

REDACTED FOR PUBLIC RELEASE



SENTINEL AUDIT III: 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 07-40
August 2007

REDACTED FOR PUBLIC RELEASE

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

EXECUTIVE SUMMARY

In March 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 case management system. 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 staff and administer the FBI's Sentinel Program Management Office (PMO), with the total estimated cost of Sentinel at \$425 million. The initial schedule for the Lockheed Martin contract called for all phases to be completed in December 2009.

On June 19, 2007, the FBI announced that it had fully deployed Phase 1 of Sentinel to provide FBI employees with user-friendly, web-based access to information currently in the FBI's antiquated Automated Case Support (ACS) system and improved search capabilities.¹ Phase 1 of Sentinel features a personal workbox, which summarizes a user's cases and leads, and a squad workbox, which allows supervisors to better manage resources and make assignments.²

The Sentinel project integrates commercial off-the-shelf (COTS) components and eventually 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 that, "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

* 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 ACS is the FBI's current case management system. Deployed in 1995, ACS is a mainframe computer system.

² A lead is a request from any FBI field office or headquarters for assistance in the investigation of a case.

REDACTED FOR PUBLIC RELEASE

support our current priorities, including our number one priority: preventing terrorist attacks.”³

Audit Approach

The Office of the Inspector General (OIG) is performing audits of the Sentinel project at the request of the FBI Director and congressional appropriations and oversight committees. This audit is the third in a series of audits on Sentinel that the OIG intends to conduct to evaluate Sentinel’s progress and implementation. The objectives of this third audit were to evaluate: (1) the status of the project, including the FBI’s monitoring of the contractor’s performance during Phase 1, (2) the planning for and progress of Phase 2, and (3) the resolution of concerns identified in our two previous Sentinel audits.⁴ Future OIG audits will continue to examine the progress of Sentinel over its remaining phases and assess whether Sentinel’s cost, schedule, performance, and technical benchmarks are being met.⁵

OIG Audit Results in Brief

Phase 1 of Sentinel, which was completed on June 19, 2007, delivered two key project components: a web-based portal to ACS and workboxes that summarize case information. The user friendliness of the portal and workboxes should enhance access to information and case management within the FBI. The FBI deferred one deliverable initially planned for Phase 1 because it would be more technically feasible to accomplish it in Phase 2, and the FBI did not clearly articulate which components of another deliverable would be accomplished in Phase 1 and which components would be accomplished in later project phases. While we cannot yet assess the

³ FBI Press Release entitled *FBI Announces Award of Sentinel Contract*, March 16, 2006.

⁴ See 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; and Department of Justice, Office of the Inspector General, *Sentinel Audit II: Status of the Federal Bureau of Investigation’s Case Management System*, Audit Report Number 07-03, December 2006.

⁵ Although we originally intended to cover the early stages of Phase 2 of Sentinel in this report, Phase 2 had not yet begun when our audit fieldwork was completed in May 2007. However, we evaluated the impact the FBI’s experience with Phase 1 had on how the FBI plans to approach Phase 2. We will evaluate progress under Phase 2 of the project in our next audit.

REDACTED FOR PUBLIC RELEASE

full impact of completing an original Phase 1 deliverable in a subsequent project phase, some future cost and schedule pressures may result. In addition, we question why cost adjustments did not occur in Phase 1 due to reduced requirements.

In addition, Phase 1 was completed in about 14 months instead of the planned 12 months. Our audit found the following four primary causes for this short delay: (1) an unrealistic schedule, (2) delays by Lockheed Martin in fully staffing the project with appropriately experienced personnel, (3) challenges in integrating the various COTS software components to work as a system, and (4) problems in assessing the project's progress against the approved schedule.

Our audit found that one of the four deliverables initially planned for completion in Phase 1 was deferred to Phase 2: cleansing the data in the electronic case file module of ACS so that the data is in a uniform format for eventual transfer (migration) to Sentinel. As the Sentinel project progressed, the FBI determined that the data cleansing planned for Phase 1 posed significant risks to the integrity of the data and should be moved to Phase 2. In addition, the FBI did not adequately define one of the four Phase 1 deliverables, the foundational components of a service-oriented architecture.⁶ Because the FBI's expectations for implementing a service-oriented architecture in Phase 1 were vague, we could not assess whether Phase 1 achieved its objectives in this area. FBI officials said that Phase 1 delivered an enterprise service bus, which they said was the only foundational component of a service-oriented architecture that was appropriate for this initial phase of the project.⁷

Our audit also found that the costs for the Sentinel project have increased a small amount from the initial estimates for Phase 1. As a result of a series of contract modifications, some of which pre-purchased software for Phase 2, the budget for the Phase 1, including award fees, increased from \$57.2 to \$59.7 million. However, the overall contract value of \$305 million did not change. Lockheed Martin also estimates that its costs exceeded the revised contract amount by approximately \$4.4 million due to requirements the FBI added but did

⁶ A service-oriented architecture is a software design approach in which software components, called services, can be re-used by multiple software applications.

⁷ An enterprise service bus is software "middleware" that connects software components and allows the components to communicate with each other.

REDACTED FOR PUBLIC RELEASE

not include in contract modifications. However, both parties agreed that Lockheed Martin would be paid the \$59.7 million amount in the revised budget, which includes the \$2 million budgeted for award fees.⁸ Over the course of Phase 1, the FBI deferred a total of 57 mostly low-level requirements from Phase 1 to later phases because they were outside of the scope of Phase 1, did not add value to Phase 1, or required the modification of ACS. Despite the somewhat decreased functionality Lockheed Martin was required to deliver in Phase 1, none of these deferrals resulted in a decrease in the cost of Phase 1.

At the time of our audit, the FBI's activities for Phase 2 of the Sentinel project were limited to planning for that phase. However, we believe the FBI gained valuable experience during Phase 1, and the lessons learned can improve the implementation of Sentinel's remaining phases. Based primarily on the FBI's experience in dealing with the legacy ACS system during Phase 1 of the project, the FBI has begun to reexamine whether dividing development and implementation of Sentinel into four phases was still the most effective way to manage the work on the project. When our audit concluded in May 2007, the FBI had not yet decided on the number of remaining phases or the content of them.

Since the project began, the FBI has implemented several management controls and processes designed to help it adequately manage the development of Sentinel and bring it to a successful conclusion. We reviewed four of these controls and processes in-depth: (1) earned value management, (2) independent verification and validation, (3) risk management, and (4) bill of materials. We found that the FBI has made significant progress in each of the four, but that additional progress needs to be made in the implementation of earned value management, risk management, and the bill of materials. In our opinion, if implemented correctly these processes and controls can provide reasonable assurance of project success.

However, while the FBI has implemented earned value management to monitor Sentinel, the quality of Lockheed Martin's cost data concerns us and the FBI. For example, when Lockheed Martin notified the FBI that its costs exceeded the revised budget by \$4.4

⁸ Lockheed Martin did not receive an award fee. Instead, the FBI allowed Lockheed Martin to transfer the \$2 million budgeted for the award fee to the cost portion of the budget to cover the cost overruns.

REDACTED FOR PUBLIC RELEASE

million, Lockheed Martin's earned value management data continued to show that Lockheed Martin was within budget on the project.

The FBI also has created a list of 16 risks it is monitoring that are associated with the Sentinel project. While the FBI's establishment of a risk management program is a positive step, we have several concerns with the program's implementation, including irregular review of the risks, a lack of contingency plans, and incomplete plans to mitigate identified risks. We are also concerned that the personnel assigned to manage these risks may not have sufficient time or expertise to adequately develop and implement a strategy to reduce the risks Sentinel faces.

Our audit also determined that the FBI has made good progress in addressing most of the concerns we identified in our two previous audits of the Sentinel project. Five of the 12 recommendations made in our prior reports have been closed, and the FBI is in the process of taking action to close the remaining recommendations. For example, in addressing one of our key recommendations, the FBI developed a plan and hired a contractor to perform independent verification and validation of the project's development. To close the remaining recommendations, the FBI must complete system security and training plans, fully staff the PMO, determine the appropriate amount of management reserve for the phases of Sentinel, and develop adequate contingency plans for Sentinel. We will continue to monitor the FBI's progress in implementing the remaining open recommendations.

In sum, the first phase of the Sentinel project is complete, although with some difficulty and without providing all of the deliverables originally intended for this phase of the project. Moreover, the most difficult portions of the project lay ahead. As Sentinel progresses, the FBI must ensure the deliverables for each phase are clearly documented and communicated to FBI management and oversight entities. We believe that the lessons learned during Phase 1, combined with the processes the FBI has established to manage and control the Sentinel project, can help provide reasonable assurance of Sentinel's ultimate success. However, rigorous implementation of processes and lessons learned is necessary to minimize any significant deviations from cost, schedule, technical, or performance baselines.

Background

The Sentinel project follows the FBI's unsuccessful 3-year, \$170 million effort to develop a modern investigative case management system called the Virtual Case File as part of the FBI's Trilogy information technology (IT) modernization project. The Virtual Case File originally was intended to provide the FBI with a modern system so that the existing obsolete ACS system could be retired. During multiple OIG reviews over the past several years, we reported that ACS uses outmoded technology, is cumbersome to operate, and does not provide necessary workflow and information-sharing functions.

The Sentinel contract, awarded in March 2006 to Lockheed Martin through a government-wide acquisition contract, is a cost-plus-award-fee contract that uses task orders to complete work for each phase of the project.⁹ The cost of the original task order for Phase 1 of Sentinel was \$57 million. According to the contract, the FBI may exercise options for \$248 million to cover three additional phases of the project and future operations and maintenance costs. Under the terms of the contract, Lockheed Martin can also be rewarded for meeting established goals in four areas: project management, cost management, schedule, and technical performance. This type of contract and award fee structure is common for large government IT projects.

While this type of contract proved problematic under Trilogy, our two prior Sentinel audits 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. As we reported in each of our two previous Sentinel audits, we believe the FBI is establishing clear milestones and requiring critical decision review points in managing this contract. For instance, if the contractor does not meet its milestones, it is penalized by loss of the award fee.

The FBI's initial plan called for implementing Sentinel's 4 phases over 45 months, with each phase providing distinct capabilities until the project is fully functional in December 2009. Originally, the FBI

⁹ An award fee is a financial incentive provided to a contractor based on the contractor's performance. A task order specifies the services required and the negotiated terms at which they will be provided, subject to the terms of the contract.

REDACTED FOR PUBLIC RELEASE

expected to complete each of the phases in 12 to 16 months. As discussed later in this report, however, the FBI is now considering a modification of the four-phase approach based on its experience with the first phase.

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

- Phase 1 introduces the Sentinel portal to provide access to data from the existing ACS system and eventually, through incremental changes in subsequent project phases, will support access to the newly created investigative case management system. Phase 1 also provides a case management personal workbox that presents a summary of all cases in which the user is involved, rather than requiring the user to perform a series of queries to find the cases as is necessary in the ACS system. In addition, a squad workbox will facilitate management of cases. The Findings and Recommendations section of this report contains a more comprehensive discussion of the Phase 1 deliverables.
- 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, 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 FBI employees' ability to "connect the dots" among various pieces of information and 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.

Phase 1 Schedule, Cost and Performance

When Lockheed Martin delivered Phase 1 of Sentinel on June 19, 2007, 2 months behind the proposed schedule, the revised contract amount had increased from \$57.2 million to \$59.7 million due to an overall increase in the scope of work, including pre-purchasing software for Phase 2. However, Lockheed Martin's costs exceeded the revised contract amount – including \$2 million budgeted for award fees – by approximately \$4.4 million. Lockheed Martin and the FBI agreed that Lockheed Martin would only be paid \$59.7 million, the amount of the revised budget, rather than being paid the entire \$4.4 million overage. FBI officials stated that the net project cost remained the same due to offsetting adjustments to the Phase 1 and Phase 2 budgets, and there was no change in the overall contract value.

At the conclusion of Phase 1, Lockheed Martin delivered two key deliverables: a web-based portal to ACS and case management workboxes. The FBI deferred to Phase 2 another deliverable, the cleansing of data in ACS's electronic case file module for migration into Sentinel. As a result of deferring this deliverable to Phase 2, Sentinel's total costs may be higher than currently projected. The FBI's expectations for implementing a service-oriented architecture in Phase 1 were vague, so we could not fully assess whether Phase 1 achieved its objectives in this area. However, the FBI's explanation that the enterprise service bus was the only appropriate component of a service-oriented architecture for Phase 1 appears reasonable, and that component was delivered.

Schedule Delay

Our audit found the following four primary causes for the 2-month delay in the delivery of Phase 1: (1) an unrealistic schedule, (2) delays by Lockheed Martin in fully staffing the project with appropriately experienced personnel, (3) challenges in integrating the various COTS software components to work as a system, and (4) problems in assessing the project's progress against the approved schedule.¹⁰

¹⁰ Although we view the schedule as unrealistic, FBI officials in commenting on a draft of this report stated that they would describe the schedule as aggressive, rather than unrealistic, because had Lockheed Martin been able to provide adequate staffing from the beginning, the 12-month schedule might have been met.

Unrealistic Schedule

According to FBI officials, Lockheed Martin based its Phase 1 project schedule on the FBI's proposed notional, or hypothetical, schedule created prior to formally soliciting proposals for development of Sentinel. That schedule divided the project into four phases, identified deliverables for each phase, and provided an estimated timeline for completion of each phase. While information the FBI provided potential vendors advised that they were free to propose a different number of phases or change the deliverables of each phase, vendors still had to meet the FBI's target completion date of 2009. In addition to broad outlines of the project's overall schedule, the FBI also dictated certain project milestones in the Sentinel Statement of Work. The Sentinel Program Manager told us that, in retrospect, the timeframes outlined in the Statement of Work were overly aggressive because they did not allow Lockheed Martin adequate time to staff the project.

Delays in Staffing

Almost immediately following the contract award, Lockheed Martin fell behind in its projected staffing levels. The FBI attributed this to the difficulty in hiring qualified personnel with top secret clearances and personnel costs 25 to 40 percent higher than Lockheed Martin projections. A 6-month suspension in processing security clearances for government contractors shortly after the Sentinel contract was awarded also depleted the supply of cleared contractor personnel and increased the cost of hiring those who were available.¹¹

In addition, Lockheed Martin and the FBI also underestimated the level of expertise in integrating COTS software that personnel would need for the Sentinel project. In a January 2007 briefing to the FBI's Associate Deputy Director, the Sentinel Program Manager said that both the FBI and Lockheed Martin based their original personnel cost estimates on the assumption that most of the work could be completed by recent college graduates, an approach Lockheed Martin had successfully used on a large scale information technology project

¹¹ According to the FBI, shortly after the Sentinel contract was awarded the Defense Security Service, the organization responsible for performing background investigations and granting clearances, suspended its processing of clearances for all government contractors for 6 months due to significant backlogs.

REDACTED FOR PUBLIC RELEASE

at the Social Security Administration. However, several PMO and FBI Chief Information Office personnel said that throughout Phase 1 of Sentinel, the level of expertise required of the Lockheed Martin staff to deal with Sentinel's COTS software was not sufficient for the project, although they said that Lockheed Martin eventually added the required expertise. FBI officials said the quality of the Lockheed Martin staff had improved during the first phase, but that additional improvements need to be made if the subsequent phases of the project are going to be successful. Other FBI officials said, however, that Lockheed Martin should have considered contracting with the software manufacturers who developed the most challenging pieces of software to help with implementation.

Challenges of Integrating the Software

Several PMO officials, including the Sentinel Program Manager and Lockheed Martin's Deputy Project Manager, stated that integrating the various commercial off-the-shelf software modules that comprise Phase 1 of Sentinel into a system that functions as intended was a major challenge. For example, analyzing why a particular software problem occurred within such an integrated system was difficult due to the number of variables in complex systems such as Sentinel. The COTS software used in Sentinel is so complex that the Lockheed Martin Project Manger said that it is virtually impossible to complete a COTS-based system without hands-on experience with its component software packages. Another factor that compounded the general challenge of COTS integration was that Sentinel is based on cutting-edge software, some of which had bugs. In at least one case, the software manufacturer was not aware of a problem until notified by the FBI and Lockheed Martin. Because this was a new bug, the manufacturer had to research its cause and develop a solution before Lockheed Martin could implement the software patch.

Problems in Assessing Progress

PMO personnel said that the methodology used by Lockheed Martin to construct the Sentinel project's schedule made it difficult to assess the project's progress. Specifically, they cited the following concerns about the schedule:

- Overuse of "hard constraints." Hard constraints are specific dates entered into a schedule that require a task to begin or end on that date, regardless of any other activity within the schedule. Hard constraints cloud an assessment of the

REDACTED FOR PUBLIC RELEASE

impact of schedule slippages because the scheduling software will assume that the task met the constraint, regardless of whether or not it did. Lockheed Martin's project schedule contained many hard constraints, which made assessing progress difficult.

- Logic problems. PMO officials said Lockheed Martin's schedule did not always accurately reflect the interdependence between tasks, often linking some that were not interdependent and not linking others that were interdependent.
- High percentage of "level-of-effort" tasks. Some of the tasks in the development of an IT system are referred to as "level of effort," meaning that progress toward completion of a task is measured by the passage of time rather than progress toward completing the task. Tasks that do not have a defined deliverable, such as project management, are often measured using level of effort. However, because level-of-effort tasks are not tied to discrete deliverables, it is difficult to determine how much their completion contributes to the overall progress of a project. As a result, it is prudent to have a schedule with as few level-of-effort tasks as possible. Lockheed Martin's project schedule contained a significant number of level-of-effort tasks.

Cost and Deliverables

The contract awarded to Lockheed Martin to develop Sentinel represents about 72 percent of the total cost of the entire Sentinel project, so Lockheed Martin's ability to deliver its portion of Sentinel within budget is critical to the cost performance of the overall Sentinel project. As the result of a series of contract modifications, the value of Lockheed Martin's task order for Phase 1 increased from \$57.2 million at the time of the integrated baseline review (IBR) in May 2006 to \$59.7 million in March 2007. However, in June 2007 Lockheed Martin advised the FBI that it had incurred costs totaling \$64.1 million in the performance of Phase 1. Lockheed Martin attributed the cost overruns to unanticipated work in interfacing with existing FBI computer systems and modifications to the FBI's testing approach.

However we found that three factors obscured a precise accounting of Lockheed Martin's cost performance. First, even though the FBI transferred some Phase 1 requirements to later phases of the

REDACTED FOR PUBLIC RELEASE

project, it received minimal cost reductions on Phase 1 from Lockheed Martin for deferring completion of these requirements. Second, the FBI did not adequately define the foundations of a service-oriented architecture expected to be delivered in Phase 1 and did not tie all of the deliverables to the requirements agreed upon for Phase 1, making it difficult to evaluate what the Phase 1 budget was supposed to pay for. Third, the FBI transferred \$2.5 million in materials and services from Lockheed Martin's budget to the PMO's budget and increased the amount of equipment the FBI furnished for the project. As a result, the amount paid to Lockheed Martin understates the cost of the work Lockheed Martin was originally tasked with.

Requirements Deferred

Over the course of Phase 1, the FBI deferred a total of 57 mostly low-level requirements from Phase 1 to later phases.¹² Despite decreasing the amount of functionality Lockheed Martin was required to deliver in Phase 1, none of these deferrals resulted in a decrease in the cost of Phase 1. According to the FBI, it deferred most of the 57 requirements because it decided the requirement was outside of the scope of Phase 1, did not add value to Phase 1, would require the modification of ACS, or would duplicate a capability included in a future phase of Sentinel. FBI officials said they did not believe it was prudent to invest in upgrading ACS because Sentinel is intended to replace it.

We recognize that phased projects using COTS components often transfer requirements from one phase to another and, in general, we do not disagree with the FBI's transfer of these 57 requirements. However, as noted previously, we are concerned that the FBI did not require that Lockheed Martin determine the financial impact of not doing this work in Phase 1 and adjust the cost of Phase 1 accordingly.

Phase 1 of Sentinel has delivered a web-based user interface to ACS data, giving a much more modern look and feel to ACS data and allowing users to navigate through the database using a mouse. For example, users can view and download ACS documents. However, this version of the web-based portal does not allow users to perform all of the functions included in ACS, meaning that FBI personnel may

¹² For example, the requirement that Sentinel be able to perform unstructured searches against items collected during investigations was deferred from Phase 1 to Phase 2.

also need to continue using the old system as well. Because many of the functions now performed by ACS will not be incorporated into Sentinel until Phase 2, the Phase 1 web portal to ACS will be used only until the completion of Phase 2.

As a result, the FBI decided that duplicating all of ACS was not cost effective and chose instead to include only the most frequently used functions in the Phase 1 portal. FBI officials said they recognize in retrospect that they overlooked some critical functions in the Phase 1 portal, such as the ability to upload documents into ACS, and that Phase 1 should have incorporated those functions.

Deliverables III-Defined

Throughout the Sentinel project, FBI documents, including slides from weekly briefings of the FBI Director, have shown four major anticipated deliverables for Phase 1: (1) a web-based portal to ACS, (2) a case workbook, (3) the foundational components of a service-orientated architecture, and (4) data cleansing of the electronic case file portion of ACS. As implemented, Phase 1 delivered the most important deliverables, the ACS portal and case workbook. Because the foundational components of a service-oriented architecture were ill-defined, we could not evaluate the extent to which this deliverable was achieved. However, FBI officials stated that the only component applicable to Phase 1 was the enterprise service bus, which was delivered. They said that the fourth planned deliverable, the data cleansing of the electronic case file portion of ACS, was deferred because it was more technically feasible to do so.¹³ As Sentinel progressed through the life cycle management process, the FBI's internal technical reports have noted this divergence from the original set of deliverables.

Neither the foundational components of a service-oriented architecture nor the data cleansing of electronic case file data were specified in the requirements for Phase 1, so the deferral of these goals did not require the deferral of requirements. However, achieving both of these goals may potentially require additional financial and personnel resources. And as mentioned previously, deferral of these goals did not result in a corresponding decrease in the Phase 1 contract amount.

¹³ See page 34 for a discussion of the common components of a service-oriented architecture.

REDACTED FOR PUBLIC RELEASE

The FBI's Incremental Development Plan, which was provided to all potential Sentinel bidders as a framework from which to describe the intent of the Sentinel program, refers to a service-oriented architecture framework and foundational services but does not define these terms. The FBI said that as a result, it had no expectation that Lockheed Martin would specifically address the commonly recognized basic components of a service-oriented architecture in Phase 1.

The Incremental Development Plan does not include any data cleansing or data migration capabilities for Phase 1. Rather, the plan states "There are no specific requirements for migration of case data in Phase 1." However, Lockheed Martin's proposal included data cleansing of electronic case file data as part of Phase 1 in preparation for the data's transfer, or migration, to the Sentinel database in Phase 2. The FBI subsequently agreed to Lockheed Martin's data cleansing approach and the proposed scope of the data cleansing efforts was built into the project's integrated master schedule. However, as stated above, after further consideration the FBI deferred data cleansing until Phase 2 because it had technical concerns with cleansing data in advance of migrating it.

While deferring the data cleansing to Phase 2 did not affect the functionality of Phase 1, it pushed time-consuming activities into Phase 2 and the FBI did not adjust the Phase 2 end date. In addition, similar to the deferral of requirements, the deferral of the data cleansing did not result in a decrease in the amount of the Phase 1 contract.

Costs Transferred

Through a series of six contract modifications during Phase 1, the FBI increased the total contract value of Phase 1 by \$2.5 million, from \$57.2 million to \$59.7 million. As expected in a project of Sentinel's size and complexity, some of the modifications increased the scope of Phase 1, while others decreased it. However, the decreases either transferred the cost for the tasks to the PMO budget or to the amount budgeted for Lockheed Martin's award fee. For example, in March 2007 the FBI issued a modification which deleted \$2.1 million for tape silos from the Phase 1 contract.¹⁴ Although the tape silos were still necessary for Phase 1, the FBI purchased silos with more

¹⁴ A tape silo is computer hardware that uses tapes to store large amounts of computer data.

storage capacity using funds from the PMO's budget and used the funds in the Lockheed Martin contract originally allocated to tape silos to offset the cost of additions to the scope of Phase 1. FBI officials stated that the various cost adjustments did not affect the overall contract value of \$305 million.

Phase 2 Planning and Project Management

The FBI has implemented several management controls and processes in addition to its life cycle management directive that are designed to help it adequately manage the development of Sentinel and bring it to a successful conclusion. In this audit, we reviewed four of these controls and processes in depth: earned value management (EVM), risk management, independent verification and validation, and bill of materials. We concluded that the FBI has made significant progress in each of the four areas, but that substantial additional progress is needed in risk management and the bill of materials.

In addition to these four areas, the FBI recognizes that the lessons learned during Phase 1 will aid the FBI in its planning of Phase 2. Although Phase 1 is complete, the most difficult portions of Sentinel development and implementation lay ahead. To reduce the risk to Phase 2 and subsequent phases of Sentinel, that the FBI must implement corrective actions resulting from the problems encountered during Phase 1.

It is also important to note that the FBI has taken action to alleviate or resolve most of the concerns identified in our first two audits of the Sentinel project relating to project management. We believe that the FBI's efforts to improve its project management capabilities can help provide reasonable assurance that the Sentinel project can be successfully completed, if the processes are implemented as intended.

Earned Value Management

As required by the Office of Management and Budget (OMB), and with Department of Justice (Department) guidance, the FBI has established an Earned Value Management (EVM) system for Sentinel. 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

REDACTED FOR PUBLIC RELEASE

status should 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 implemented and utilized, EVM allows project management to pinpoint potential problems and address them before they escalate.

The Sentinel contract requires Lockheed Martin to fully implement EVM in accordance with the Sentinel EVM plan, including having an EVM system that complies with American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard 748-A.¹⁵ This allows the FBI to gather EVM data on the development portion of the project through monthly electronic data transfers from Lockheed Martin.

Our review of EVM reporting from September 2006 to March 2007 showed that the FBI has continued to implement EVM and use that data to help manage Phase 1 of Sentinel. However, several issues decreased the effectiveness of EVM as a tool to manage the Sentinel development contract. The most significant issue was the reliability of the EVM data Lockheed Martin provided the FBI. In June 2007, the FBI rejected Lockheed Martin's April 2007 EVM data after Lockheed Martin notified the FBI that it estimated that it had incurred approximately \$64.1 million in costs during Phase 1 of Sentinel. Because the EVM baseline for Phase 1 was \$59.7 million, Lockheed Martin's estimate showed that its EVM system was not collecting accurate data on Sentinel costs as Lockheed Martin was accruing the costs – one of the primary purposes of an EVM system.

Further, while the FBI's implementation of EVM comports with the Department's guidance, it does not provide all the data that OMB believes necessary for oversight purposes. As a result of OMB concerns that the FBI reprogrammed or rebaselined Phase 1 of Sentinel without required OMB approval, we reviewed all changes to the time-phased budget used to measure Sentinel's progress.¹⁶ We

¹⁵ ANSI/EIA Standard 748-A is the criteria selected by the OMB for EVM systems. The standard includes 32 specific criteria in 5 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.

¹⁶ Reprogramming, or rebaselining, revises the project baselines and eliminates all cost and schedule variances. Rebaselining usually occurs when a project's progress deviates significantly from the original plan and the remaining time and funds are not sufficient to complete the project.

REDACTED FOR PUBLIC RELEASE

concluded that the FBI had not rebaselined the project, but that frequent replanning diminished the quality and usefulness of the EVM data for higher-level oversight.¹⁷

Independent Verification and Validation

In September 2006, the FBI obtained the services of Booz Allen Hamilton (Booz Allen) to perform the independent verification and validation function for the Sentinel project. Since then, Booz Allen has participated in FBI-only project meetings and joint FBI-Lockheed Martin project reviews. In addition, Booz Allen has provided written comments and recommendations on many project documents, and produced 15 project-status briefings and monthly reports. Booz Allen also produced monthly reports and biweekly briefings that were sent directly to the FBI's Chief Information Officer.

These reports and briefings highlight recent activities, upcoming events, and the independent verification and validation team's view of the overall status of the project, including a discussion of risks that could affect the project's cost, schedule, or performance. The independent verification and validation products also included recommendations and best practices observed by Booz Allen. As of May 2007, Booz Allen had made over 70 recommendations based on risks and other areas it identified. Booz Allen also reported several project management and oversight weaknesses that increased the risks associated with Sentinel, including concerns about:

- the ability of Lockheed Martin's developers to build Phase 1 to meet the FBI's needs before Lockheed Martin had completed the design; and
- the quality of most of the test procedures submitted by Lockheed Martin for the test readiness review.

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 should identify procedures used to

¹⁷ Replanning revises the time-phased budget for completing the work remaining in a project without any changes to the total scope of work, baselined cost, or scheduled completion of the project.

REDACTED FOR PUBLIC RELEASE

manage risk throughout the life of the program. Risks are categorized by severity and identified as either open or resolved. Open risks are tracked in a risk register maintained by the risk manager until resolved.

The FBI has created a list of 16 risks it is monitoring that are associated with the Sentinel project. While the FBI's establishment of a risk management program is a positive step, we have several concerns with the program's implementation, including irregular review of the risks, a lack of contingency plans, and incomplete plans to mitigate identified risks.

As required, the FBI has developed plans to mitigate the highest ranked risks. However, the mitigation plans for these top-ranked risks are incomplete because they do not include a method to measure whether the steps in the mitigation plan are effective. In addition, the FBI has developed contingency plans for only 50 percent of the risks that are required to have such plans. The Sentinel risk manager said that the mitigation plans do not include a method to measure their effectiveness because it is very difficult to develop accurate measures. However, we believe that risk management is critical to the success of Sentinel.

When a new risk is opened, the Sentinel Risk Review Board assigns an owner to that risk to develop a mitigation and contingency plan and to ensure that the mitigation plan is implemented. We support the idea of having one person taking a lead role – having "risk ownership" in managing each risk. However, this process does not appear to be functioning as intended. During interviews with risk owners we found that some could not explain the nature of the risks they had been assigned, while others said they thought they did not have the authority or capability to implement a risk's mitigation strategy.

With respect to currently identified project risks, we view Sentinel's ability to interface with existing FBI systems from which it will extract data as a potentially significant challenge. In Phase 1, Lockheed Martin had unanticipated problems connecting Sentinel with ACS because there was no detailed documentation describing how ACS works. Consequently, Lockheed Martin had to create the documentation itself. The Sentinel PMO did not anticipate this task because the managers of ACS told the PMO that all of the necessary documentation existed. Because this unexpected task strained both the Phase 1 budget and schedule, the PMO is now tracking

documentation for the other systems with which Sentinel must interface as a risk.

Bill of Materials

A bill of materials is a complete listing of all parts, assemblies, equipment, and software that make up an IT system, as well as the information required to construct new units of the system or order spare parts for it. Contractually, Lockheed Martin is required to purchase the list of items on the bill of materials it submitted with its proposal. As is to be expected in a project as complex as Sentinel, Lockheed Martin has needed to revise the bill of materials for several reasons including revisions to the project's design.

An accurate bill of materials is critical to ensuring the FBI approves all changes to Sentinel's design and that an accurate list of Sentinel's components is available to the FBI to use when reviewing Lockheed Martin's invoices. Because of the importance of an accurate bill of materials, the PMO established a Bill of Materials Deviation Policy, which establishes the criteria for what constitutes a change to the bill of materials and the criteria to assess whether Lockheed Martin needs the FBI's approval prior to making a change to the bill of materials.

According to the Sentinel Contracting Officer's Technical Representative, Lockheed Martin also established its own internal procedures for making changes to the bill of materials. However, Lockheed Martin employees viewed internal approval of changes as final approval to change the bill of materials and therefore did not submit all changes to the FBI as required. The PMO is aware of this and other shortcomings and has established a joint Lockheed Martin-FBI team to revise Sentinel's bill of materials policies and procedures to address these issues.

In addition to the issues with which the FBI was aware, we identified a significant flaw in Sentinel's Bill of Materials Deviation policy. While the policy states that a deviation is any addition or deletion to the bill of materials, the policy does not require FBI approval for additions or deletions. Instead, the policy only requires approval for cost increases and changes to purchase dates for items already on the bill of materials. FBI officials agreed that the deviation policy needs to address this issue.

REDACTED FOR PUBLIC RELEASE

Lessons Learned

Although Phase 1 was slightly delayed and over budget, the FBI appears to have learned important lessons that may allow it to reduce the risk to subsequent phases. We examined what the FBI had learned about integrating COTS software, interfacing with ACS, measuring progress, clarifying with Lockheed Martin the details of what must be done to meet a given requirement, scheduling reviews of Sentinel's design, and ensuring Sentinel's schedule accurately measures the project's progress. We believe that if the FBI implements the planned corrective actions resulting from these lessons, we believe the risk to subsequent phases of Sentinel should be reduced.

Actions Taken on Prior OIG Recommendations

During our audit, we examined the FBI's actions to address recommendations we made in our audit reports on Sentinel and found that the FBI was, in general, taking action to resolve our concerns. Based on the FBI's actions, we closed 5 of the 12 recommendations. We also noted that the FBI agreed with the remaining recommendations and was in the process of taking corrective action. Our recommendations dealt generally with the FBI's need to complete required planning and general management oversight policies and procedures for Sentinel in order to help ensure its success.

In our March 2006 report, we made seven recommendations, of which four have been closed. The FBI continues to address the remaining three recommendations that involve completing a system security plan, filling vacant positions within the Sentinel PMO, and completing comprehensive training plans for the project. We found during our audit that the FBI had completed its independent verification and validation plan, which partially closes one of the recommendations, but the system security plan still needs to be completed for full closure of the recommendation.

In our December 2006 report, we made five recommendations, one of which has been closed. The four remaining recommendations were that the FBI should: (1) develop contingency plans as required by the Sentinel Risk Management Plan, (2) provide experienced contractors to conduct an independent verification and validation process throughout the Sentinel project, (3) determine the appropriate amount of management reserve for each phase of the project, and

REDACTED FOR PUBLIC RELEASE

(4) fill the vacant Sentinel PMO positions needed to complete Phase 1 of the project.

As discussed earlier, we found that the FBI has improved in developing contingency plans as required by the Sentinel Risk Management Plan. However, as noted, we continue to have concerns about the FBI's management of risks in the Sentinel project. We also found that the FBI has begun utilizing a contractor to perform independent verification and validation and the contractor offered numerous recommendations during Sentinel's Phase 1. Because the independent verification and validation is being performed, this recommendation will be closed through our normal audit follow-up process.

For the two remaining open recommendations from our December 2006 report, we found that the FBI had not determined management reserve amounts for the remaining phases of Sentinel and did not fully staff the Sentinel PMO. Because Sentinel consists of four phases, each phase will have a separate task order and its own funding. At the end of our fieldwork for the current review, the PMO was still in the planning stage for Phase 2, which includes a risk analysis and cost implications for those risks. As a result, the management reserve had not yet been determined.

Regarding the staffing of the Sentinel PMO, we found that the FBI continued to make progress in its hiring of personnel. We found that 70 of 76 positions had been filled, and 3 individuals were pending for the remaining positions. The FBI also was planning for changes to be made in the PMO as the project evolved from planning and development to operations and maintenance.

We will continue to monitor the progress made by the FBI in implementing the remaining recommendations identified in our prior audits to ensure that the required planning and general management oversight policies and staff continue to be utilized effectively.

Conclusion

The FBI deployed the two most critical deliverables planned for the first phase of the Sentinel project – a web-based portal to ACS and personal and squad workboxes that summarizes users' cases and leads. These deliverables were completed slightly behind schedule and over budget. However, the most difficult portions of Sentinel to

REDACTED FOR PUBLIC RELEASE

implement lay ahead and several tasks originally planned for Phase 1 have been deferred to later phases.

We will monitor the quality of the Phase 1 product in our next Sentinel audit as FBI employees gain experience in using the portal and workboxes.

We believe that the lessons learned during Phase 1, combined with the processes the FBI has established to manage and control the Sentinel project, can help provide reasonable assurance of Sentinel's ultimate success. However, rigorous implementation of processes and lessons learned is necessary to minimize any significant deviations from cost, schedule, technical, or performance baselines.

OIG Recommendations

In this third Sentinel audit, we make nine recommendations to the FBI to help ensure the success of the Sentinel case management system and to better manage project costs. Among the recommendations are that the FBI limit the scope and duration of future project phases to make them more manageable; adjust the amount of task orders to reflect changes in project requirements; include both initial and revised performance baselines in EVM reports; improve the requirements for Lockheed Martin's cost reporting; improve risk management and the tracking of project deficiencies; and improve the bill of materials process.

TABLE OF CONTENTS

INTRODUCTION 1

- Background 1
- Sentinel..... 4
- Sentinel’s Phased Approach..... 5
- FBI Management Processes and Controls..... 7
- Earned Value Management System..... 8
- Prior Reports..... 9

FINDINGS AND RECOMMENDATIONS 13

- Finding 1: Phase 1 Schedule, Cost, and Performance 13
 - Schedule Delay 14
 - Causes for Delay 15
 - Tight Schedule Affected Implementation of
LCMD Processes 23
 - Lockheed Martin’s Cost Performance 25
 - Phase 1 Deliverables 28
 - Conclusion..... 37
 - Recommendations 38
- Finding 2: Phase 2 Planning and Management Issues 39
 - Management Controls and Processes 39
 - Planning for Phase 2 and Lessons Learned 60
 - Actions Taken on Previous OIG Recommendations..... 64
 - Conclusion..... 69
 - Recommendations 69

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS 71

STATEMENT ON INTERNAL CONTROLS 72

APPENDIX 1: OBJECTIVES, SCOPE, AND METHODOLOGY 73

APPENDIX 2: ACRONYMS..... 74

APPENDIX 3: THE FBI’S LIFE CYCLE MANAGEMENT DIRECTIVE 75

APPENDIX 4: PRIOR REPORTS ON THE FBI’S INFORMATION
TECHNOLOGY 83

REDACTED FOR PUBLIC RELEASE

APPENDIX 5: COMPARISON OF ACS, WACS, AND PHOENIX
FUNCTIONALITY TO SENTINEL'S
PHASE 1 DELIVERABLES..... 92

APPENDIX 6: INDEPENDENT VERIFICATION AND
VALIDATION ISSUES AND RECOMMENDATIONS 98

APPENDIX 7: RISK REGISTER OPEN RISKS 109

APPENDIX 8: PMO STAFF POSITIONS AND
RESPONSIBILITIES..... 123

APPENDIX 9: THE FEDERAL BUREAU OF INVESTIGATION'S
RESPONSE TO THE DRAFT REPORT 125

APPENDIX 10: OFFICE OF THE INSPECTOR GENERAL'S
ANALYSIS AND SUMMARY OF ACTIONS
NECESSARY TO CLOSE THE REPORT 129

INTRODUCTION

Background

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

On June 19, 2007, the FBI announced that it had fully deployed Phase 1 of Sentinel. The goal of this first phase of the project was to provide FBI employees with a user-friendly, web-based access to information currently in the FBI's antiquated Automated Case Support (ACS) system.¹⁸ Phase 1 features a personal workbox that summarizes a user's cases and leads.¹⁹ It also provides user-friendly search capabilities and a squad workbox, which allows supervisors to better manage their resources and assign leads with the click of a mouse.

According to the Sentinel 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 11 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

¹⁸ ACS is the FBI's current case management system. Deployed in 1995, ACS is a mainframe system.

¹⁹ A lead is a request from any FBI field office or headquarters for assistance in the investigation of a case.

REDACTED FOR PUBLIC RELEASE

management, workflow management, evidence management, search and reporting capabilities, and information sharing capabilities 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."²⁰

The Sentinel project follows the FBI's unsuccessful efforts to develop an automated case management system called the Virtual Case File (VCF), which was intended to replace the FBI's 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 third OIG report on Sentinel, and covers the development of Phase I of the project, planning for Phase 2, and progress made by the FBI in resolving the concerns identified in our two previous audits. The previous two reports focused on the planning for Sentinel, the FBI's processes and controls for managing information technology (IT) projects, 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 IT infrastructure and noted the 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.²¹

²⁰ FBI Press Release entitled *FBI Announces Award of Sentinel Contract*, March 16, 2006.

²¹ For a more complete discussion of the OIG's reports on Sentinel, see the Prior Reports section on page 9.

REDACTED FOR PUBLIC RELEASE

In its mission-needs statement for Sentinel, the FBI said 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 communications among FBI offices and with other law enforcement organizations.

In early 2004, after nearly 3 years of development, the FBI engaged several external organizations and contractors to evaluate the Virtual Case File (VCF), the third component 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 study evaluating the functionality of COTS and government off-the-shelf technology to meet the FBI's case management needs. Aerospace followed this study with an independent verification and validation (IV&V) report on the VCF, issued in January 2005, which recommended that the FBI pursue a COTS-based, service-oriented architecture.²² The IV&V report

²² IV&V is a standard information technology investment management (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.

REDACTED FOR PUBLIC RELEASE

concluded that a lack of effective engineering discipline led to inadequate specification, design, and development of the VCF.

The FBI modified its approach to developing the VCF, and in late 2004 divided the project into Initial Operational Capability and Full Operational Capability segments. The Initial Operational Capability segment assessed the VCF project and involved a pilot test of the most advanced version of the VCF in an FBI field office. In February 2005, the OIG issued a report on the Trilogy project questioning the FBI's ability to complete and deploy the VCF.²³

The FBI issued a final report on the Initial Operational Capability at the end of April 2005.²⁴ According to the report, the FBI terminated work on the VCF due to the lack of progress on its development. The FBI stated that it was concerned that the computer code being used to develop the VCF lacked a modular structure, thereby making enhancements and maintenance difficult. In addition, the FBI report said that the "marketplace" had changed significantly since the VCF development had begun, and appropriate COTS products, which were previously unavailable, were now available.

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 employees to maintain investigative lead and case data. 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.

²³ 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 05-07, February 2005.

²⁴ 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.

REDACTED FOR PUBLIC RELEASE

Therefore, the FBI has been working 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 is the use of COTS and government-off-the-shelf applications software. The FBI has been working to integrate the off-the-shelf products with an Oracle database, thereby separating the applications code from the underlying data being managed in order to simplify 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.

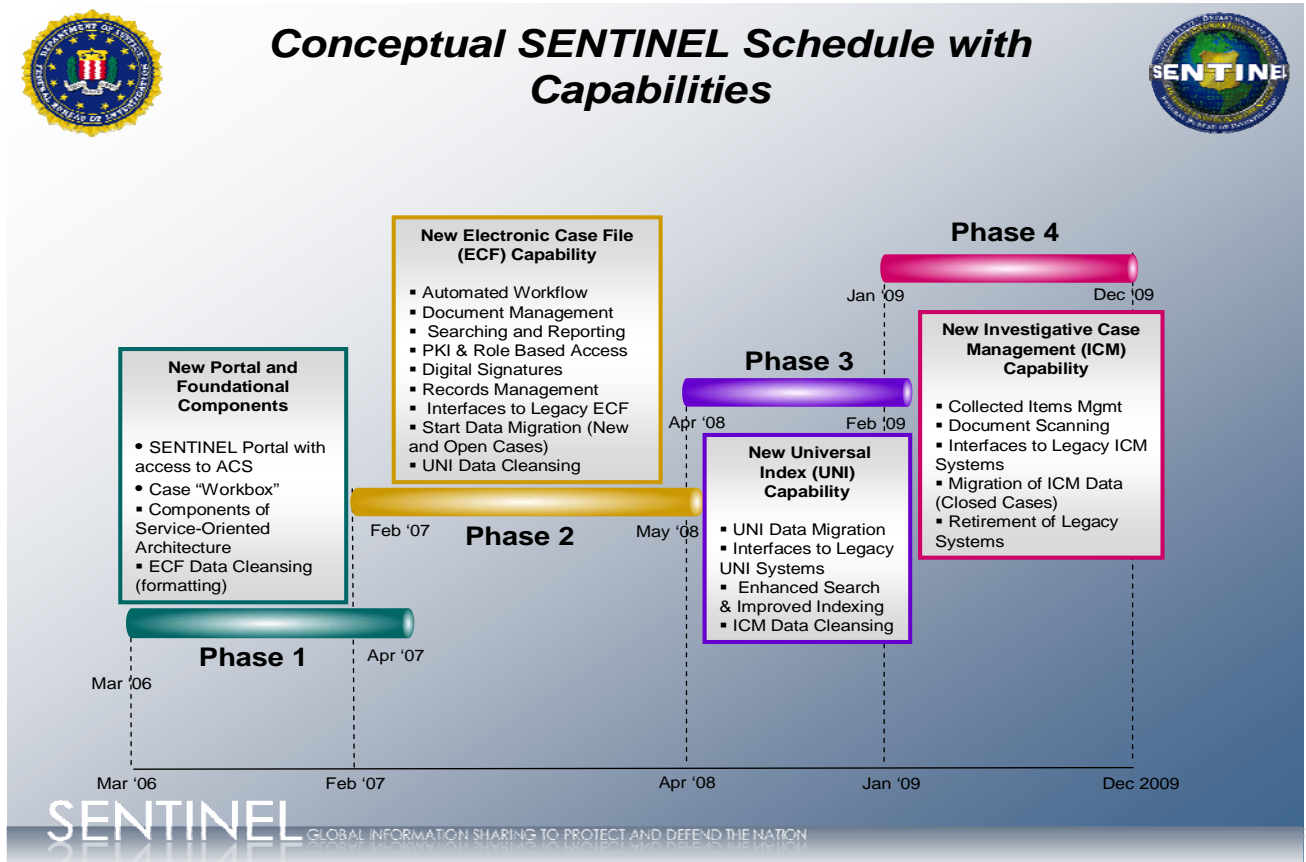
Currently, the documentation within case files is electronically managed through the ACS system, which maintains electronic copies of most documents in the case file and provides references to documents that exist in hardcopy only. Upon approval of a paper document, an electronic copy of the completed 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 will also be able to review, comment, and approve the insertion of documents into appropriate FBI electronic files through Sentinel.

Sentinel's Phased Approach

As originally conceived, the FBI expected to develop the Sentinel project in 4 partially overlapping phases, each lasting approximately 12- to 16-months. However, at the time of our audit the FBI was reevaluating the number of phases and the capabilities each phase will

deliver as it gained experience with the project's development. Each phase, when deployed, was to result in a stand-alone set of capabilities that could be added to by subsequent phases to complete the Sentinel project. The following chart shows the FBI's original conception of the four phases and their general timeframes.



Source: FBI

Phase 1 introduced the Sentinel web-based portal, which provides access to data from the existing ACS system. Eventually, through incremental changes in subsequent phases, the portal will display data from a newly created investigative case management system. Phase 1 also provides a case management workbook that presents a summary of all cases a user is involved with rather than requiring the user to perform a series of queries to find the cases as was necessary when only ACS was used. The Findings and Recommendations section of this report contains a more comprehensive discussion of the Phase 1 deliverables.

Phase 2, the most ambitious and technically difficult of the phases, will begin the transition to paperless case records and the implementation of electronic records management. A workflow tool

REDACTED FOR PUBLIC RELEASE

will support the flow of electronic documents through the review and approval cycles, and a new security framework will be implemented to support access controls and electronic signatures. Additionally, in Phase 2, the FBI will begin migrating data from the ACS electronic case file to Sentinel and preparing data from the Universal Index (discussed below) 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.²⁵ Enhancing the attributes will allow more precise and comprehensive searching within Sentinel and increase the FBI's 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 ACS 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.

FBI Management Processes and Controls

In the early stages of the Trilogy project, the OIG and U.S. Government Accountability Office (GAO) recommended that the FBI establish Information Technology Investment Management (ITIM) processes to guide the development of its IT projects. In response, in 2004 the FBI issued its Life Cycle Management Directive (LCMD). 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

²⁵ 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.

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 the project level reviews mentioned throughout this report are contained in Appendix 3.

The LCMD established policies and guidance applicable to all FBI IT programs and projects, including Sentinel. As we discussed 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 during the failed VCF effort. Since our March 2006 report on Sentinel, the FBI has further refined its LCMD and is applying the revised directive to Sentinel.

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 to 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 Office of Management and Budget (OMB) issued a memorandum requiring all federal agency Chief Information Officers (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. The Department of Justice issued its EVM policy in July 2006. In response to these requirements, the FBI developed a Sentinel Program EVM Capability Implementation Plan in August 2006 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.²⁶ Properly executed,

²⁶ The performance measurement baseline is a total, time-phased budget plan against which program performance is measured.

REDACTED FOR PUBLIC RELEASE

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 identified risks.

According to OMB guidance, 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.

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 GAO, the House of Representatives' Surveys and Investigations Staff, and others have made a variety of recommendations focusing on the FBI's management of its IT projects, particularly the VCF portion of the Trilogy 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 4.)

REDACTED FOR PUBLIC RELEASE

In the first OIG Sentinel report issued in March 2006, we 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.²⁷ In reviewing the management processes and controls the FBI had applied to the pre-acquisition phase of Sentinel, the OIG found that the FBI developed IT planning processes that, if implemented as designed, could help the FBI successfully complete Sentinel.

In particular, the OIG found that the FBI had 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 PMO dedicated to the Sentinel project.

However, at that time the OIG identified several concerns about the FBI's management of the Sentinel project, including: (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 track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's information technology investment management processes.

In December 2006, the OIG released the second in a series of audit reports that examined the FBI's development and implementation of the Sentinel project.²⁸ This report discussed: (1) the progress the FBI made in resolving the concerns identified in the first OIG report on the planning for Sentinel, and (2) whether the contract with Lockheed Martin and the FBI's ITIM processes and project management are likely to contribute to the successful implementation of Sentinel. The OIG found that the FBI resolved most of the concerns the OIG identified in its first Sentinel audit, although the audit reported that some aspects of those concerns as well as

²⁷ 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.

²⁸ Department of Justice, Office of the Inspector General. *Sentinel Audit II: Status of the Federal Bureau of Investigation's Case Management System*, Audit Report Number 07-03, December 2006.

REDACTED FOR PUBLIC RELEASE

some new concerns identified in the second audit merited continued monitoring. Specifically, the OIG found that the FBI had 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 an IV&V plan, (4) developing information sharing capabilities, and (5) hiring more PMO staff.

Among the areas that warranted continued monitoring by the FBI, the OIG, and other oversight entities were the: (1) funding of the Sentinel project and the effect on the FBI's operations or other projects if a reprogramming of funds was 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 May 2006, the GAO released a report critical of the FBI's controls over costs and assets of its Trilogy project.²⁹ 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 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 July 2007, the GAO issued a report on the extent to which the FBI had established best practices for acquiring Sentinel and estimating the project's schedule and costs.³⁰ The GAO concluded that, in general, the FBI had best practices in place for acquiring IT systems, including practices for evaluating offers and awarding contracts. In contrast, our audit examined the FBI's implementation of

²⁹ 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.

³⁰ U.S. Government Accountability Office, *Information Technology: FBI Following a Number of Key Acquisition Practices on New Case Management System but Improvements Still Needed*, July 2007.

REDACTED FOR PUBLIC RELEASE

its policies and procedures for managing the development of Sentinel, including several related to the best practices reviewed by the GAO. Because our audit focused on how these policies and procedures were actually implemented, our findings differ from the GAO's because we found areas of inadequate implementation.

FINDINGS AND RECOMMENDATIONS

Finding 1: Phase 1 Schedule, Cost, and Performance

Phase 1 of Sentinel, deployed on June 19, 2007, delivered two key components of the FBI's new information and investigative case management system: a web-based portal to ACS data and workboxes to aid in case management. However, Phase 1 took about 2 months longer than scheduled, cost slightly more than the FBI expected, and delivered less than originally planned. Our audit found four main causes for the delay, including: (1) unrealistic schedule expectations by the FBI, (2) Lockheed Martin's delays in staffing, (3) challenges Lockheed Martin encountered in integrating COTS software programs to work together as a system, and (4) FBI problems in assessing the project's progress against the approved schedule.

With regard to deliverables, Phase 1 did not deliver all the commonly understood foundational components of a service-oriented architecture (a concept that we found to be ill-defined), but did deliver the enterprise service bus component that was appropriate for the first phase of the project.³¹ Phase I did not cleanse the data in the electronic case file module of ACS as originally proposed because the FBI said it would be more efficient to do so in Phase 2 of the Sentinel project. Also, the web-based portal developed in Phase 1 did not include the full range of functionality originally anticipated.

Further, as a result of a series of contract modifications, the cost of Phase 1 exceeded the amount originally budgeted for Lockheed Martin although the overall contract value of \$305 million did not change. Lockheed Martin's costs exceeded the revised contract amount of \$59.7 million by approximately \$4.4 million. However, Lockheed Martin and the FBI agreed that Lockheed Martin would only be paid the amount of the revised budget, a figure that

³¹ An enterprise service bus is software "middleware" that connects software components and allows the components to communicate with each other.

REDACTED FOR PUBLIC RELEASE

included using the \$2 million budgeted for award fees.³² Other factors such as the transfer of requirements to later phases of the project, not tying all deliverables to the requirements, and transferring costs from Lockheed Martin's budget to the PMO's budget suggest that the cost of Sentinel ultimately may be higher than originally anticipated.

Schedule Delay

The FBI and Lockheed Martin established April 19, 2007, as the completion date for Phase 1 during the Initial Baseline Review (IBR) in May 2006.³³ During the IBR, held about 2 months after the contract award, the FBI and Lockheed Martin agreed to a schedule for Phase 1, including all the program-level reviews and life cycle management reviews.

By September 2006, the time the Critical Design Review was originally scheduled to be performed, Lockheed Martin's performance deviated from the schedule to such a degree that the FBI directed Lockheed Martin to postpone the Critical Design Review until October 2006. Specifically, several principal design documents prepared by Lockheed Martin were returned by the PMO without comment because the documents were insufficient.

Despite concerns about the completeness of these key design documents, the FBI allowed Phase 1 to pass the Final Design Review in October 2006. At that time, PMO officials told Lockheed Martin that its schedule for the remaining work was not feasible and directed Lockheed Martin to replan the schedule for the remainder of Phase 1. Lockheed Martin reconsidered the schedule for the remaining work, including the approach to the remaining tasks, the linkage between the remaining tasks, and whether additional resources could shorten the length of time needed to complete the remaining tasks. Lockheed Martin then provided a revised schedule to the FBI. The FBI approved the revised Lockheed Martin schedule, and that schedule remained in effect until March 2007 when the FBI and Lockheed Martin jointly decided that Lockheed Martin would not be able to resolve all of the

³² Lockheed Martin did not receive the award fee. Instead, the FBI allowed it to transfer the \$2 million budgeted for the award fee to the cost portion of the budget.

³³ See Appendix 3 for an explanation of the management reviews of the project discussed throughout this report.

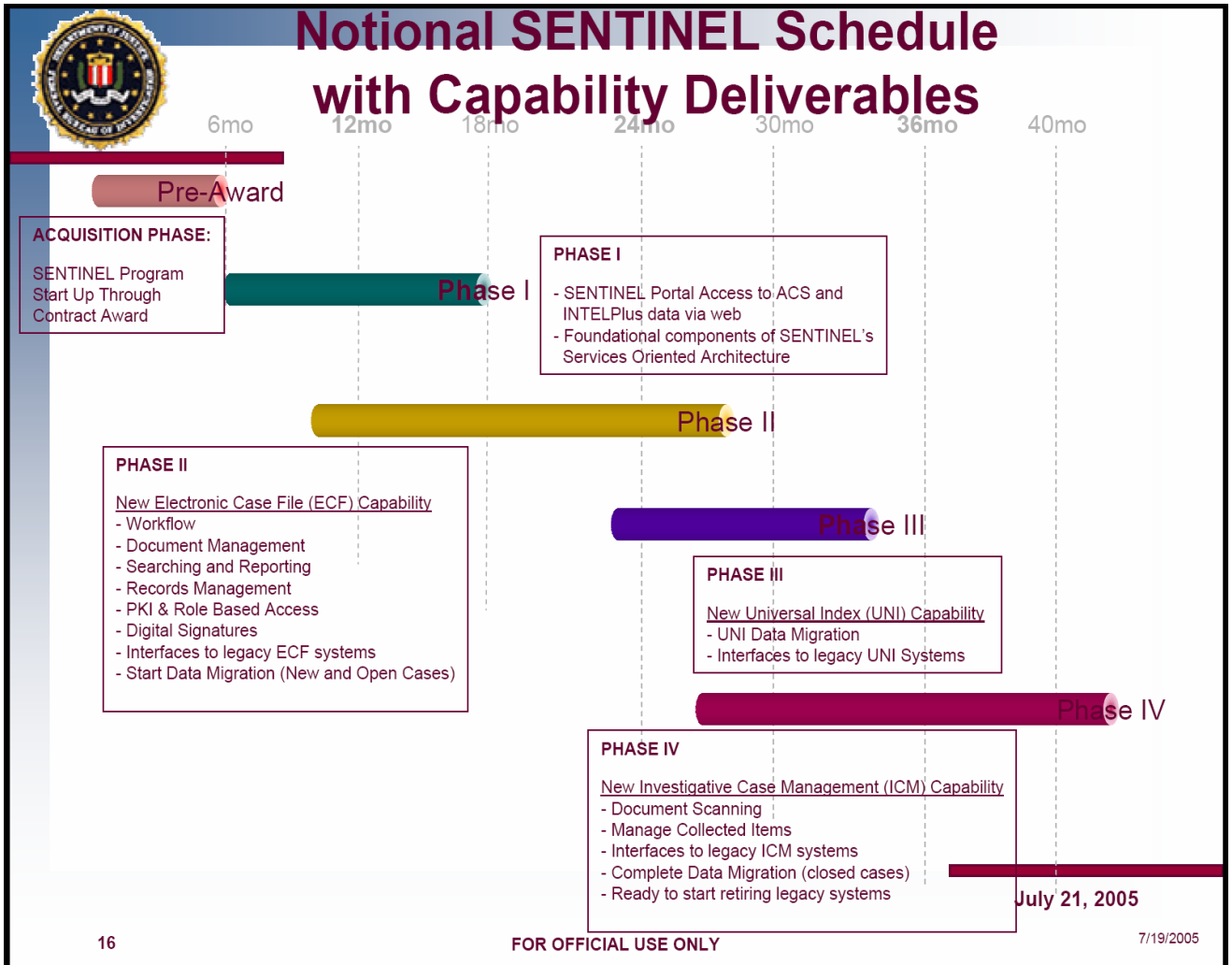
deficiencies identified during testing in time to meet the Delivery Acceptance Review scheduled for April 19, 2007. A discussion on the reasons for the delays follows.

Causes for Delay

Our audit found the following four primary causes for the delay in the delivery of Phase 1: (1) an unrealistic schedule, (2) delays by Lockheed Martin in fully staffing the project with appropriately experienced personnel, (3) challenges in integrating the various COTS software components to work as a system, and (4) a progress reporting schedule that did not allow the FBI to assess the schedule impact of changes proposed by Lockheed during the course of Phase 1.

Unrealistic Schedule

Prior to formally soliciting proposals for Sentinel, the FBI created a notional schedule that broke the project into four phases, identified deliverables for each phase, and provided an estimated timeline for each phase. Various documents outline the FBI's concept for Sentinel's development schedule, including the following timeline.



Source: The FBI

While the Sentinel Acquisition Plan clearly stated that potential vendors were free to submit proposals with a different number of phases or suggest changes to the deliverables identified in each phase, vendors' proposals had to meet the FBI's overall deadline of completion by December 2009. PMO personnel said that Lockheed Martin's proposal closely aligned with the FBI's notional schedule in an effort to win the FBI's business. The PMO personnel also stated that Lockheed Martin's proposal was completed before it familiarized itself with ACS and that instead of basing the Phase 1 schedule on the FBI's notional concept of the project, Lockheed Martin should have based the schedule on its own estimates of the time required to achieve the tasks contained in Phase 1.

In addition to broad outlines of the project's overall schedule, the FBI also dictated certain project milestones. For example,

REDACTED FOR PUBLIC RELEASE

Sentinel's Statement of Work specified the timing of the Contract Implementation Review, the Requirements Clarification Review, and the IBR. All three of these reviews, described in Appendix 3, were to occur within 60 days of the March 16, 2006, contract award date for Sentinel. Meeting the schedule specified in the Statement of Work would have required that Lockheed Martin staff the Sentinel project shortly after receiving the contract. The Sentinel Program Manager told us that, in retrospect, the timeframes in the Statement of Work were overly aggressive because they did not allow Lockheed Martin enough time to staff the project.

Delays in Staffing

In addition to the aggressive schedule, which gave Lockheed Martin little time to properly staff the Sentinel project, other factors further delayed Lockheed Martin from properly staffing the project. A high demand for personnel with current top secret clearances in the Washington, D.C., area also affected the staffing of the project, as did Lockheed Martin's underestimation of the level of experience with COTS integration that its personnel needed to have. These issues contributed to both delays in staffing and also higher-than-expected personnel costs.

Almost immediately following the contract award, Lockheed Martin fell behind in its projected staffing levels. For example, by May 2006, less than 2 months into the contract, Lockheed Martin's spending on personnel according to EVM data was \$476,000 less than expected primarily because the project had yet to be fully staffed. According to the FBI, the costs for qualified personnel with top secret clearances were 25 to 40 percent higher than the cost Lockheed Martin projected due to a limited supply of qualified personnel with top secret clearances. The FBI said that shortly after the Sentinel contract was awarded, the Defense Security Service, the organization responsible for performing background investigations and granting clearances, suspended its processing of clearances for all government contractors for 6 months in an effort to clear its backlog of requests for such clearances. As a result of the suspension, the supply of cleared contractor personnel, which was already insufficient to meet demand, dwindled even more. While Lockheed Martin had fewer staff than planned, it had to pay each individual more than expected.

In addition, Lockheed Martin and the FBI also underestimated the level of COTS integration experience that personnel would need for the Sentinel project. In a January 2007 briefing to the FBI's Associate

REDACTED FOR PUBLIC RELEASE

Deputy Director, the Sentinel Program Manager said that both the FBI and Lockheed Martin based their original personnel cost estimates on the assumption that most of the development work could be completed by recent college graduates, an approach Lockheed Martin had successfully used on a large scale information technology project at the Social Security Administration. Several PMO and FBI Chief Information Office personnel said that throughout Phase 1 of Sentinel, the level of expertise required of the Lockheed Martin staff to deal with Sentinel's COTS software was not sufficient for the project, although they said that Lockheed Martin eventually added the required expertise. FBI officials said the quality of the Lockheed Martin staff had improved during the first phase, but that additional improvements need to be made if the subsequent phases of the project are going to be successful. Others said that Lockheed Martin should have considered contracting with the software manufacturers who developed the most challenging pieces of software to help with implementation.

According to FBI officials, both the FBI and Lockheed Martin recognize that they underestimated the level of expertise necessary to work on the interface with ACS and integrate the COTS software products which make up Sentinel and a service-oriented architecture (explained in more detail later in this report). According to the FBI, at the time of contract award the division of Lockheed Martin awarded the Sentinel contract had a limited personnel pool from which to draw, and it was not successful in hiring the additional personnel needed in a timely manner. As a result, Lockheed Martin relied more heavily on subcontractors than anticipated and transferred personnel from within other parts of the company.

COTS Integration

Several PMO officials, including the Sentinel Program Manager and Lockheed Martin's Deputy Program Manager, stated that integrating the various software modules that comprise Phase 1 into a unified system was a major challenge in Phase 1. Several variables affect how a given piece of software will perform, including: the hardware that the software is running on, the settings for that hardware, the settings for the software itself, and the addition of other software on the system and the settings of that software. According to PMO personnel, many of the individual software products can be configured in hundreds of different ways. As a result, there are hundreds of potential issues that can occur when integrating different pieces of software into a system. Consequently, identifying why a

REDACTED FOR PUBLIC RELEASE

particular problem occurred within an integrated system is difficult due to the number of variables impacting the system.

The Lockheed Martin Deputy Program Manager said that while software and hardware manufacturers' literature, demonstrations, and trade studies provide information about the functionality of their products, hands-on experience is necessary to determine if the general capabilities of a particular COTS product can be configured to implement the specific functions required by a particular customer. According to the Deputy Program Manager, it is virtually impossible to complete a design involving COTS products without hands-on experience with the product and its interfaces. Risk factors for COTS integration include the number of COTS components, the number of interfaces, the complexity of the interfaces, and the amount of knowledge and experience the integrator has with the product. Because Sentinel is using multiple software programs, and more than one software product may be capable of performing a particular function, Lockheed Martin had to decide which product to use based on the advantages and disadvantages of each choice. Most COTS products are complex enough that some amount of manufacturer support is required to use the product efficiently.

Several of these factors appear to have had an impact on Sentinel development during Phase 1 of the project. As discussed previously, Lockheed Martin did not have staff assigned to the project with significant expertise in the software components being used to build Sentinel. Also, the major COTS software manufacturers were not official Lockheed Martin subcontractors, so their input was not sought in the design phase of the project. Once Sentinel encountered problems, obtaining support from the software manufacturers was time-consuming.

Two other factors compounded the general challenge of COTS integration. First, according to the FBI CIO the FBI is using the latest software and technologies in developing Sentinel, and therefore some of the software has bugs that had not previously been identified by the manufacturer. In at least one case, the developer of the software was not aware of the bug until being notified by the FBI and Lockheed Martin. Because this was a new bug, the manufacturer had to research the cause and develop a solution before Lockheed could implement the patch to the software. Second, Lockheed Martin did not develop a COTS integration strategy to describe what approach it would take to overcome the compatibility issues of Sentinel's various

components.³⁴ The Sentinel architect and the independent verification and validation (IV&V) team both cited the lack of an integration strategy as a primary reason for the integration problems Lockheed Martin faced during Phase 1.³⁵

Assessing Progress

Sentinel PMO personnel said that the methodology used by Lockheed Martin to construct the Sentinel project's schedule made it difficult to assess the progress of the project. Specifically, they said the schedule: (1) overused "hard constraints", (2) contained logic problems, (3) was not updated accurately, and (4) contained a high percentage of "level-of-effort" tasks.

Hard Constraints

Lockheed Martin utilized project management software that included a program to establish the project's schedule. Within the schedule, timeframes were set for the completion of specific tasks, and these tasks were entered into the schedule as "hard constraints." Hard constraints are dates entered into a schedule that require a task to begin or end on a specific date, regardless of any other activity with the schedule. Additionally, if a hard constraint is entered into the schedule for a task, the schedule's software will assume that the task met the constraint, regardless of whether or not it did. For example, if a task had a hard constraint to be completed by December 1, 2006, unless the date was updated the project software would assume that the task was completed by that date, regardless of the actual progress on the task. Also, if a task has a fixed end date entered into the scheduling software and the task is not actually completed by that date, all of the subsequent phases will not be delayed within the schedule and the completion date for the whole project will not be moved back. Because of this, hard constraints cloud an assessment of the impact of schedule slippages on the project end date.

³⁴ In general, the strategies for integrating COTS components include adjusting the standard configuration settings of the system's components, modifying the system's components, replacing problematic components, and adding additional components.

³⁵ In September 2006, the FBI obtained the services of Booz Allen Hamilton to perform the IV&V function for the Sentinel project. See Finding 2 for a more detailed discussion of IV&V.

REDACTED FOR PUBLIC RELEASE

While the Sentinel Deputy Program Manager stated that hard constraints are helpful in creating a sense of urgency about completing a task, we found that using a large number of hard constraints limited the FBI's ability to assess the progress being made on the Sentinel project. Several PMO personnel attributed the overuse of hard constraints to Lockheed Martin's problems hiring and retaining an experienced scheduler, an issue they now believe Lockheed Martin has resolved. At the PMO's request, Lockheed Martin has removed many of the hard constraints from the Sentinel development schedule.

Logic Problems

PMO officials also cited problems with some of the logic of Lockheed Martin's schedule. Specifically, they said Lockheed Martin's schedule did not always accurately reflect the interdependence between tasks and linked some tasks that were not interdependent while failing to link others that were.

Schedule Updates

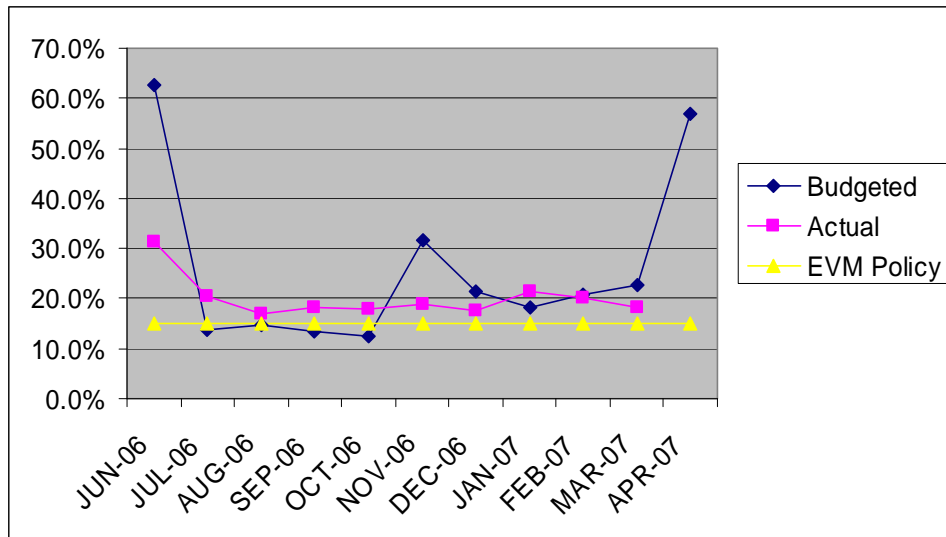
Assessing the project's progress was also difficult because Lockheed Martin did not accurately update the schedule as required. Sentinel PMO personnel said a task's reported rate of completion appeared to be based on Lockheed Martin management's assessment of what it thought the FBI wanted to hear, rather than an actual assessment of the percentage of the task completed. Two IV&V reports confirmed problems with Lockheed Martin's maintenance of the schedule, including that the schedule was not updated to reflect activities that occurred in the most recent reporting period and inaccurate reporting on the percentage of completion of tasks. Specifically, the IV&V team found that various tasks would be 99 percent complete for more than one reporting period, allowing Lockheed Martin to claim all but 1 percent of the cost of a task but not claim that the task was completed.

Level-of-Effort Tasks

An FBI policy on EVM issued by the FBI CIO in March 2006 recognizes that some portion of the development of IT systems will be characterized as level-of-effort, meaning that progress toward the completion of a task is measured by time spent on the task rather than progress toward completing the task. Tasks that do not have a defined deliverable, such as project management, are often measured using level of effort. However, because level-of-effort tasks are not

tied to a deliverable, it is difficult to determine how much their completion contributes to the overall progress of a project. Therefore, in IT development projects like Sentinel it is prudent to have a schedule with as few level-of-effort tasks as possible. Recognizing this, the FBI's EVM policy requires a project to receive approval from the Chief of the Project Assurance Unit when planned level-of-effort tasks exceed 15 percent of the total work hours for a project. The FBI's Project Assurance Unit denied the PMO's request to exceed the 15 percent threshold for Sentinel. However, the PMO appealed the denial to the FBI's CIO and received his approval for the planned level-of-effort hours. As shown in the graph below, for every month since the IBR the actual percentage of level-of-effort tasks exceeded the 15 percent threshold established by the FBI. With the exception of July 2006 through October 2006, the budgeted amount of level-of-effort tasks also exceeded 15 percent of the budgeted hours. A high level of both budgeted and actual level-of-effort tasks makes it difficult to accurately assess the progress of a project toward meeting its goals.

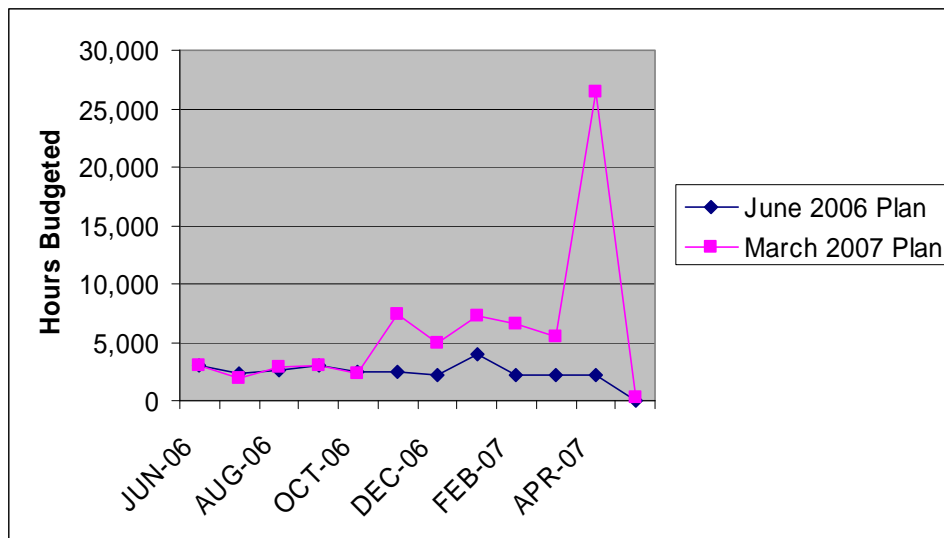
**Level-of-Effort Tasks as a Percentage of Total Work Hours
June 2006 through April 2007**



Source: FBI data

As Phase 1 progressed, the percentage of hours budgeted for level-of-effort tasks increased. The following graph shows the increase in level-of-effort hours budgeted for June 2006 through April 2007 at the IBR to the hours budgeted in the Phase 1 budget as of March 2007.

Hours Budgeted for Level-of-Effort Tasks June 2006 Plan vs. March 2007 Plan



Source: FBI data

As of April 2007, spending on level-of-effort tasks accounted for 27 percent of the total Phase 1 budget. An FBI analysis of the increase in spending on level-of-effort tasks concluded that most of the increase resulted from higher than expected spending on program management costs. This, in turn, resulted from higher than expected staffing and labor costs.

Tight Schedule Affected Implementation of LCMD Processes

In attempting to meet the Phase 1 schedule, the FBI took risks that affected the quality of some of the Phase 1 deliverables and may have contributed to the schedule delays. Specifically, the FBI allowed Lockheed Martin to begin building Phase 1 before the design documentation was complete, contributing to some of the problems encountered in the testing of Phase 1. The FBI also allowed Phase 1 to progress to the next stage of testing before correcting all critical deficiencies identified in previous stages of testing.

Incomplete Design

In October 2006, the Sentinel PMO allowed Phase 1 to pass through the Critical Design Review despite hundreds of unaddressed FBI comments on the System Design Document and the Interface Design Document, key design documents that provide programmers with the specifics required to build a system to a customer's

REDACTED FOR PUBLIC RELEASE

specifications. Both the System Design Document and the Interface Design Document are supposed to be finalized and approved during the Critical Design Review.

The PMO knew of these documents' shortcomings at the time of the Critical Design Review. Lockheed Martin had submitted both documents to the PMO 3 weeks before the Critical Design Review to allow the FBI time to review and comment on the documents. The FBI's review concluded that the documents did not meet standards for content, completeness, consistency, and quality, and returned the documents to Lockheed Martin for additional work. The FBI directed Lockheed Martin to resubmit the documents and advised Lockheed Martin that it would require 2 weeks to provide formal written comments on the revised plans. Lockheed Martin resubmitted the documents on October 4, 2006, 1 day before the Critical Design Review. As agreed, the FBI did not complete its formal review of the documents until October 18, 2006, 2 weeks after they had been resubmitted. However, the FBI and Lockheed Martin still held the Critical Design Review on October 5-6, 2006, during which time the PMO concluded that Lockheed Martin's design documentation was sufficient to ensure that the design presented could be produced and when built would meet the design specification.

Similarly, the Technical Review Board – part of the FBI's Life Cycle Management process described in Appendix 3 – concluded that the system design was not complete or well documented. However, at Sentinel's Final Design Review in October 2006, the Board granted the PMO conditional approval to proceed with the project but required that six technical issues be addressed, such as the need to provide details on the number of modules and design details. The Board's approval authorized the development of Phase 1 of the project, while also requiring that the deficiencies found in the design documents be addressed. Of the six conditions the Board cited, four had not been resolved as of April 2007, including three that concerned design documents.

While a temporary delay would have occurred if the FBI required Sentinel's design to be completed before development began, the time invested during the delay may have shortened the actual time spent on Phase 1. An April 2007 IV&V report stated that "Historically, most deficiencies occurred around the display of information to the Personal and Squad Workbox; prototyping and a complete System Design Document and Interface Design Document would have avoided many of these deficiencies."

Testing

In an apparent effort to keep Sentinel on schedule, the PMO deviated from sound project management and Sentinel's Test Evaluation Master Plan. The PMO allowed Phase 1 to pass through two program level reviews – the Product Test Readiness Review and the Site Test Readiness Review – without resolving all high priority deficiency reports as required by the Test and Evaluation Master Plan.³⁶ The IV&V contractor was repeatedly critical of Sentinel's testing and expressed concern about the impact the testing modifications would have on the stability of the system as it moved forward.

While we believe that adherence to schedule goals is desirable, the risk of project failure appreciably rises if corners are cut and there is not adequate quantitative data to assess the risks to the project of not implementing disciplined processes in critical areas. Ineffective implementation of these processes exposes a project to the unnecessary risk that costly reworks could be required, which in turn would adversely affect the project's cost and schedule and can adversely affect the ultimate performance of the system. Effective project management requires quantitative data or metrics to assess whether a project plan needs to be adjusted and to determine what oversight actions may be needed to ensure that the project meets its stated goals and complies with agency guidance.

Lockheed Martin's Cost Performance

The cost of the contract awarded to Lockheed Martin to develop Sentinel is about 72 percent of the total Sentinel budget.³⁷ Therefore, Lockheed Martin's ability to deliver its portion of Sentinel within budget is critical to the cost performance of the overall project. As the result of a series of contract modifications, the value of Lockheed Martin's task order for Phase 1 increased from \$57.2 million at the time of the integrated baseline review (IBR) to \$59.7 million in March 2007. However, in June 2007 Lockheed Martin advised the FBI that it had incurred costs totaling \$64.1 million in the performance of Phase 1. Lockheed Martin attributed the cost overruns to unanticipated work in

³⁶ A deficiency report documents a problem identified in testing and the resolution of the problem.

³⁷ The remaining 28 percent of Sentinel's budget funds the PMO.

REDACTED FOR PUBLIC RELEASE

interfacing with existing FBI computer systems and modifications to the FBI's testing approach.

Specifically, Lockheed Martin said the documentation and functionality of the FBI's Web-enabled Automated Case Support (WACS), Phoenix, and ACS systems differed from the descriptions provided in the FBI's Request for Proposals.³⁸ As a result, Lockheed Martin was not able to reuse portions of the WACS, Phoenix, or ACS portal interfaces, as it previously assumed it could. Consequently, Lockheed Martin had to develop extensive amounts of new code to provide the functionality it believed it was going to be able to reuse from these existing systems. In addition, Lockheed Martin said it had to develop an interface control document for ACS. Lockheed Martin estimates that these two issues required 7 weeks of additional effort and cost approximately \$3.4 million. The Sentinel Program Manager agreed that the ACS interface control document was not sufficient for Lockheed Martin to do its work, and that the development of a satisfactory interface control document added several weeks to the schedule.

Lockheed Martin said that changes to the FBI's testing approach during Site Acceptance Testing and User Acceptance Testing also resulted in schedule delays and increased costs.³⁹ Specifically, the FBI's decisions requiring the closure of all high-priority defects prior to the start of Site Acceptance Testing, increasing the scope of Site Acceptance Testing, adding unofficial User Acceptance Testing, and piloting the system before full deployment cost an additional 3 weeks and \$1 million for Phase 1. FBI officials told us there was no change in the testing requirements, but to ensure that the system met the FBI's specifications, supplementary testing was added after the system failed initial tests.

³⁸ Web-Enabled Automated Case Support (WACS) is ACS updated with access through a web portal. Phoenix is the second generation of WACS intended to access ACS through mini-programs specifically written to run within Web browsers.

³⁹ In general, testing ensures the system satisfies FBI requirements for utility and performance. Site Acceptance Testing executes a complete set of test procedures on the software that has actually been delivered from the contractor to the FBI and installed in order to insure consistency and functionality in the operation of the software. The purpose of User Acceptance Testing is to gain end users' acceptance of Sentinel.

REDACTED FOR PUBLIC RELEASE

In June 2007, the FBI and Lockheed Martin agreed that Lockheed Martin would absorb approximately \$4.4 million in costs it incurred in excess of the agreed-upon contract amount and that \$2 million budgeted for award fees would be used to reimburse Lockheed Martin for costs incurred during the development of Phase 1.

We found that three factors obscured a precise accounting of Lockheed Martin's cost performance, which we describe below. First, even though the FBI transferred some Phase 1 requirements to later phases of the project, it received cost reductions on Phase 1 from Lockheed Martin for deferring completion of these requirements. Second, the FBI did not adequately define all of the Phase 1 deliverables and did not tie all of the deliverables to the requirements agreed upon for Phase 1. Third, the FBI transferred \$2.5 million in materials and services from Lockheed Martin's budget to the PMO's budget.

Deferred Requirements

Over the course of Phase 1, the FBI deferred a total of 57 high- and low-level requirements from Phase 1 to later phases. As a result of these deferrals, Lockheed Martin was required to deliver less functionality in Phase 1 than agreed upon at the time the project budget was established. However, the FBI did not require Lockheed Martin to determine the decrease in the amount of time and materials required for Phase 1 resulting from these deferrals, and none of these deferrals resulted in a decrease in the cost of Phase 1.

The majority of these requirements addressed user interface or security capabilities. For example, the capability to display a list of leads that a squad had completed in accordance with current ACS screens was deferred to Phase 2.⁴⁰ Other areas addressed by the deferred requirements include the system's ability to format, sort, and search data.

⁴⁰ FBI field offices are divided into squads that have specific subject matter responsibilities such as drug trafficking or counterterrorism. A Supervisory Special Agent manages each squad and supervises the personnel assigned to the squad.

Phase 1 Requirements Deferred to Later Phases

Requirement Area	Number of Requirements Deferred	Example of Deferred Requirement
Reports	3	Display the number of copies, printer, case identification, document types, activity dates, user name and identification, and sort option when printing Case Document Inventory Reports.
Search	2	Perform unstructured searches against items collected during investigations.
Security	22	Display restricted items with identification information (e.g., serial, case identification, case owner) in search results or reports for users who do not have permission to view the item. All other record information shall be displayed as "Xs".
User Interface	30	Display a list of covered leads for a squad.

Source: OIG analysis of FBI data

According to the FBI, it deferred most of the 57 requirements because it decided the requirement was outside of the scope of Phase 1, did not add value to Phase 1, would require the modification of ACS, or would duplicate a capability included in a future phase of Sentinel. FBI officials said they did not believe it was prudent to invest in upgrading ACS because Sentinel is intended to replace it. We recognize that phased projects using COTS components often transfer requirements from one phase to another and, in general, we do not disagree with the FBI's transfer of the requirements to later phases. However, we are concerned that the FBI did not require Lockheed Martin to determine the financial impact of deferring this work in Phase 1 and adjust the cost of Phase 1 accordingly.

Phase 1 Deliverables

Throughout the Sentinel project, FBI documents, including slides from weekly briefings to the FBI Director, have shown four major anticipated deliverables for Phase 1: (1) a web-based portal to ACS, (2) a case workbook, (3) the foundational components of a service-orientated architecture, and (4) data cleansing of the electronic case file (ECF) portion of ACS. As implemented, Phase 1 delivered the key ACS portal and case workbook. Phase 1 also delivered the one component of the ill-defined foundational components of a service-

REDACTED FOR PUBLIC RELEASE

oriented architecture that was appropriate for that phase, but did not provide the data cleansing of the ECF portion of ACS.⁴¹ As Sentinel progressed through the life cycle management process, the FBI's internal technical reports noted this divergence from the original set of deliverables. For example, a technical report issued as part of the design review process noted that "The analysis is based on the ability of the project to meet the SENTINEL Phase 1 goals. Initially, Phase 1 was to include foundational components of a service-oriented architecture and ECF Data Cleansing. These two initiatives were pushed beyond Phase 1 and are not germane to this analysis." Neither the foundational components of a service-oriented architecture nor the data cleansing of ECF data were specified in the requirements for Phase 1, so the deferral of these goals did not require the deferral of requirements. However, achieving both of these goals may potentially require significant financial and personnel resources. And as mentioned previously, deferral of these goals did not result in a corresponding decrease in the Phase 1 contract amount.

In June 2006, the FBI and Lockheed Martin held an IBR for Phase 1 of Sentinel. One of the goals of an IBR is to agree on the scope of work.⁴² At the IBR, Lockheed Martin identified the following three major goals for Phase 1.

- Portal – a single web-based user interface to the system providing access to ACS functionality, a case "workbox" that summarizes a user's workload, enhanced search capabilities including saved queries, and a single sign-on within Sentinel.
- ACS ECF Data Cleansing – prepare the ECF portion of ACS data to be transferred to Sentinel in Phase 2.
- Service-oriented Architecture/Enterprise Service Bus – provide the governance of the service-oriented architecture and web services, and preliminary public key infrastructure (PKI) services for Sentinel system administrator login.⁴³

⁴¹ See page 34 for a discussion of the common components of a service-oriented architecture.

⁴² See the Introduction to this report for a more detailed discussion of the goals of an IBR.

⁴³ Service-oriented architecture governance is the policies and controls used to manage any changes to a service-oriented architecture. PKI is a system of

Sentinel Portal

Phase 1 of Sentinel delivered a web-based user interface to ACS data, giving a much more modern look and feel to ACS data and allowing users to navigate through the system using a mouse. However, the portal will not allow users to perform all of the functions in the three modules that make up ACS: ECF, Investigative Case Management (ICM), and Universal Index (UNI). Because many of the functions now performed by ACS will be performed by Sentinel starting in Phase 2, the web portal to ACS will be useful only until the completion of Phase 2. As a result, the FBI did not believe that duplicating all of ACS was cost effective and chose to include only the most frequently used functions in the Phase 1 portal. The table below summarizes the number of functions included in the Phase 1 portal and compares the ACS, the web-enabled ACS (WACS), and Phoenix.

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

Because some functionality can be found only in ACS, such as the uploading of documents, FBI personnel will have to continue to use ACS while Sentinel is being developed. Appendix 5 lists the functionality found in WACS, Phoenix, and Sentinel Phase 1. For those functions not available in any of these three systems, users will have to continue using ACS until the functions are available in a later phase of Sentinel. According to the Sentinel Program Manager, the FBI recognizes that some critical functions, such as uploading documents, are currently available only in ACS and those functions need to be integrated into Sentinel as soon as possible. As part of Phase 2, the FBI plans to enhance Phase 1 to allow users to upload documents.

computers, software, and data that relies on cryptography to provide some aspects of computer security.

Data Cleansing

Before Sentinel is completed, 23 million ACS records must be transferred from ACS to Sentinel. The IDP does not include any data cleansing or data migration capabilities for Phase 1. Rather, the IDP states "There are no specific requirements for migration of case data in Phase 1." However, Lockheed Martin's proposal included data cleansing of ECF data as part of Phase 1 in preparation for the data's transfer, or migration, to the Sentinel database in Phase 2. As a result, the FBI added this capability to its description of the Phase 1 capabilities.

Specifically, Lockheed Martin's proposal described the overall data migration effort as consisting of two basic steps: (1) data cleansing, and (2) data migration. The data cleansing approach described in Lockheed Martin's proposal yields an Error Assessment Report, which documents all of the data errors found in a system. These errors are then used to build data transformation rules, which improve the quality of legacy data before the data is migrated to the system being built. The FBI agreed to Lockheed Martin's data cleansing approach at the IBR, and the proposed scope of the data cleansing efforts were built into the integrated master schedule. However, further analysis and coordination with FBI headquarters divisions responsible for ACS and data security led to the conclusion that the full scope of Lockheed Martin's proposed data cleansing effort could not be implemented in Phase 1 and that the actual data cleansing would have to be deferred to a later phase.

FBI personnel told us that the FBI deferred data cleansing until Phase 2 because of technical concerns the FBI had with cleansing data in advance of migrating it. Specifically, the FBI was concerned that synchronizing the cleansed data with the actual ACS records at the time of migration would be difficult. Since the FBI would continue to add and modify data between the time of the data cleansing and the time the data would be migrated to Sentinel, the two sets of data would be different and resolving those differences presents significant challenges. FBI officials also had concerns about where, or within what system, to store the large volume of data in the interim between cleansing and migration.

The final Data Migration Plan described the Phase 1 data cleansing efforts as testing and prototyping only. The goals of the Phase 1 data cleansing efforts are described below.

REDACTED FOR PUBLIC RELEASE

- Complete installation, configuration, and testing of the Phase 1 data migration environment in the FBI's testing and quality assurance environments.
- Complete performance benchmarking of ACS data access using the FBI's testing and quality assurance environments.
- Complete testing, integration, and validation of COTS products using the FBI's testing and quality assurance environments.
- Complete testing, integration, and validation of the target word search filtering capabilities of two COTS products using the FBI's testing and quality assurance environments.
- Complete error assessment report generation testing using the FBI's testing and quality assurance environments.
- Initiate ECF data analysis and migration planning for Phase 2.
- Initiate installation, configuration, and testing of Phase 2 data migration environment in the FBI production environment.

The Data Migration Plan states that data quality assessment, data migration, and data cleansing of ACS ECF production data will not occur until Phase 2. However, the FBI did not conduct, or have Lockheed Martin conduct, a cost assessment of the reduction in scope of the Phase 1 data cleansing on Phase 1 or Phase 2. While the scope of the Phase 1 data cleansing activities decreased, there was no corresponding decrease in the cost of Phase 1. Similarly, while some data cleansing activities were deferred until Phase 2, there was not an increase in the cost of Phase 2. This change of scope occurred without a change to the Phase 1 requirements because the System Requirements Specifications does not contain any requirements that specifically address data cleansing or migration. Therefore, there were no requirements allocated to Phase 1 and no requirements deferred to Phase 2. According to the Sentinel statement of work, "The contractor shall perform all activities (extract, translate and error correction, load) necessary to migrate legacy data needed for the operation of capabilities delivered in each Phase." Because Lockheed Martin's proposal included ECF data cleansing in Phase 1, Lockheed Martin

effectively created a derived requirement, one that was deferred until Phase 2 without any cost implications.⁴⁴

FBI officials said that while Lockheed Martin had not done any actual data cleansing during Phase 1, it had made substantial progress on the data cleansing task, including configuring and testing the data cleansing software, setting up the data cleansing facility that will be used during Phase 2, and establishing data cleansing procedures to adjudicate the resolution of problem data.

Service-Oriented Architecture

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. Common components of a service-oriented architecture include a metadata repository, governance, a service registry, and an enterprise service bus, all of which are described below.

- Metadata repository – a database of data descriptions which is intended to provide consistent and reliable access to data.
- Governance – the mechanisms and policies to control what services are available via a service-oriented architecture and to whom they are available.
- Service Registry - the infrastructure for building, deploying, and discovering services on a service-oriented architecture.
- Enterprise Service Bus – software “middleware” that connects software components and allows the components to communicate with each other.

Of these four components, Phase 1 delivered an enterprise service bus. However, none of Sentinel’s requirements specifically address the service-oriented architecture, and therefore the FBI could not validate whether Lockheed Martin delivered the foundation of a service-oriented architecture, one of the stated goals for Phase 1. The FBI’s Incremental Development Plan (IDP), which was provided to all potential Sentinel bidders as a framework from which to describe the intent of the Sentinel program, states that Phase 1 “may include an

⁴⁴ A derived requirement is a requirement deduced or inferred from the requirements in the statement of work.

REDACTED FOR PUBLIC RELEASE

Enterprise Service Bus (ESB) and foundation services," but does not further describe what is meant by either "foundation services" or "foundational components." According to the FBI, the definition of "foundational components of a service-oriented architecture" was introduced during an internal review of the Sentinel design and was not specifically shared with Lockheed Martin as a goal, objective, or requirement of Phase 1. The FBI said that as a result, it had no expectation that Lockheed would specifically address the commonly recognized basic components of a service-oriented architecture in Phase 1. FBI officials said that Phase 1's enterprise service bus and web portal are both foundational components of a service-oriented architecture and that the enterprise service bus was the only one of the four common foundational components that was applicable to Phase 1.

At the IBR, according to Lockheed Martin the scope of work for Phase 1 included governance of Sentinel's service-oriented architecture, web services, and preliminary public key infrastructure (PKI) services for the Sentinel system administrator login.⁴⁵ The FBI and Lockheed Martin also agreed the scope of the Phase 1 service-oriented architecture would include the following: define and document the service-oriented architecture including the enterprise service bus, portal, access control framework with single sign on, ACS access, services management/governance, data protection/distribution/ recovery, and workboxes.

However, at the time of the Phase 1 Preliminary Design Review, the PMO told the FBI's Technical Review Board that the "core service-oriented architecture implementation design/components will be presented in Phase 2," and "[t]he enterprise service bus description, design, architecture will be introduced during Phase 2." In addition, the PMO said, "Please note that the bulk of service-oriented architecture information will come during Phases 2, 3 and 4." The technical report done for the combined Deployment Readiness Review and Site Testing Readiness Review states that a service-oriented architecture "could not be completed in Phase 1" and that it was deferred to a later phase.

⁴⁵ Service-oriented architecture governance is the policies and controls used to manage any changes to a service-oriented architecture. PKI is a system of computers, software, and data that relies on cryptography to provide some aspects of computer security.

REDACTED FOR PUBLIC RELEASE

The System Requirements Specifications do not delineate requirements for Sentinel's service-oriented architecture or the foundational components of a service-oriented architecture. Because the System Requirements Specifications are the source for requirements allocation by phase to supporting program documents, such as the Requirements Clarification Document (RCD), the RCD did not allocate any service-oriented architecture related requirements to Phase 1. Without any service-oriented architecture requirements, the FBI cannot test whether Phase 1 met the stated service-oriented architecture objectives.

Transferred Costs

Through a series of six contract modifications, the FBI increased the total contract value of Phase 1 by \$2.5 million, from \$57.2 million to \$59.7 million, but the overall contract value of \$305 million did not change. As expected in a project of Sentinel's size and complexity, some of the modifications increased the scope of Phase 1, while others decreased it. However, the decreases either transferred the cost for the tasks to the Sentinel PMO budget or to the amount budgeted for Lockheed Martin's award fee. For example, in March 2007 the FBI issued a modification which deleted tape silos (computer hardware that uses tapes to store large amounts of computer data) from the Phase 1 contract. Although the tape silos were still necessary for Phase 1, the FBI purchased silos with more storage capacity with funds from the PMO's budget and used the funds originally allocated to the tape silos to offset the cost of additions to the scope of Phase 1. The table below shows the deletions in scope to the Phase 1 task order.

REDACTED FOR PUBLIC RELEASE

Reductions in the Phase 1 Task Order

Item	Reason for Change	Amount
Waiver of award fee	Lockheed Martin volunteered to waive any award fee it might receive during the first evaluation period	(\$482,712)
Capability Maturity Model Integration (CMMI) Level 3 for the PMO ⁴⁶	The PMO believed its staff had the necessary expertise for the PMO to achieve CMMI level 3	(\$503,826)
Tape silos	higher-capacity silos purchased as part of FBI-wide procurement	(\$2,106,877)
Total Deletions		(\$3,093,415)

Source: FBI

The increases in scope to Phase 1 were for items that Lockheed Martin believed the government was obligated to provide, subsequent phases of Sentinel, the operations and maintenance of Phase 1, or requirements added by the FBI. The following table shows the additions in scope to the Phase 1 task order.

⁴⁶ Capability Maturity Model[®] Integration is a process improvement approach that provides the essential elements of effective processes. There are six capability levels, numbered 0 through 5. Each capability level corresponds to a goal and a set of practices.

REDACTED FOR PUBLIC RELEASE

Additions to the Phase 1 Task Order

Item	Reason for Change	Amount
[REDACTED] ⁴⁷	The software was not included in the baseline bill of materials and the FBI agreed it was necessary to complete Phase 1	\$610,451
Work-in-progress accounting for Phase 1	The FBI's Finance Division added the requirement	\$160,863
[REDACTED] Licenses and Maintenance	Phase 2 software purchased at a price advantageous to the FBI	\$2,443,644
Ramp up for Phase 1 operations and maintenance	Lockheed Martin needed time to hire and train the personnel to operate Phase 1	\$671,932
Early Execution of Planning for Phase 2	Allow Lockheed Martin additional time to plan for Phase 2	\$1,512,385
Non-Sentinel [REDACTED] Enterprise License and Maintenance ⁴⁸	Purchase enterprise license at reduced price due to Sentinel purchase of same software	\$643,064
Total Additions		\$6,042,339

Source: The FBI

⁴⁷ [REDACTED]

⁴⁸ While the FBI purchased the [REDACTED] enterprise license through the Sentinel contract, Sentinel funds were not used for the purchase.

Conclusion

Phase 1 delivered the two key components of Sentinel, the web-based portal and the workboxes. However, it did not include all the deliverables planned for Phase 1. While we cannot yet assess the full impact of deferring some of the original Phase 1 deliverables to subsequent project phases, we believe that deferring these deliverables may add cost and schedule pressures to subsequent phases of the project. In addition, we question why cost adjustments did not occur in Phase 1 due to reduced requirements.

The FBI's ITIM framework and the Sentinel PMO both establish processes that should enable the FBI to avoid the problems that occurred in the failed Trilogy project, but rigorous implementation of these processes is necessary for the FBI to reduce the risks it faces in implementing Sentinel. The schedule and cost issues the FBI encountered during Phase 1 demonstrate that inadequate implementation of any of the disciplined processes in systems development can reduce or overcome the positive benefits of other processes. For example, the FBI's decision to allow Lockheed Martin to begin building Phase 1 without completing the design documents likely had an impact on the time required for testing and the number of defects found during testing.

The FBI is currently reexamining whether the current development approach is best for the subsequent phases of Sentinel. Other approaches feature shorter phases and inherently lower the risk of spending substantial amounts of money on a deliverable that does not meet the customer's needs. However, shorter phases may increase the overall cost and schedule of Sentinel. In our judgment, while the FBI must continue to closely manage Sentinel's cost and schedule, the FBI's primary consideration in reevaluating Sentinel's development approach should be delivering a system that meets the needs of the FBI regardless of how many discrete project phases may be needed to accomplish that goal.

Recommendations

We recommend that the FBI:

1. Reconsider the four-phase approach to developing Sentinel to limit the scope of future phases to allow them to be completed in 9 months or less.
2. Negotiate decreases in the cost of future phases if requirements are deferred in that phase.

Finding 2: Phase 2 Planning and Management Issues

The FBI has implemented several management controls and processes that are designed to help it adequately manage the development of Sentinel and bring it to a successful conclusion. We reviewed four of these controls and processes in-depth: (1) EVM, (2) independent verification and validation (IV&V), (3) risk management, and (4) bill of materials. We found that the FBI has made significant progress in each of the four, but that additional progress needs to be made in the implementation of EVM, risk management, and the bill of materials.

In addition to these controls and processes, we found that the FBI has identified lessons learned during Phase 1 of the Sentinel project. We examined six key lessons that, if acted upon, will aid the FBI in planning Phase 2 of the Sentinel project and reduce risks. We also reviewed the status of the recommendations we made in our previous two reports on the Sentinel project and found that the FBI is taking action to resolve our concerns. We have closed 5 of the 12 prior recommendations and note that the FBI agreed with the remaining recommendations and was in the process of taking corrective action. These recommendations dealt generally with the FBI's need to complete the required planning and general management oversight policies and procedures for Sentinel in order to help ensure its success.

Management Controls and Processes

The FBI has established four important management controls and processes that, if implemented correctly and fully, will help the FBI better manage the Sentinel project. However, the FBI needs to improve its implementation of three of the controls and processes to ensure their effective use.

Earned Value Management

As we reported in December 2006, the FBI established an EVM system for Sentinel as required by OMB, and our current audit found that the FBI is continuing to implement it. EVM helps manage project risks by producing reliable cost estimates, evaluating progress, and allowing the analysis of project cost and schedule performance trends.

REDACTED FOR PUBLIC RELEASE

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 implemented and utilized, EVM allows project management to pinpoint potential problems and address them before they escalate.

According to the FBI's EVM plan, the Sentinel PMO will use the plan to measure both its and Lockheed Martin's earned value performance and report the results 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 Alliance (EIA) Standard 748-A.⁴⁹ 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.

Our review of EVM reporting from September 2006 to March 2007 showed that the FBI had continued to make efforts to implement EVM and use EVM data to help manage Phase 1 of Sentinel. Although the FBI's implementation of EVM was consistent with the Department's guidance, several issues decreased the effectiveness of EVM as a tool to manage the Sentinel development contract.

Reliability of EVM Data

The most significant issue was the reliability of the EVM data Lockheed Martin provided the FBI. In June 2007, the FBI rejected Lockheed Martin's April 2007 EVM data after Lockheed Martin notified the FBI that it estimated that it had incurred approximately \$64.1 million in costs during Phase 1 of Sentinel. Because the EVM baseline for Phase 1 was \$59.7 million, Lockheed Martin's estimate showed that its EVM system was not collecting accurate data on Sentinel costs as Lockheed Martin was accruing the costs – one of the primary purposes of an EVM system. While Phase 1 was behind schedule, the EVM data indicated that the cost would not exceed the baseline of \$59.7 million. In the last EVM report released before the end of Phase 1, the FBI

⁴⁹ 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.

REDACTED FOR PUBLIC RELEASE

estimated that on April 19, 2007, the original planned end date, there would be enough unallocated funds to pay for an additional 5 weeks of effort by Lockheed Martin. In addition, the EVM data used for the March 2007 EVM report indicated that the project was on budget for the amount of progress made.

Changes in Performance Measure Baseline

In addition, Lockheed Martin and the FBI agreed to several changes in the performance measurement baseline, including two significant reallocations (also called "replanning") of resources within the original baseline amount of \$57.2 million.⁵⁰ To remain compliant with the ANSI/EIA Standard 748-A and OMB direction, the FBI must control changes to the performance measurement baseline. To clarify what types of changes are appropriate and define the process for authorizing changes, the Department's Office of the CIO (OCIO) developed and distributed guidance on revisions to a project's performance measurement baseline. Once the baseline has been established, any changes to it must be managed through a documented change control process. If a change is authorized, it should be incorporated into both the project's budget and schedule in a timely manner. Any changes to the baseline must be recorded prior to the commencement of the new work in the baseline revision.

The Department's guidance describes four categories of baseline revisions: (1) internal replanning, (2) customer-directed change; (3) application of management reserve; and (4) reprogramming.

- Internal replanning involves adjustments to future work in the baseline as long as the adjustments do not affect the total scope of work, baselined cost, or scheduled completion of the project. Replanning, which requires the program manager's authorization, should not result in any changes to the total amount authorized or key schedule milestones. Replanning may include revisions such as:
 - adjusting future work between work packages within the cost and schedule constraints of a single control account;

⁵⁰ Replanning revises the time-phased budget for completing the work remaining in a project without any changes to the total scope of work, baselined cost, or scheduled completion of the project.

REDACTED FOR PUBLIC RELEASE

- adjusting future work between control accounts; and
- distributing undistributed budget to control accounts.
- Customer-directed changes include contract changes and modifications that typically add or remove scope to the original performance measurement baseline. Funds from contract changes and modifications should be distributed to control accounts as soon as possible. While the contracting officer authorizes the contract modification, the program manager authorizes the change to the performance measurement baseline. A customer-directed change may result in an increase to the performance measurement baseline and may require the adjustment of key milestones.
- The management reserve, a portion of a project's budget set aside to cover any unanticipated costs of a project's scope of work, is not part of the project management baseline and therefore its use requires a change to the baseline. The program manager can authorize the use of the management reserve, which may result in an increase to the performance measurement baseline. However, the Department CIO should authorize any changes to a project's key milestones.
- Reprogramming revises the project baselines. This typically takes place when project performance deviates significantly from the original plan – usually the cost and time necessary to complete the project's remaining work exceeds the budget and schedule. Reprogramming sets planned value and earned value equal to actual cost, thus eliminating any cost and schedule variances. However, reprogramming should always be accompanied by a thorough replanning of the remaining work and should never be implemented solely to eliminate current variances. Reprogramming is authorized by the Department CIO and usually results in changes to the performance measurement baseline and the adjustment of key milestones.

Customer-directed changes, applying the management reserve, and reprogramming usually change the amount of the project management baseline since these types of revisions adjust a project's scope, cost, or schedule. Customer-directed changes and application of the management reserve do not have any effect on the cost variances or schedule variances. Reprogramming sets planned value

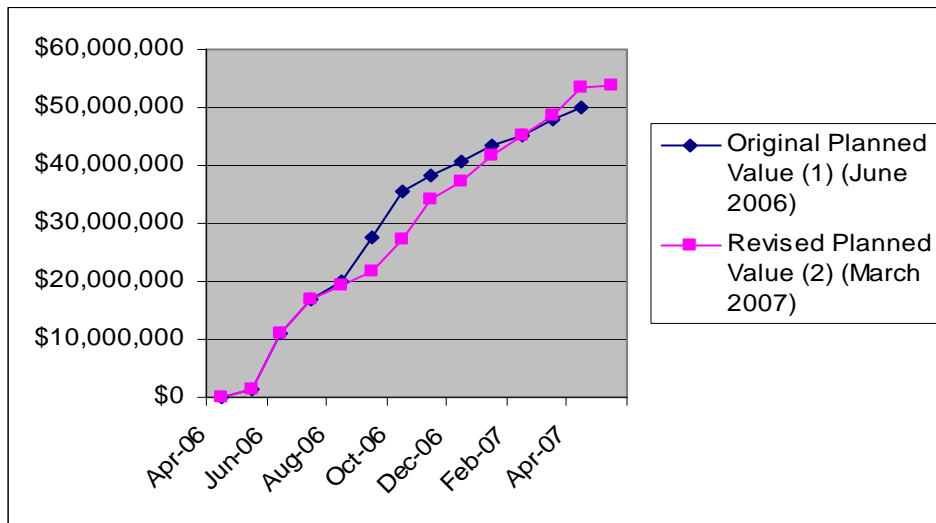
REDACTED FOR PUBLIC RELEASE

and earned value equal to actual cost, thus eliminating any cost and schedule variances. The Department's guidance refers to reprogramming as an extreme measure that should be applied when, due to performance issues, all key stakeholders agree that the original plan was either seriously flawed or is no longer practical. Any baseline revisions, regardless of the type, should be documented according to a change control process compliant with the ANSI/EIA-748A guidelines.

We reviewed the revisions to the Sentinel Phase 1 performance measurement baseline and found that the FBI and Lockheed Martin revised the project management baseline via internal replanning, customer directed change, and application of the management reserve. In addition, in a revision very similar to the application of management reserve, Lockheed Martin and the FBI agreed to transfer about \$483,000 in potential award fees to supplement the performance measurement baseline.

The most substantial of the revisions occurred in August 2006 when, as part of a replanning effort, the FBI transferred about \$15 million from the distributed budget to the undistributed budget and, through a transfer from the management reserve, increased the performance measurement baseline by \$1.6 million. Almost all of the transfer to the undistributed budget was the result of a decrease in the amount budgeted for equipment. FBI officials said changes in the planned equipment and uncertainty about other equipment necessitated the transfer. This replanning effort also delayed the timing of equipment purchases and moved the planned value associated with those purchases. As shown below, the revisions had a significant impact on the project's planned value, the basis for measuring a project's progress against its schedule.

**Original Planned Value vs. Revised Planned
April 2006 through May 2007**



Source: OIG analysis of FBI data

Compared to the original plan, these revisions reduced the amount the FBI planned to accomplish from August 2006 through February 2007. In July 2006, the EVM data showed Lockheed Martin's progress was about 10 percent behind schedule. By October 2006, 2 months after the replanning, the EVM data showed that Lockheed Martin was only 1 percent behind schedule. If the original plan had been in effect, Lockheed Martin would have been 24 percent behind schedule. However, neither the prior cost variance nor the prior schedule variance was set to zero as part of this replanning.

As previously discussed, the FBI issued a series of four contract modifications which increased or decreased the scope of work and the contract amount. These contract modifications also required revisions to the performance measurement baseline and the respective cost accounts. In addition, the modifications funded planning for Phase 2 and preparation for Phase 1 operations and maintenance, both of which are outside of the scope of the development of Phase 1. In our judgment, frequent and numerous changes to the scope of work make EVM data less reliable. The Department's CIO agreed and said that revisions to the performance management baseline are expected but frequent revisions make it difficult to determine what the EVM data is measuring against.

The FBI's implementation of EVM comports with the Department's guidance and aids the FBI in managing the project, but

REDACTED FOR PUBLIC RELEASE

it does not provide all the data the OMB believes necessary for oversight purposes. OMB officials said it would be helpful to them to be able to compare Sentinel's performance to the original baseline. As a result of OMB concerns that the FBI reprogrammed or rebaselined Phase 1 of Sentinel without the required OMB approval, we reviewed all changes to the time-phased budget used to measure Sentinel's progress. We concluded that the FBI had not rebaselined the project, but that its frequent replanning diminished the quality and usefulness of the EVM data for higher-level oversight.

Independent Verification and Validation

Inadequate implementation of any one of the disciplined processes in systems development can significantly reduce or overcome the positive benefits of others. When this happens, it is important to act promptly to address risks so as to minimize their impact. One way to monitor the processes used in systems development is to implement an IV&V process. In September 2006, the FBI hired Booz Allen Hamilton (Booz Allen) to perform the IV&V function for the Sentinel project. Since then, Booz Allen has participated in FBI-only project meetings and joint FBI-Lockheed Martin project reviews. In addition, Booz Allen has provided written comments and recommendations on many project documents, and produced 15 project status briefings and monthly reports. Booz Allen also produced monthly reports and biweekly briefings that were sent directly to the FBI's CIO.

These reports and briefings highlighted recent activities, upcoming events, and Booz Allen's view of the overall status of the project, including a discussion of risks that could affect the project's cost, schedule, or performance. The IV&V products also included recommendations and best practices. As of May 2007, Booz Allen had made over 70 recommendations based on risks and other areas it identified. Booz Allen also reported several project management and oversight weaknesses that increased the risks associated with Sentinel, including the following:

- *Design Incompleteness* - In December 2006, the IV&V team noted that the PMO staff made several hundred comments on

REDACTED FOR PUBLIC RELEASE

System Design Document and the Interface Design Document.⁵¹ Due to the level of effort and time required to address the comments in the documents, the PMO and Lockheed Martin decided not to address these comments in the final design documentation prior to development, but to address the comments in the Software Product Specification, which describes the specifications of a system as it was actually built. Booz Allen was concerned that the developers would create Sentinel without a complete understanding of the agreed-upon design. Booz Allen recommended that the FBI categorize and prioritize the comments, and then requested that Lockheed Martin incorporate the high-priority comments into revised documents.

- *Test Procedures* - In December 2006, Booz Allen reviewed the test procedures submitted by Lockheed Martin in preparation for the Product Test Readiness Review (PTRR), which assesses the readiness of a system for formal testing. (See Appendix 3 for a description of a PTRR.) Booz Allen found that 90 percent of procedures were unsatisfactory for performing dry-run or system-level tests for one or more of the following reasons: unclear test objectives, inadequate text description of the test, insufficient details on the test procedures, inadequate description of the results expected from the test, or unclear user roles. Booz Allen warned that inconsistent test procedures could result in inconclusive evidence that the system met requirements and that the project could be delayed since a verified set of test procedures would be completed before proceeding to formal testing. Booz Allen made a series of recommendations to improve the test procedures and recommended that the FBI and Lockheed Martin reexamine the testing schedule to determine whether the needed improvements to the test procedures would cause a delay in the start of formal testing.

In addition, as of May 2007 Booz Allen considered the following significant issues open and was tracking their resolution.

⁵¹ The System Design Document contains the design decisions made for the system as well as the system's architectural design and the services it will utilize. The Interface Design Document details the design of and responsibility for both internal data exchanges (within Sentinel) and external data exchanges (with systems outside of Sentinel).

REDACTED FOR PUBLIC RELEASE

- *Testing* - In April 2007, Booz Allen noted that the Sentinel system had been tested with a maximum of only 217 concurrent users, a load which Booz Allen viewed as unrealistic. Because the limited load was not representative of the user activity Sentinel would face once it was deployed, Booz Allen concluded that Sentinel was vulnerable to performance degradation – such as increased response times – during periods of high workload. Booz Allen recommended load testing with a number of users similar to the load that would be placed on Sentinel once it was deployed nationwide. Booz Allen believed this additional testing was necessary to identify and fix any performance related errors prior to the production release.
- *Physical Architecture* – In April 2007, Booz Allen identified the proposed hardware system as a potential vulnerability due to concerns about the system’s ability to be available to users whenever needed. Specifically, Booz Allen believed that the system did not have the redundant components needed to keep it up and running should a server fail. Booz Allen recommended enhancing the current hardware architecture to ensure higher availability, reliability, and performance of the Sentinel system.
- *Earned Value Management* – Lockheed Martin was not contractually required to generate variance analysis reporting at the control account level. As a result, Booz Allen reported that Lockheed Martin did not provide in-depth insight into the cost and schedule drivers for the discrete technical areas. While the PMO required Lockheed Martin to complete a “root cause” analysis when a substantial variance occurred for the program as a whole, it did not require one for variances in major control accounts. Booz Allen was concerned that a high-level analysis of the program’s variances from the plan would not allow the FBI to completely evaluate the technical risk posed by the variance or Lockheed Martin’s proposed strategy for eliminating the variance. In addition, Booz Allen had the following EVM concerns:
 - *Activities in the Integrated Master Schedule (IMS) without Work Breakdown Structure Alignment* – Booz Allen identified several activities in the IMS without

REDACTED FOR PUBLIC RELEASE

baseline dates and with no cross-reference to the work breakdown structure.⁵²

- *Inaccurate Statusing* (reporting of level of completion of an activity) – Booz Allen reported that the IMS showed that Lockheed Martin had claimed that some tasks were completed when they were not. For example, Lockheed Martin reported that it delivered the Security Vulnerability Risk Matrix on March 12, 2007, and recorded the task as 100 percent complete in the IMS. However, the matrix Lockheed Martin submitted was essentially a copy of the FBI template and contained no data. Booz Allen expressed concern that the ground rules for taking credit for meeting a task may only require deliverable submission and not address quality, acceptance by the FBI, and rework.
- *IMS Logic Conflicts* – These types of IMS constraints limit impact analysis. Activities with “hard constraints” are likely to adversely impact the critical path. Booz Allen noted that the IMS used “hard constraints” such as “Must Finish On.” The use of hard constraints created conflicts in the underlying logic of the schedule. For instance, the use of “Must Finish On” forced the scheduling software to record that a given activity finished on the “Must Finish On” date, regardless of whether that activity was finished early or had not yet been completed. Without an accurate record of when the task is completed, it is difficult to assess when tasks that depend on the completion of the first task can begin.

The IV&V process has resulted in numerous Booz Allen recommendations related to Sentinel Phase 1 development. We believe that Booz Allen has been able to identify areas of concern, explore them, develop recommendations and inform FBI decision

⁵² At a minimum, an integrated master schedule shows the expected start and stop dates for each event and accomplishment in a project’s integrated master plan. To aid in the day-to-day management of a program, each event or accomplishment may be broken down into multiple level hierarchy of tasks necessary to achieve the larger task. A work breakdown structure is a tool for defining the hierarchical breakdown of tasks and activities in an integrated master schedule.

makers in a timeframe that allows for meaningful changes to the project. See Appendix 6 for a list of Booz Allen's IV&V recommendations.

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 Program Manager and a Risk Review Board, which, according to the Risk Management Plan, is supposed to meet biweekly.⁵³ 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 Life Cycle Management Directive (LCMD).⁵⁴

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.

According to the Sentinel Risk Management Plan, risks are to be identified, managed, 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

⁵³ According to the Sentinel Risk Management Plan, the Sentinel Risk Review Board will include representatives from the following: program manager, systems engineer, program manager support personnel, systems engineer support personnel, program sponsor, users, the prime contractor, sub-contractors (as determined by the prime contractor), the Project Assurance Unit, and the Sentinel risk coordinator.

⁵⁴ 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).

REDACTED FOR PUBLIC RELEASE

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 turn into an issue or to reduce the severity of a risk's impact on Sentinel.

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.

As of April 2007, the FBI had identified and was managing 16 open risks to the Sentinel program, including the following top-ranked risks:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Risk Management Challenges

We view the FBI's ability to interface with other FBI IT systems from which it will extract data as a potentially significant challenge. The project manager said that during the planning stage of Sentinel, he was assured by the FBI that the documentation about ACS that Lockheed Martin needed in order to develop Sentinel existed. However, as discussed previously, Lockheed Martin had unanticipated problems with the ACS system documentation. In order for Sentinel to be able to extract information from ACS files, Lockheed Martin had to reverse engineer ACS to create satisfactory system documentation, which was then used to build the necessary interfaces between the two systems. According to the project manager, as part of the documentation re-creation Lockheed Martin had to develop new documentation for approximately 71 modules. The unexpected project took 4 weeks to design and an additional 4 weeks to develop. As a result, the Sentinel Program Manager has identified the potential lack of adequate documentation for other systems' interfaces and business processes as a risk to the remaining phases of Sentinel. This risk has the potential to impact both the budget and schedule of the Sentinel project.

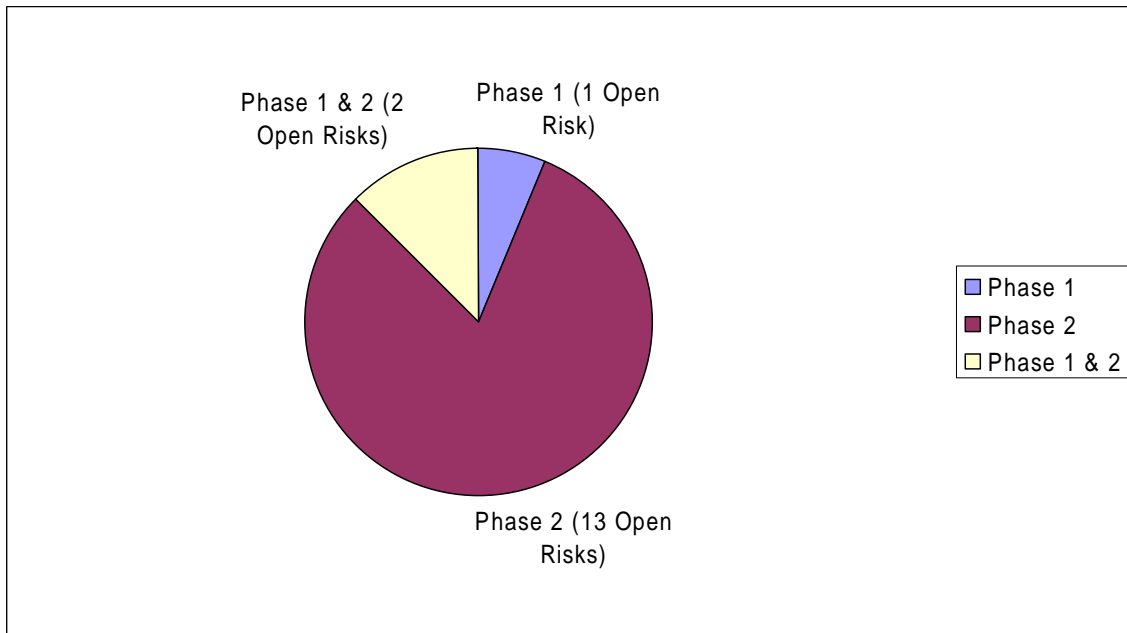
We also view the FBI's ability to prepare the data for transfer from ACS into Sentinel as a significant challenge. Much of the work to be done for data cleansing will depend on the condition of the data in ACS, which is the data to be cleansed then migrated to Sentinel. According to the FBI, one significant problem in ACS is that the data fields do not check or correlate. This means that data in a given field may not represent the data expected in that field. For example, "XXXXX" could be entered in the field for recording the date an item was entered into ACS. If a large amount of data in ACS is in this or a similar condition, this could have a significant impact on Sentinel's development schedule.

Migration of data from ACS to Sentinel is another potential significant challenge. There are more than 23 million records in ACS that will need to be migrated to Sentinel, and a major problem for the data migration is that ACS data is linked by serial numbers. One of the challenges will be to keep the data together during migration. In addition, the timing of this data migration will be crucial. During data migration there needs to be a minimal number of new ACS entries;

otherwise migration can never be fully completed. One idea the FBI is considering is to make ACS inaccessible for a period of time during this migration. Two other options are to turn off the electronic case file (ECF) on ACS and only allow entries into Sentinel while still using the ACS user interface or to flag ECF data when it has been accessed and queue the flagged data for migration into Sentinel within 24 hours.

Our review of the April 30, 2007, risk register showed that the majority of the 16 open risks are most likely to affect the second phase of the Sentinel project.⁵⁵ As shown in the following chart, the Risk Review Board classified 15 of the 16 (94 percent) risks as having a potential impact on Phase 2.⁵⁶ Appendix 7 lists the 16 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

Risk Mitigation Strategies

According to the Risk Management Plan, a risk mitigation strategy should be developed for each open risk to eliminate or reduce the probability or impact of the risk on Sentinel’s success. According

⁵⁵ The April 30, 2007, risk register is the latest register that the FBI provided us.

⁵⁶ Two risks were assigned to both Phases 1 and 2.

REDACTED FOR PUBLIC RELEASE

to the Risk Management Plan, risk mitigation strategies should include the following information:

- description of the mitigation activity (required),
- organization and individual responsible for executing the mitigation strategy (required),
- measure of effectiveness (required),
- schedule of activities with completion dates, and
- resources required and cost estimates of additional activities

The Risk Management Plan requires a mitigation strategy for any open risk assessed with at least a medium impact or probability of occurrence and calls for the mitigation strategies to be recorded in the risk register. The strategies should be reviewed and revised during team status meetings and risk management meetings.

We reviewed the April 30, 2007, risk register and found that the FBI had developed mitigation strategies for the 9 risks for which a strategy is required.⁵⁷ However, we found that mitigation strategies for all 9 were incomplete because none of them included a description of how the effectiveness of the mitigation strategy would be measured. In addition, none of the mitigation strategies described the resources required to implement the strategy or the cost of its implementation.

Contingency Plans

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 at least medium 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 April 30, 2007, risk register included a contingency trigger and

⁵⁷ Of the 16 open risks in the April 30, 2007, risk register, 6 had both a probability of occurrence and severity of impact assessed below "medium" and are therefore not required to have a mitigation strategy. However, the FBI developed mitigation strategies for them anyway. One of the 10 remaining risks did not have probability or severity ratings, so we could not determine whether it required a contingency plan.

contingency plan for only 3 of the 9 risks required to have a contingency plan. In addition, only 2 of the risks ranked in the top 5 risks had a contingency trigger or plan. Yet, while the FBI is not fully complying with the risk management plan's contingency trigger and contingency plan requirements, we found that the FBI's compliance has improved since our previous audit in December 2006.

The Sentinel Risk Manager said that the Phase 1 schedule delays had caused the Sentinel PMO to focus its efforts on avoiding further delays and that the discipline required to maintain the risk register had been diverted to other tasks. That explanation notwithstanding, 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.

Closed Risks

According to the Sentinel Risk Management Plan, risks that are resolved or closed will continue to be tracked and periodically reviewed to prevent occurrence and to document effectiveness and unintended consequences of the mitigation strategy employed. We reviewed the 68 closed risks in the April 30, 2007, risk register and found no evidence that the mitigation strategies for 32 of the risks had been fully implemented. We recognize that full implementation of a risk's mitigation strategy may not be necessary to prevent a risk from occurring. However, none of the entries for the 32 risks indicated that full implementation of the mitigation strategy was not warranted. To maintain the integrity of Sentinel's risk management process and to show that the FBI has effectively addressed all closed risks, we believe that the basis for closing risks should be clearly documented in the Sentinel risk register.

Risk Register Maintenance

The Sentinel Risk Management Plan requires that the Sentinel Risk Review Board meet at least biweekly and that the risk register be updated after each meeting. We found during the period from August 11, 2006, through May 4, 2007, the Sentinel Risk Review Board met 16 of the required 20 times. During this 8-month period, we identified 4 periods when the Risk Review Board went 3 weeks or more without meeting. The Sentinel Risk Manager told us holidays and major program reviews caused the lapses in the standard meeting schedule.

REDACTED FOR PUBLIC RELEASE

In addition, we found other problems with the maintenance of the risk register.

- The risk register did not always accurately document the date of the Risk Review Board meeting, suggesting to us that FBI personnel could not determine whether they were looking at the most recent risk information.
- Some risk registers with different dates were exact duplicates, indicating to us that the risk information had not been updated.

When the FBI does not adhere to the disciplined processes required by the Sentinel Risk Management Plan, the project becomes increasingly vulnerable to risks. For Sentinel to succeed, risks must be diligently monitored and managed, and accurate data on the risks facing Sentinel must be available to the PMO staff as well other oversight organizations both within and outside the FBI.

Risk Ownership

When a new risk is opened, the Sentinel Risk Review Board assigns an owner to that risk. Risk owners are required to: (1) draft the risk mitigation plan; (2) determine contingency triggers, (3) draft contingency plans to reduce the impact of a risk condition actually occurring, (4) report on statistics, and (5) ensure that mitigation plan is implemented. At the time of our audit, most risk owners headed one of the units that make up the Sentinel PMO. Most of the risk owners also sat on Sentinel's risk review board. We support the idea of having one person taking a lead role in managing each risk. However, as discussed below, the process of risk ownership does not appear to be functioning as intended. Specifically, during interviews with risk owners we found that some:

- could not explain the nature of the risks they had been assigned,
- were not the most active in designing or implementing the strategy for mitigating the risk,
- thought they did not have the expertise to fulfill their role as risk owner, or

REDACTED FOR PUBLIC RELEASE

- thought they did not have the authority or capability to implement a risk's mitigation strategy.

In addition, the responsibility for managing Sentinel's risks is disproportionate; two people were responsible for the majority of the risks open as of April 2007. In our judgment, risks cannot be adequately managed if the personnel assigned cannot do not have the required expertise or cannot devote a sufficient amount of time to a particular risk.

Issue Tracking

According to the Sentinel Risk Management Plan, risks that are considered unavoidable, and therefore its mitigation strategy options are outside of Sentinel program management control, are to be assigned as an issue and tracked and reported accordingly. If a risk is identified as an issue by the Sentinel PMO, it is transferred from the open risk section of the risk register to the closed risk section, where it is no longer actively managed. However, the FBI has not implemented a system to track issues and their resolution. Sentinel officials told us that they are aware of the need to actively manage issues and are considering different methods to do so.

The FBI has made significant progress in implementing a program to manage the risks that threaten Sentinel's cost, schedule, and performance. However, the effectiveness of the risk management program depends on disciplined implementation, and we found that the FBI has not always adequately implemented the processes necessary to reduce the risks that Sentinel faces. With respect to currently identified project risks, we view the FBI's ability to interface with the systems from which it will extract data as a potentially significant challenge. In Phase 1, Lockheed Martin had unanticipated problems connecting Sentinel with ACS because there was no detailed documentation describing how ACS works. Consequently, Lockheed Martin had to create the documentation itself. The Sentinel PMO did not anticipate this task because the managers of ACS told the PMO that all of the necessary documentation existed. Because this unexpected task strained both the Phase 1 budget and schedule, the PMO is now tracking documentation for the other systems with which Sentinel must interface as a risk.

REDACTED FOR PUBLIC RELEASE

Bill of Materials

A Bill of Materials (BOM) is a document that centralizes information from numerous system documents. The BOM should list all parts and components, both hardware and software, that comprise an IT system. According to the FBI's LCMD, a BOM should provide a complete list of all parts, assemblies, COTS equipment, and software that make up the system as well as the information required to construct new units for the system or order spare parts for it.

Lockheed Martin submitted a BOM, as required, as part of its proposal when competing for the Sentinel project. Contractually, Lockheed Martin is required to purchase the list of items on the BOM. However, as is to be expected in a project as complex as Sentinel, Lockheed Martin has needed to revise the BOM submitted in its proposal. Several allowable reasons for BOM revisions include:

- Specific models of equipment have become obsolete prior to purchase;
- Model numbers of specific equipment have changed;
- The cost of specific hardware or software has changed;
- Items were mistakenly omitted on the original BOM; and
- The design or approach of Sentinel has evolved as the project has progressed.

Because of the importance of having an accurate BOM, the Sentinel PMO established a BOM Deviation Policy. This policy establishes the criteria for what constitutes a change to the BOM and whether Lockheed Martin needs the FBI's approval prior to making a change to the BOM. The policy defines a deviation as any difference between the original cost, model number or purchase date, or any addition or deletion of material. Lockheed Martin must obtain approval from the Sentinel Contracting Officer's Technical Representative (COTR) for changes when the cost of materials to be purchased increases from the originally proposed cost by the lesser of 5 percent or \$1,000, or there is a change to the purchase date of material by

REDACTED FOR PUBLIC RELEASE

30 days or more.⁵⁸ However, changes to the BOM resulting from Sentinel Configuration and Change Management Board proceedings do not require approval from the COTR.⁵⁹ Every month, Lockheed Martin is required to submit a BOM Deviation Report that lists all changes made to the BOM in the last month, regardless of whether FBI approval is needed.

According to the Sentinel COTR, Lockheed Martin also established its own procedures for making changes to the BOM, requiring its Engineering Review Board to approve every change request before seeking approval from the FBI. However, according to the COTR Lockheed Martin employees viewed approval by the Engineering Review Board as final and therefore did not submit all changes to the FBI as required. The Sentinel PMO has recognized that Lockheed Martin employees were not fully aware of the PMO's policies for making changes to the BOM and has begun working with Lockheed Martin to clarify its policies.

In addition to not following the policy for making changes to the BOM, Lockheed Martin also did not submit the required BOM Deviation Reports. According to the Sentinel COTR, Lockheed Martin's failure to submit the deviation reports was linked to confusion about the approval process for making changes to the BOM, as discussed above. Instead of BOM Deviation Reports, Lockheed Martin provided periodic equipment purchase reports to the PMO. However, these reports could not be reconciled to the BOM and did not document proper FBI approval, so the PMO could not verify whether all items on the purchase report were listed on the BOM or received FBI approval. The same was true of Lockheed Martin's invoices.

The Sentinel PMO is aware of these shortcomings and has established a joint Lockheed Martin-FBI team to revise the PMO's policies for making changes to the BOM. FBI officials said the revised policy would include solutions to all of the issues discussed above. In

⁵⁸ The Sentinel COTR is assigned to the Business Management Unit and assists the contracting officer with the technical oversight necessary to execute the Sentinel contract. Specifically, the COTR is the official recipient of all contract deliverables, coordinates the delivery of government furnished equipment and information to the prime contractor, and verifies invoices.

⁵⁹ The Sentinel Configuration and Change Management Board is responsible for approving updates to any of Sentinel's baselines. The Board adjudicates proposed changes affecting system requirements, configuration management, risk management, and documents that affect the project's scope, schedule and cost.

REDACTED FOR PUBLIC RELEASE

addition, at the close of Phase 1 the FBI required Lockheed Martin to submit a BOM documenting the system as it was built and reconcile that BOM to Lockheed Martin's invoices.

In addition to the issues with which the FBI was aware, we identified another significant flaw in the PMO's BOM deviation policy. While the policy states that a deviation is any addition or deletion to the BOM, the policy does not require FBI approval for these additions or deletions. Instead, the policy only requires approval for cost increases and changes to purchase dates for items already on the BOM. The lack of written procedures for making changes to the BOM increases the risk that the document will not provide an accurate reflection of the equipment that has been purchased or that needs to be purchased to ensure successful completion of the project. This information is necessary to control costs, manage property, and prevent unnecessary or wasteful purchases. The Sentinel PMO agreed with our concerns and said that this issue would be addressed in revised BOM policies.

According to Lockheed Martin records obtained from the FBI, changes to the BOM have been significant, resulting in a reduction of nearly \$7 million from the cost of Phase 1. As shown in the following table, during Phase 1 Lockheed Martin deferred the purchase of \$5.8 million worth of equipment to later phases and purchased \$1.5 million worth of equipment originally scheduled to be purchased during future phases. Coupled with changes resulting from modifications in the design of Sentinel and the substitution of newer equipment not available at the time of Lockheed Martin's proposal, the cost of materials for Phase 1 decreased by nearly \$7 million.

REDACTED FOR PUBLIC RELEASE

Changes to the Bill of Materials

Description of Change	Added Cost	Savings	Total Added Cost & Savings
Deferred Equipment Purchases (from Phase 1 to future phases)	\$0	-\$5,830,907	-\$5,830,907
Forwarded Equipment Purchases (from future phases to Phase 1)	\$1,541,887	\$0	\$1,541,887
Change in Equipment Design or Selection	\$0	-\$3,081,112	-\$3,081,112
Additions, Price Modifications, and Deletions	\$434,768	\$0	\$434,768
Total	\$1,976,655	-\$8,912,019	-\$6,935,364

Source: Lockheed Martin data obtained from the FBI

We concluded that the FBI needs better controls to ensure the accuracy of the equipment on the BOM and adequate cost control and property management. In addition, we found that the FBI cannot track changes made to successive versions of the BOM. Without a reliable system to track equipment purchased by the BOM to FBI property management records, the opportunity exists for the loss of system equipment. Management of project costs is also made more difficult, resulting in the increased possibility that project funds could be wasted. Finally, absent a way to document changes as the BOM is updated, it is difficult to determine whether the listed equipment is current and necessary for completion of the project.

The Sentinel Program Manager agreed with our assessment of the BOM deviation policy. He acknowledged that he has found discrepancies between the BOM and the equipment listed in the FBI's property management system. As noted above, one of the close-out activities for Phase 1 was a line-by-line inventory of all equipment listed on the BOM.

Planning for Phase 2 and Lessons Learned

The FBI's experience with Phase 1 has had a substantial impact on planning for the remaining phases of Sentinel. At the conclusion of our audit field work in May 2007, the FBI's Phase 2 activities were limited to planning rather than development. The FBI and Lockheed

REDACTED FOR PUBLIC RELEASE

Martin were examining the best way to divide the remaining Sentinel development tasks. To accomplish this, Lockheed Martin and the FBI were negotiating an engineering change proposal to replan the remaining work, but the FBI had not decided on the number of subsequent phases or the content of those phases. However, FBI officials said the cost estimate and overall timeframe of Sentinel completion by December 2009 had not changed. Below we discuss six lessons the FBI and Lockheed Martin learned during Phase 1 and how the FBI plans to adjust future phases to reduce risk identified by these lessons.

Complexity of COTS Integration

In our December 2006 Sentinel report, we cited the integration of COTS components into a system that meets the FBI's needs as one of the most significant risks to Sentinel's cost, schedule, and performance. During Phase 1, integrating COTS software proved to be a significant challenge for Lockheed Martin, one that contributed to the delay in the delivery of Phase 1. This challenge was compounded by Sentinel's use of relatively new software and the need for personnel with security clearances.

According to the Chief of the Sentinel System Development Unit, while the complexity of integrating COTS software also will affect subsequent phases of Sentinel, it is difficult to determine the degree of the impact. In an effort to mitigate the schedule and cost risks associated with these complexities, the FBI and Lockheed Martin plan to set up a prototyping lab for Phase 2 in which engineers will be able to test early in the phase how different COTS products interact when they are integrated. This will allow engineers to gain early insight into potential problems that may occur during Phase 2 and allow Lockheed Martin enough time to adjust its design accordingly.

Interfacing with ACS is Complex

The web portal developed in Phase 1 displays data stored in ACS. To accomplish this, Lockheed Martin had to build interfaces between Sentinel and ACS, a task during which Lockheed Martin gained familiarity with the complexity of interfacing with ACS. According to Sentinel PMO officials, the documentation or blueprints for ACS were not sufficiently detailed to allow Lockheed Martin to build the interfaces necessary for Phase 1 as it initially intended. Instead, as described previously, Lockheed Martin had to reverse engineer and fix approximately 30 interfaces to build the Phase 1 portal. This

REDACTED FOR PUBLIC RELEASE

unexpected additional work resulted in a significant strain on the project schedule and budget.

To minimize the cost and schedule risk associated with interfacing with ACS and other legacy systems, the FBI plans to reexamine the functionality of the subsequent phases of Sentinel and the need to interface with the FBI's legacy systems. At a March 2007 meeting, the FBI eliminated from the project plans several interfaces with little-used FBI legacy systems. As discussed previously, the FBI and Lockheed Martin are currently restructuring the remaining phases of Sentinel and a major factor in that restructuring is the desire to minimize temporary interfaces with ACS.

Phase 1 Schedule Focused on Documents

According to the FBI's Sentinel Program Manager, some of the deliverables in the Phase 1 schedule were documents. However, in some cases, Lockheed Martin delivered incomplete or poorly constructed documents so that it could meet due dates. Because these documents did not serve their intended function, the project was delayed.

According to the program manager, the Phase 2 deliverables will be based more on the delivery of functionality rather than the delivery of documents. For example, Lockheed Martin may not be required to deliver a document detailing the Phase 2 design if the same need can be met using computer software. While some of the Phase 2 deliverables will still be documents, their purpose will be to support a specific function. According to the PMO, documents delivered by Lockheed Martin will not be accepted unless they meet FBI standards.

Weaknesses in Phase 1 Requirements Validation

Requirements validation is the process by which FBI and Lockheed Martin personnel meet during what is called the Requirements Clarification Review (RCR) to discuss the requirements to be completed during the upcoming phase of the project. The RCR is held at the beginning of each phase. During the RCR, requirements that were identified at the beginning of the project are reviewed by both parties to determine whether the functionality provided by completion of the requirement is still necessary. If the requirement is determined to still be applicable to the project, RCR participants then break the requirement down into sub-requirements to be completed in support of the main requirement. The product of the RCR is the

REDACTED FOR PUBLIC RELEASE

Requirements Clarification Document (RCD) which delineates the requirements and sub-requirements to be completed during the current phase.

FBI officials said that not enough time was devoted to requirements validation during Phase 1 and consequently some of the Phase 1 requirements were unclear or incomplete. These shortcomings in the Phase 1 requirements led to disagreements with Lockheed Martin about the design of Phase 1 and created problems during testing. To resolve the issues stemming from the Phase 1 requirements validation, the PMO and Lockheed Martin plan to begin Phase 2 requirements validation well in advance of the start of Phase 2 and devote more time to the effort.

Scheduling of Design Reviews

The Phase 1 schedule did not allow enough time between the Preliminary Design Review, the Critical Design Review, and the Final Design Review. Key design documents must be developed by Lockheed Martin and reviewed by the FBI at each of these interrelated design reviews. In addition, the schedule needs to allow adequate time for the following:

- The FBI must review and comment on the documents;
- Lockheed Martin must incorporate the FBI's comments and resubmit the documents to the FBI; and
- The FBI must verify that Lockheed Martin adequately addressed the FBI's comments.

As discussed in the previous finding, the lack of time between design reviews led to incomplete design documents that did not incorporate all of the FBI's technical comments. In turn, the incomplete design documents led to problems during the testing phase of the project. In the subsequent phases of Sentinel, the FBI has committed itself to allowing sufficient time between design reviews.

Construction and Maintenance of Schedule

According to the Sentinel Program Manager, the Phase 1 schedule was extremely tight from its inception. In addition, some of the tasks were scheduled out of order. Another issue that the PMO and Lockheed Martin encountered was starting and ending dates for

REDACTED FOR PUBLIC RELEASE

tasks were entered into the schedule as hard constraints. This means that even if the project progressed at a faster rate than planned, tasks could not be recorded as started until the date specified. This, in effect, prevented the project from ever achieving an "ahead of schedule" status.

These hard constraints were also applied to task end dates. As a result, whether or not the tasks had actually been completed and signed off on by the PMO, on the end date identified in the schedule the tasks were automatically listed as complete. The Sentinel Program Manager said that Lockheed Martin personnel mismanaged the schedule in this way because of intense pressure from FBI and Lockheed Martin managers to stay on schedule. This misidentification of task status contributed to further delays and provided poor visibility into the project's actual status.

For future phases, the PMO plans to work with Lockheed Martin to ensure a more accurate assessment of progress. The PMO and Lockheed Martin also plan to reduce the number of hard constraints from the schedule to improve the accuracy of progress measurement. The removal of constraints will also allow for the adjustment of task end dates in the event the project falls behind schedule. During Phase 1, when a task that affected the completion of a related task fell behind schedule, the end date of the related task remained static. This resulted in schedule compression and creation of an unrealistic schedule. The removal of hard constraints will allow for greater visibility into how delays affect the completion of other tasks and ultimately the entire phase.

Actions Taken on Previous OIG Recommendations

During our audit, we examined the FBI's actions to address recommendations we made in our earlier audit reports on Sentinel and found that the FBI was, in general, taking action to resolve our concerns. Based on the FBI's actions, we closed 5 of the 12 recommendations. We also noted that the FBI agreed with the remaining recommendations and was in the process of taking corrective action. Our recommendations dealt generally with the FBI's need to complete required planning and general management oversight policies and procedures for Sentinel in order to help ensure its success.

In our March 2006 report, *The Federal Bureau of Investigation's Pre-Acquisition Planning For and Controls Over the Sentinel Case*

REDACTED FOR PUBLIC RELEASE

Management System, we made seven recommendations, of which four have been closed. The remaining three recommendations relate to the need to complete certain planning documents, the staffing of the Sentinel PMO, and Sentinel training. In addressing these recommendations, we found that the FBI:

- continued to work on completing its system security plan and completed its independent verification and validation (IV&V) plan, which partially closes this recommendation;
- filled 70 of 75 positions within the Sentinel PMO, with three of the vacancies tentatively filled; and
- continued work on a comprehensive training plan with schedule and cost estimates.

In our December 2006 report, *Sentinel Audit II: Status of the Federal Bureau of Investigation's Case Management System*, we made five recommendations, one of which has been closed. The four remaining recommendations were that the FBI should: (1) develop contingency plans as required by the Sentinel Risk Management Plan, (2) provide experienced contractors to conduct an IV&V process throughout the Sentinel project, (3) determine the appropriate amount of management reserve for each phase of the project, and (4) fill the vacant Sentinel PMO positions needed to complete Phase 1 of the project.

In performing the fieldwork for our current audit, and as mentioned earlier in this report, we found that the FBI has improved its development of contingency plans and triggers as required by the Sentinel Risk Management Plan. With the implementation of Phase 1, there is no longer a need to address the risks related to that phase. However, we continue to have concerns regarding the FBI's implementation of its Risk Management Plan, as well as some of the risks we noted earlier concerning the future Phases of Sentinel, and we will continue to monitor their implementation during future audit work.

Also noted earlier in this report, we found that the FBI has begun utilizing a contractor, Booz Allen, to perform IV&V of the Sentinel project. We found that the IV&V process has resulted in numerous recommendations to Sentinel Phase 1 development. Based on our examination of the FBI's implementation of this process, this recommendation can be closed through our normal audit follow-up process.

REDACTED FOR PUBLIC RELEASE

Because each of Sentinel's four phases will have a separate task order with its own funding, and planning for Phase 2 continued after our fieldwork ended, we were unable to determine whether the FBI is establishing a management reserve based on an assessment of the project risks for each phase and for the project overall. However, we will continue to monitor the FBI's utilization of management reserves in future audit work. After the completion of Phase 2 planning, the methodology currently being used by the FBI to develop management reserves should become more apparent.

Due to the importance of the PMO in the oversight of Sentinel, we recommended in both of our previous Sentinel audits that the PMO complete hiring as soon as possible for the vacant PMO positions. 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 December 2006 audit the PMO has increased its planned size from 73 positions to 76 positions, reallocated positions among PMO units, and was in the process of filling 3 positions. As of May 2007, the PMO consisted of 70 of the 76 personnel identified in the FBI's Sentinel Staffing Plan (92 percent) as required to properly oversee the project. According to the FBI, the objective in staffing the PMO is to form an integrated team of subject matter experts from government, federally funded research and development centers, and system engineers and technical assistance contractors to maximize program expertise.⁶⁰ The following table summarizes the PMO's staffing level as of May 15, 2007, and shows the progress the FBI has made in staffing the office since October 2006.

⁶⁰ 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.

SENTINEL PMO STAFFING REQUIREMENTS

Organizational Units	Planned Staff ^(a)	Staff on Board, October 2006	Staff on Board, May 2007 ^(b)
PMO Front Office	11	11	10
Organization Change Management Team	6	3	4
Business Management	11	13	11
Program Integration	10	10	9
System Development	28	25	28
Transition	5	4	5
Operations & Maintenance	5	0	3
Total	76	65	70

Source: The FBI

Notes: (a) Since October 2006, the Sentinel PMO has revised the total planned staff from 73 to 76. 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.

(c) In our previous report, we identified this unit as two separate units; Program Leadership, and Direct Report Staff.

For a more complete description of PMO staff and their duties, see Appendix 8.

Of the current vacancies, one is a government position — a Supervisory Special Agent — and one is a contractor position — an Organizational Change Management (OCM) expert. Hiring for the other position — a System Engineer — has been delayed until Phase 3. The Chief of the Business Management Unit said that a setback in filling PMO positions quickly occurred when the FBI instituted a hiring freeze as a result of the FY 2007 continuing resolution. He said that another setback to filling open PMO positions quickly is the amount of time that is required to execute and adjudicate Top Secret clearance

REDACTED FOR PUBLIC RELEASE

background checks; he said that the PMO has been submitting its background check requests in expedited status.

The following table shows the changes in the number of planned staff from October 2006 to May 2007.

**Changes in Sentinel PMO Staffing Requirements,
October 2006 to May 2007**

Organizational Unit	Change in Planned Staff
PMO Front Office	+1
Organization Change Management Team	+2
Business Management	-3
System Development	+3
Total	+3

Source: The FBI

The FBI Deputy CIO said he thinks the PMO is “pretty lean” in comparison to other PMOs he has seen. He said that he and the Sentinel Program Manager looked at best practices while developing the structure of the PMO, but were also mindful that while they could select whomever they wanted internally in the FBI to work at the PMO, this would also put another component of the FBI at a disadvantage by losing top personnel. For expertise in areas in which the government was weak, contractors were chosen. The FBI Deputy CIO said that he is happy with the PMO’s return on investment thus far in the project.

The FBI Deputy CIO also said that as the Sentinel project progresses, the focus areas and personnel needs of the PMO will shift. For example, Operations and Maintenance (O&M) will become more of a focus, especially by the end of Phase 2. Since this will result in the need for a different skill set than is currently available at the PMO, there will be changes in personnel. Fewer designers will be needed, and more people to maintain the system will be required. The FBI Deputy CIO said the PMO will probably start trading personnel out of the PMO as the need arises.

While we concluded that the FBI is making progress in implementing the recommendations we have made during our prior

audits, we will continue to monitor the progress made by the FBI in implementing the remaining open recommendations through our audit follow-up process and through our future Sentinel work.

Conclusion

The FBI has a broad range of management controls and processes that should aid it in managing the development of Sentinel. Of the four controls and processes we reviewed in depth, we found that the FBI has made significant progress in implementing each. However, the FBI's experience with Phase 1 demonstrates the high priority the FBI must assign to the entire range of management controls and processes over the project. During Phase 1, issues the FBI experienced with three of the four of controls – earned value management, risk management, and the bill of materials – show that additional improvements need to be made to allow the FBI to adequately monitor cost, schedule, and performance of future phases of Sentinel.

Lockheed Martin and the FBI will likely face many of the issues encountered in Phase 1 during subsequent phases of Sentinel's development. For example, even though the FBI plans early prototyping to reduce the likelihood of problems when integrating COTS components, the next phase of Sentinel will likely encounter unexpected problems integrating the various COTS components into legacy FBI systems in a way that meets the FBI's needs. However, rigorous implementation of processes and lessons learned is necessary to minimize significant deviations from cost, schedule, technical, or performance baselines.

Recommendations

We recommend that the FBI:

3. Collect and report EVM data for both the performance measurement baseline approved at the integrated baseline review as well as the revised performance measurement baseline.
4. Reconcile the discrepancy between the costs Lockheed Martin reported for Phase 1 with Lockheed Martin's EVM data, and develop and implement policies and procedures to prevent any future discrepancies.

REDACTED FOR PUBLIC RELEASE

5. Develop and implement effectiveness measures for all risk mitigation plans.
6. Ensure that personnel assigned to manage Sentinel risks devote sufficient time to the risk and have the experience and authority to adequately manage the risk.
7. Document and track project issues, risks that have occurred, as well as the plan to resolve those issues and their ultimate resolution.
8. Implement policies and procedures to ensure that any changes to the bill of materials receive proper authorization and that the changes can be reconciled to the bill of materials submitted in Lockheed Martin's proposal.
9. Implement policies and procedures to ensure that materials contained in Lockheed Martin invoices can be reconciled to the bill of materials or an FBI approval for a change to the bill of materials.

REDACTED FOR PUBLIC RELEASE

**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,
- 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.

- EVM cost data needs to be reconciled with the costs incurred that was reported by Lockheed Martin, the prime contractor for the development of Sentinel.
- Contingency plans for highly ranked project risks need to be developed.
- Measurements of effectiveness for risk mitigation plans need to be developed.
- Project issues (risks that have occurred) and their resolution are not tracked.

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.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

The objectives of this audit were to determine: (1) the status of the Sentinel project, including the FBI's monitoring of the contractor's performance during Phase 1; (2) the planning for and progress of Phase 2; and (3) the resolution of remaining concerns identified in our previous two audit reports.

Scope and Methodology

The audit was performed in accordance with the *Government Auditing Standards*, and included tests and procedures necessary to accomplish the audit objectives. We conducted work at FBI headquarters in Washington, D.C., and at the FBI Sentinel Program Management Office in McLean, Virginia.

To perform our audit, we interviewed officials from the FBI, Office of the Director of National Intelligence (DNI), the Department of Justice, and the Office of Management and Budget. 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; prior OIG Sentinel reports; and other reports from the OIG and other agencies on the FBI's information technology.

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 also examined actual costs, progress toward completion of Phase 1, and planning for Phase 2. Additionally, we interviewed FBI officials responsible for contract implementation.

To update issues identified in the OIG's December 2006 Sentinel audit report, we interviewed responsible FBI and contractor officials and reviewed plans and procedures for cost tracking, risk management, contingency planning, IV&V, and PMO staffing. We also interviewed FBI officials and obtained the updated status on issues relating to information sharing and EVM.

ACRONYMS

ACS	Automated Case Support
Booz Allen	Booz Allen Hamilton
BOM	Bill of Materials
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-The-Shelf
ECF	Electronic Case File
EVM	Earned Value Management
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
IBR	Integrated Baseline Review
ICM	Investigative Case Management
IMS	Integrated Master Schedule
IT	Information Technology
ITIM	Information Technology Investment Management
IV&V	Independent Verification and Validation
LCMD	Life Cycle Management Directive
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PMO	Program Management Office
RCD	Requirements Clarification Document
RCR	Requirements Clarification Review
SRS	System Requirements Specifications
UNI	Universal Index
VCF	Virtual Case File
WACS	Web-Enabled Automated Case Support

THE FBI'S LIFE CYCLE MANAGEMENT DIRECTIVE

The FBI's IT Systems Life Cycle Management Directive (LCMD) is comprised of interrelated components that include Life Cycle Phases, Control Gate Reviews and Boards, and Project Level Reviews. Because Sentinel has multiple phases, it will pass many of the life cycle phases, control gate reviews, and project level reviews multiple times.

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	<u>System Concept Review</u> approves the recommended system concept of operations and occurs at the end of Phase 1 of LCMD.
Gate 2	<u>Acquisition Plan Review</u> 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	<u>Final Design Review</u> 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	<u>Deployment Readiness Review</u> 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 Gate 4 signifies readiness for system implementation.
Gate 5	<u>System Test Readiness Review</u> 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	<u>Operational Acceptance Review</u> 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	<u>Disposal Review</u> 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**

New FBI Process for Overseeing IT Projects

In November 2006, a new FBI IT governance secretariat began operations. The governance secretariat established several working groups to assess an IT project each time it requests approval to pass through an LCMD gate. Based on the need for varying expertise, the role of each working group varies according to the LCMD gate, but the entire process requires input from the following working groups: the Investment Project Review Working Group, Technical Review Working Group, Enterprise Architecture Working Group, and the Configuration Management Quality Assurance Working Group.

Assessments Under New Governance Process

As Sentinel approaches an LCMD gate, the Sentinel PMO works with the working group responsible for doing assessments for that gate. LCMD control gate documentation is normally submitted 3 weeks in advance of the final assessment for review.

The cognizant working group has 3 days to provide a preliminary assessment of the documentation. To save resources and time, the FBI will cancel the formal gate review if the working group discovers significant issues during the preliminary assessment. If a project's manager disagrees with the working group's preliminary assessment, the Chief Technology Officer makes a determination.

If a project passes the preliminary assessment, the working groups have 10 days to conduct a full assessment. The executive summaries of the working groups are compiled along with conditions necessary for the project to clear the gate, and a formal gate review meeting is conducted, during which one of the following four FBI IT Decision Board decides whether the project should clear the gate.

- The Investment Management Board oversees the System Concept Review (Control Gate 1).
- The Project Review Board oversees the Acquisition Plan Review (Control Gate 2) and the Disposal Review (Control Gate 7).

REDACTED FOR PUBLIC RELEASE

- The Technical Development and Deployment Board oversees the Final Design Review (Control Gate 3), the Deployment Readiness Review (Control Gate 4), the System Test Readiness Review (Control Gate 5), and the Operational Acceptance Review (Control Gate 6).

Previous FBI Process for Overseeing IT Projects

The FBI's previous IT governance system did not require working group assessments of a project's documentation at each LCMD control gates. However, under the old system, the Technical Review Board was required to review the project at Gate 3, the Final Design Review.

- 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.

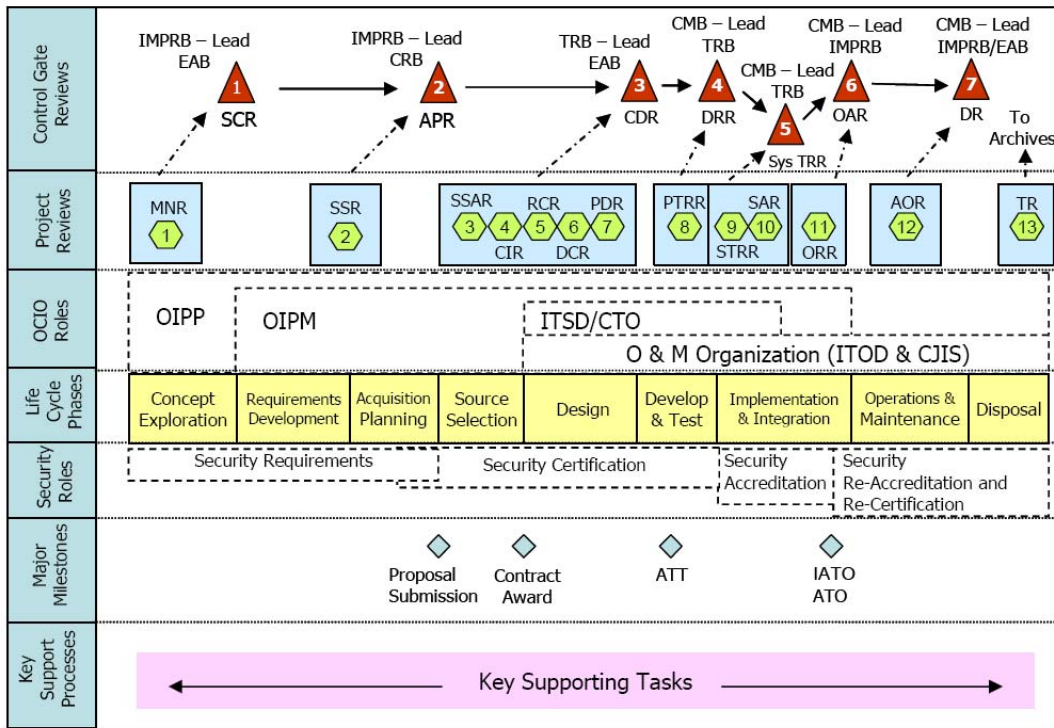
**PROJECT LEVEL REVIEWS:
CONCEPT EXPLORATION PHASE THROUGH DESIGN PHASE**

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	Technical review of the decomposition of the system or product (hardware, software, and manual operations).
7. Preliminary Design Review	Can be a single event or spaced out over time during the Design Phase to cover logical groupings of configuration items. The review proves that the concept and the specification for the concept are feasible and will satisfy higher level requirements allocated to it, and to approve the preliminary design-to specifications and associated verification plans. All hardware, software, support equipment, facilities, personnel, and tooling should be reviewed in descending order of system to assembly.

REDACTED FOR PUBLIC RELEASE

REVIEW NAME	DESCRIPTION
8. Critical Design Review	Approves the build-to and code-to documentation and associated draft verification procedures, to ensure that the design presented can be produced, and that when built is expected to meet its design-to specification at verification.
9. Product Test Readiness Review	Series of technical reviews at which the customer concurs that the solution provider is ready to conduct official "sell-off" tests during which official verification data will be produced.
10. Site Test Readiness Review	Technical review at which the customer concurs that the supplier is ready to conduct official "sell-off" tests during which official verification data will be produced.
11. Site Acceptance Review	Technical review where customer organization accepts the system or segment delivered to the site.
12. Operational Readiness Review	Technical review between the Project Office and the product user to verify readiness for system validation required by the Operational Readiness Plan developed in compliance with the Mission Requirements Concept of Operations Document at the outset of the project.
13. Operational Acceptance Test	Tests the operational capability of the system from a deployed user perspective. Becomes the basis for government acceptance of the Phase 1 product.
14. Deployment Acceptance Review	Provides the final approval ("go-ahead") to deploy the Phase 1 system.

FBI'S LCMD IT SYSTEMS LIFE CYCLE



LEGEND

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

PRIOR REPORTS ON THE FBI'S INFORMATION TECHNOLOGY

Below is a listing of relevant reports discussing the FBI's information technology (IT) 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 December 2006, the OIG issued a report entitled, *Sentinel Audit II: Status of the Federal Bureau of Investigation's Case Management System*. The report stated that the FBI made progress addressing concerns previously reported. The OIG recommended that the FBI take the following steps:

- ensure that the management reserve is based on an assessment of project risk 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, and
- complete hiring as soon as possible for the vacant Project Management Office (PMO) positions needed during the current project phase.

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:

REDACTED FOR PUBLIC RELEASE

- 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 Earned Value Management (EVM) process,
- the FBI's ability to track and control Sentinel's costs, and
- the lack of complete documentation required by the FBI's information technology investment management (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 Modernization 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.

REDACTED FOR PUBLIC RELEASE

- 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 July 2007, the GAO issued a report on the extent to which the FBI had established best practices for acquiring Sentinel and estimating the project's schedule and costs.⁶¹ The GAO concluded that the FBI was managing Sentinel in accordance with several key best practices for acquiring IT systems, including practices for evaluating offers and awarding contracts. However, the GAO also concluded that the FBI had not established performance and product quality standards for the program management contractors who support the FBI in overseeing Sentinel. In addition, the GAO reported that the FBI's

⁶¹ U.S. Government Accountability Office, *Information Technology: FBI Following a Number of Key Acquisition Practices on New Case Management System but Improvements Still Needed*, July 2007.

REDACTED FOR PUBLIC RELEASE

policies, procedures, and supporting tools that formed the basis of Sentinel's schedule and cost estimates did not incorporate several key best practices. As a result, the GAO questioned the reliability schedule and cost estimates, noting that the estimates did not include all relevant costs and used inadequately documented methodologies.

In April 2007, the GAO issued a report entitled, *INFORMATION SECURITY: FBI Needs to Address Weaknesses in Critical Network* identifying ineffective controls in protecting the confidentiality, integrity, and availability of information and information resources. The GAO found that the FBI did not consistently (1) configure network devices and services to prevent unauthorized insider access and ensure system integrity; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Taken collectively, these weaknesses place sensitive information transmitted on the FBI's network at risk of unauthorized disclosure or modification, and could result in a disruption of service, increasing the FBI's vulnerability to insider threats.

In October 2006, the GAO issued a report entitled, *INFORMATION TECHNOLOGY: FBI Has Largely Staffed Key Modernization Program, but Strategic Approach to Managing Program's Human Capital Is Needed*. This report credited the FBI for filling almost all positions in its staffing plan. However, the report also noted a few key vacancies, and that the staffing plan was not derived using a documented data-driven methodology and did not provide for inventorying the knowledge and skills of existing staff, forecasting future knowledge and skill needs, analyzing gaps in capabilities between the existing staff and future workforce needs, and formulating strategies for filling expected gaps.

In February 2006, the GAO issued a report entitled *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

REDACTED FOR PUBLIC RELEASE

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 1,205 missing pieces of equipment valued at \$7.6 million.

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 (CIO) 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.

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

REDACTED FOR PUBLIC RELEASE

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.

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 plans 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

REDACTED FOR PUBLIC RELEASE

basis are inevitable and must be anticipated in the budget process if the FBI is to maximize the operational leverage that IT offers.

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 systems that could be used in developing a case management system and also an Independent Verification and Validation of Trilogy's VCF. In December 2004, the contractor issued the 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 17 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

REDACTED FOR PUBLIC RELEASE

Resources Management official did not have effective organization-wide authority.

- The FBI had not developed and implemented a data architecture.
- 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 late 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 21st 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

REDACTED FOR PUBLIC RELEASE

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.

Comparison of ACS-ICM, WACS, and PHOENIX Functionality to Sentinel's Phase 1 Deliverables

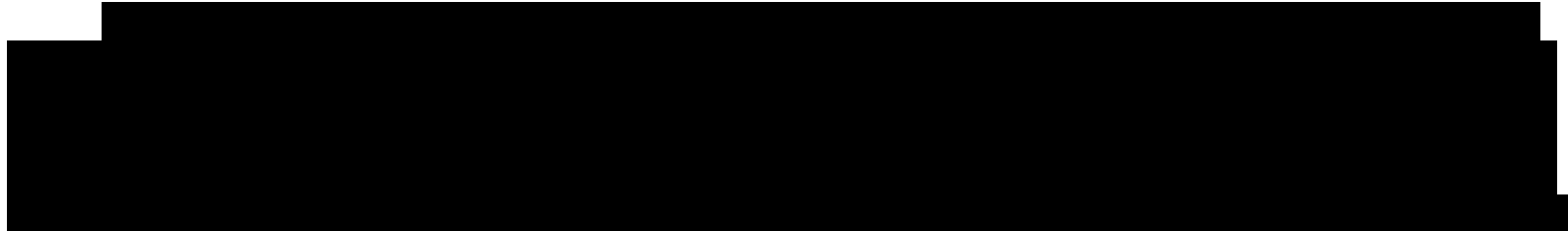
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

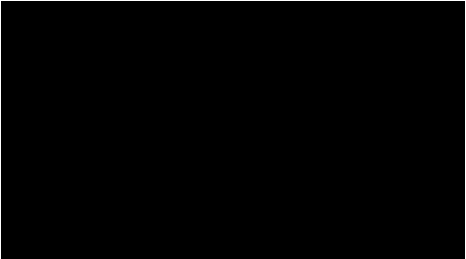

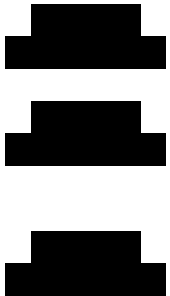
REDACTED FOR PUBLIC RELEASE

[REDACTED]			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: FBI

INDEPENDENT VERIFICATION AND VALIDATION
ISSUES AND RECOMMENDATIONS



	Issue/Risk	Recommendation	Status
1			

	Issue/Risk	Recommendation	Status
2	[REDACTED]	[REDACTED]	[REDACTED]
3	[REDACTED]	[REDACTED]	[REDACTED]

	Issue/Risk	Recommendation	Status
	[REDACTED]	[REDACTED]	[REDACTED]
4	[REDACTED]	[REDACTED]	[REDACTED]

	Issue/Risk	Recommendation	Status
5	[REDACTED]	[REDACTED]	[REDACTED]
6	[REDACTED]	[REDACTED] [REDACTED]	[REDACTED] [REDACTED]

	Issue/Risk	Recommendation	Status
7	[REDACTED]	[REDACTED]	[REDACTED]

	Issue/Risk	Recommendation	Status
8	[REDACTED]	[REDACTED]	[REDACTED]
9	[REDACTED]	[REDACTED]	[REDACTED]
10	[REDACTED]	[REDACTED]	[REDACTED]

	Issue/Risk	Recommendation	Status
11	[REDACTED]	[REDACTED]	[REDACTED]
12	[REDACTED]	[REDACTED]	[REDACTED]
13	[REDACTED]	[REDACTED]	[REDACTED]

	Issue/Risk	Recommendation	Status
14	[REDACTED]	[REDACTED]	[REDACTED]

REDACTED FOR PUBLIC RELEASE

	Issue/Risk	Recommendation	Status
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
15	[REDACTED]	[REDACTED]	[REDACTED]
16	[REDACTED]	[REDACTED]	[REDACTED]
17	[REDACTED]	[REDACTED]	[REDACTED]
18	[REDACTED]	[REDACTED]	[REDACTED]
19	[REDACTED]	[REDACTED]	[REDACTED]

	Issue/Risk	Recommendation	Status
20	[REDACTED]	[REDACTED] [REDACTED]	[REDACTED] [REDACTED]
21	[REDACTED]	[REDACTED] [REDACTED]	[REDACTED] [REDACTED]

	Issue/Risk	Recommendation	Status
22	[REDACTED]	[REDACTED]	[REDACTED]

Source: IV&V Contractor Reports

REDACTED FOR PUBLIC RELEASE

APPENDIX 7

RISK REGISTER OPEN RISKS

INFORMATION REDACTED

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 110 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 111 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 112 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 113 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 114 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 115 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 116 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 117 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 118 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 119 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 120 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

- 121 -

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

INFORMATION REDACTED

REDACTED FOR PUBLIC RELEASE

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.

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

U.S. Department of Justice



Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 22, 2007

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 III:
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 III: 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 feel free to contact me on 202-324-6165, or Ms. Robin Davis of my staff should you have any questions. Ms. Davis may be reached on (202) 324-2866.

Sincerely,

A handwritten signature in black ink, appearing to read "Zalmi Azmi", is positioned above the typed name.

Zalmi Azmi
Chief Information Officer

Enclosure

REDACTED FOR PUBLIC RELEASE

**Federal Bureau of Investigations (FBI)
Response to the Department of Justice (DOJ)
Office of the Inspector General (OIG) Draft Audit Report
SENTINEL Audit III: Status of the Federal Bureau of Investigation's
Case Management System**

Responses to Recommendations:

The FBI concurs with the recommendations of the DOJ OIG's Audit Report and has already taken positive measures to incorporate the recommendations in Program Management Office (PMO) operations. The following comments are provided:

Finding 1: Phase 1, Schedule, Cost, and Performance:

Recommendation #1: Reconsider the four-phase approach to developing SENTINEL to limit the scope of future phases to allow them to be completed in 9 months or less.

FBI Response: Completed. During a meeting with the DOJ OIG, the FBI OCIO, the SENTINEL Program Manager (PM), SENTINEL Deputy PM, and SENTINEL System Development Unit Chief on April 23, 2007, the philosophy of waterfall and incremental methodologies was discussed based on Phase 1 lessons learned. At that time, the FBI informed the DOJ OIG that it planned to modify its methodology to provide users with capabilities at a more rapid pace rather than delivering all capabilities at the end of a phase.

In that regard, Lockheed Martin (LM), with PMO participation, has been developing the strategic plan which will implement an incremental development and delivery schedule. This plan is scheduled to be finalized and delivered to the FBI on August 31, 2007.

Recommendation #2: Negotiate decreases in the cost of future phases if requirements are deferred in that phase.

FBI Response: Agree. The SENTINEL PMO is currently awaiting an Engineering Change Proposal, due on August 31, 2007. At that time, the costs for Phases 2-4 will be presented, discussed and, if necessary, negotiated with LM.

Finding 2: Phase 2 Planning and Management Issues:

Recommendation #3: Collect and report EVM data for both the performance measurement baseline approved at the integrated baseline review as well as the revised performance measurement baseline.

FBI Response: Completed. On March 29, 2007, the FBI and LM agreed to report Earned Value Management (EVM) performance against both the original Integrated Baseline Review (IBR) and subsequent baseline revisions, if any. This agreement will be implemented as part of the new strategic plan for Phases 2- 4.

Recommendation #4: Reconcile the discrepancy between the costs Lockheed Martin reported for Phase 1 with Lockheed Martin's EVM data, and develop and implement policies and procedures to prevent any future discrepancies.

FBI Response: Agree. On June 14, 2007, the PMO "stood down" EVM reporting and has not accepted any LM invoices pending LM's disclosure of the reasons for cost discrepancies and an acceptable action plan to prevent further occurrence. On August 7, 2007, LM disclosed the reasons causing the discrepancies and proposed an action plan. The PMO is currently evaluating those reasons and the action plan.

Recommendation #5: Develop and implement effectiveness measures for all risk mitigation plans.

FBI Response: Agree. SENTINEL is considering methods on how the effectiveness of the mitigation strategy would be measured.

Recommendation #6: Ensure that personnel assigned to manage SENTINEL risks devote sufficient time to the risk and have the experience and authority to adequately manage the risk.

FBI Response: Agree. Each SENTINEL risk is assigned to a Risk Working Group in which experienced personnel with diverse qualifications have sufficient time and authority to adequately manage the risk. The dedicated Risk Coordinator maintains risks and action item status in the Risk Register.

Recommendation #7: Document and track project issues, risks that have occurred, as well as the plan to resolve those issues and their ultimate resolution.

FBI Response: Agree. The PMO agrees to track and report on issues (including realized risks) that have a material impact on the program. Material impact will be defined as any issue that has a "Medium" or higher impact (cost, schedule, technical, or business impact) as specified in the FBI Risk Management guidance documents and the SENTINEL Risk Management Plan.

REDACTED FOR PUBLIC RELEASE

Recommendation #8: Implement policies and procedures to ensure that any changes to the Bill of Materials receive proper authorization and that the changes can be reconciled to the Bill of Materials submitted in Lockheed Martin's proposal.

FBI Response: Agree. The PMO has developed an updated Bill of Materials Deviation Policy and Procedure to ensure any changes are fully vetted by appropriate LM and PMO review boards prior to approval. As proposed, changes to the Bill of Materials will pass through appropriate decision boards including the Configuration and Change Management Board (CCMB) of LM Financial, the PMO CCMB, the PMO's Business Management Unit (BMU) and internal Finance Division boards. That document is currently in the review and approval process.

Recommendation #9: Implement policies and procedures to ensure that materials contained in Lockheed Martin invoices can be reconciled to the bill of materials or an FBI approval for a change to the bill of materials.

FBI Response: Agree. As of June 2007, the PMO's BMU now requires LM Financial to map their invoices to the Bill of Materials. LM was required to implement this new procedure prior to the acceptance of any invoices by the PMO.

APPENDIX 10

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

Pursuant to the OIG's standard audit process, the OIG provided a draft of this audit report to the FBI on August 6, 2007, for its review and comment. The FBI's August 22, 2007, response is included as Appendix 9 of this final report. The FBI concurred with the nine recommendations in the audit report. Our analysis of the FBI's response to the nine 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.** This recommendation is resolved based on the FBI's statement that it plans to modify its methodology to provide users with capabilities at a more rapid pace rather than delivering all the capabilities at the end of a phase. Further, Lockheed Martin, with PMO participation, is developing a strategic plan to implement an incremental development and delivery schedule, due on August 31, 2007. This recommendation can be closed when we receive documentation that the FBI has revised its four-phase approach for developing Sentinel to limit the scope of future phases to allow them to be completed in 9 months or less.
2. **Resolved.** In response to this recommendation, the FBI stated that the Sentinel PMO is currently awaiting an Engineering Change Proposal, due on August 31, 2007. At that time, the costs for Phases 2-4 will be negotiated, if necessary, with Lockheed Martin. This recommendation was based on our concern that when requirements are deferred from a phase, cost adjustments should be made to that phase accordingly. This recommendation can be closed when the FBI provides documentation of a policy requiring negotiations to reduce the cost of future phases if requirements are deferred from one phase to a later phase. We will continue to monitor the FBI's implementation of this recommendation over future project phases.

REDACTED FOR PUBLIC RELEASE

3. **Resolved.** This recommendation is resolved based on the FBI's stated agreement with Lockheed Martin to report EVM performance against both the original integrated baseline review and subsequent baseline revisions, if any. Additionally, this agreement will be implemented as part of the new plan for Phases 2-4. This recommendation can be closed when we receive documentation that EVM data is being collected and reported for both the performance measurement baseline approved at the integrated baseline review as well as the revised performance measurement baseline.
4. **Resolved.** The FBI agrees with this recommendation and stated that the Sentinel PMO "stood down" EVM reporting on June 14, 2007, and has not accepted any Lockheed Martin invoices pending disclosure of the reasons for cost discrepancies and an acceptable action plan to prevent further occurrence. The FBI also stated that on August 7, 2007, Lockheed Martin disclosed the reasons causing the discrepancies and proposed an action plan. The FBI is currently evaluating those reasons and the action plan. This recommendation can be closed when the FBI provides documentation reconciling the discrepancies between the costs Lockheed Martin reported for Phase 1 with Lockheed Martin's EVM data and also provides documentation that policies and procedures have been implemented to prevent any future discrepancies.
5. **Resolved.** This recommendation is resolved based on the FBI's statement that it is considering methods on how the effectiveness of the mitigation strategy would be measured. This recommendation can be closed when the FBI provides documentation demonstrating the implementation of effectiveness measures for all risk mitigation plans.
6. **Resolved.** The FBI agrees with this recommendation and stated that each Sentinel risk is assigned to a Risk Working Group in which experienced personnel with diverse qualifications have sufficient time and authority to adequately manage the risk. Additionally, the dedicated Risk Coordinator maintains risks and action item status in the Risk Register. This recommendation can be closed when we receive documentation demonstrating that the personnel assigned to manage risks devote sufficient time to the risks and have the experience and authority to adequately manage the risks.
7. **Resolved.** In response to this recommendation, the FBI stated that the PMO agrees to track and report on issues that have a

REDACTED FOR PUBLIC RELEASE

material impact on the Sentinel program (i.e., any issue that has a "medium" or higher impact as specified in the FBI Risk Management guidance documents and the Sentinel Risk Management Plan). This recommendation can be closed when we receive documentation demonstrating that project issues are being documented and tracked as well as the plans to resolve those issues and their ultimate resolution.

8. **Resolved.** In response to this recommendation, FBI stated that the PMO has developed an updated Bill of Materials Deviation Policy and Procedure to ensure any changes are fully vetted by appropriate Lockheed Martin and PMO review boards prior to approval. This policy is currently in the review and approval process. This recommendation can be closed when we receive documentation demonstrating that procedures are in place to ensure that any changes to the Bill of Materials receive proper authorization and that the changes can be reconciled to the Bill of Materials submitted in Lockheed Martin's proposal.
9. **Resolved.** The FBI agrees with this recommendation and stated that as of June 2007, the PMO has required Lockheed Martin to map its invoices to the Bill of Materials. Additionally, Lockheed Martin was required to implement this new procedure prior to the acceptance of any invoices by the PMO. This recommendation can be closed when we receive documentation demonstrating that the FBI has implemented policies and procedures to ensure that materials contained in the Lockheed Martin invoices can be reconciled to the Bill of Materials or an FBI approval for a change to the Bill of Materials.