentation showing that the FBI has completed contingency plans as required by the Sentinel Risk Management Plan.

4. **Resolved.** The FBI agrees with this recommendation, stating that it will provide experienced contractors to conduct an independent verification and validation process throughout the project. The independent verification and validation contractor will report to the FBI's CIO on both the performance of Lockheed Martin and the Sentinel PMO. This recommendation can be closed when we receive documentation showing that the FBI has ensured that the independent verification and validation process is conducted through project completion.

5. **Resolved.** The FBI agrees with this recommendation and said that the Sentinel PMO continues to work aggressively to fill government and contractor positions. The FBI noted that the two vacancies cited in our report represent less than five percent of the PMO's total staff. The Sentinel PMO believes this vacancy rate is significantly less than government and industry levels. The FBI said that the Sentinel PMO requires contractors to have existing security clearances, allowing its contractors to fill vacancies usually within 30 days. The six operations and maintenance vacancies discussed in our report are currently being finalized for recruitment. This recommendation can be closed when we receive documentation showing that the FBI has completed hiring for the vacant PMO positions needed during the current project phase.