SENTINEL AUDIT IV: 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 09-05
December 2008

REDACTED – FOR PUBLIC RELEASE

SENTINEL AUDIT IV: 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 Sentinel, its new information and case management system. The cost of Lockheed Martin's contract, broken down into four phases, 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), which placed the total estimated cost of Sentinel at $425 million. The initial schedule for the Lockheed Martin contract called for the project to be completed in December 2009.

In June 2007, the FBI announced that it had fully deployed Phase 1 of Sentinel, providing FBI employees with user-friendly, web-based access to information currently in the FBI's Automated Case Support system (ACS) as well as improved search capabilities. Phase 1 of Sentinel also features a personal workbox, which summarizes a user's cases and leads, and a squad workbox, which helps supervisors manage resources.[1]

The Sentinel program integrates commercial off-the-shelf (COTS) components and is intended to eventually 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 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.

---

* The full version of this report includes information that the FBI considered to be law enforcement sensitive or proprietary and confidential in nature, and therefore could not be publicly released. To create this public version of the report, the OIG redacted the portions of the full report that the FBI considered sensitive, and indicated where those redactions were made.

[1] A lead is a request from an FBI field office or a headquarters division for assistance in an investigation.

Sentinel will support our current priorities, including our number one priority: preventing terrorist attacks."[2]

Audit Approach

The Department of Justice 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 fourth in a series of audits that the OIG has conducted to evaluate Sentinel's progress and implementation.

In our third audit, *Sentinel Audit III: Status of the Federal Bureau of Investigation's Case Management System* (Sentinel III), we reported that Phase 1 of Sentinel was completed in June 2007, 2 months later than scheduled. We attributed the brief delay to four factors: unrealistic scheduling, Lockheed Martin's delays in fully staffing the project with experienced staff, difficulties in integrating COTS software components to work together as a system, and problems in assessing Sentinel's progress against the approved schedule. We determined that at the conclusion of Phase 1, the Sentinel project was generally within budget and Lockheed Martin had delivered two key project components: a web-based portal to ACS and personal and squad workboxes. However, the FBI had deferred one major deliverable – data cleansing of some ACS data for eventual migration to Sentinel. We recommended that the FBI continue to implement the "lessons learned" from Phase 1 and that the FBI consider modifying its four-phase approach to allow for more frequent updates to Sentinel. Finally, we noted that even though the FBI had completed Phase 1, the most difficult portions of Sentinel lay ahead.

The objectives of this current audit, the fourth in our ongoing reviews of Sentinel's progress, were to: (1) evaluate the FBI's planning for and implementation of Phase 2 of the Sentinel program, including cost and schedule performance; (2) determine if Phase 1 of the Sentinel program met technical and performance expectations; and (3) assess the FBI's progress in resolving concerns identified in the OIG's previous Sentinel audits.

---

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

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.[3]

We conducted our audit work at FBI headquarters in Washington, D.C., and at the FBI Sentinel PMO in McLean, Virginia. To perform our audit, we interviewed officials from the FBI, the Sentinel PMO, and the Department of Justice (Department). We reviewed documents related to the Sentinel contract; cost and budget documentation; and Sentinel plans, processes, and guidelines. Appendix I contains further description of our audit objectives, scope, and methodology.

OIG Audit Results in Brief

After completion of Phase 1 of Sentinel and before proceeding with Phase 2, the FBI directed Lockheed Martin to develop a strategic plan that would address the technical and managerial challenges encountered during Phase 1. The resulting strategic plan proposed dividing each of Sentinel's remaining phases into smaller segments, which would result in more frequent delivery of smaller or incremental portions of the overall product. The plan also proposed a realignment of the capabilities to be delivered in Phases 2 through 4.

The incremental development model divided Phase 2 into four segments. Segment 1, which was completed in April 2008, improved the Sentinel infrastructure, making it easier to install software upgrades and identify the cause of performance problems. These capabilities were originally part of Phase 1, but they were deferred to Phase 2 because of technical difficulties and schedule pressures, as well as the FBI's decision to delay the acquisition of certain software and licenses from Phase 1 to a timeframe closer to when they were actually going to be deployed in Sentinel's development.

Segment 1 also delivered the initial version of the enterprise portal, the central point for all FBI personnel to log onto the FBI's systems, which the FBI intends to enhance during future phases of Sentinel.

---

[3] This audit and the previous three OIG audits of Sentinel did not address Sentinel's property management controls because the Government Accountability Office (GAO) has published a series of reviews examining that issue. A list of other OIG audits and GAO reports appears in the Prior Reports section of the body of this report.

In addition to the changes in the development approach and schedule suggested by Lockheed Martin, the FBI reduced the number of information technology (IT) systems that Sentinel will interface with or replace.

As a result of these changes and the strategic planning effort, at the time of our audit the total estimated cost of Sentinel had increased from $425 million to $451 million and the completion date for Phase 4 had been extended from December 2009 to June 2010.

Sentinel's Earned Value Management (EVM) practices, which measure project performance, have changed substantially as a result of the new incremental development model. However, we found that Sentinel's EVM System Description, which governs Sentinel's EVM implementation, had not been updated to reflect the changes.[4] As a result, we could not determine whether Phase 2 was on schedule and within budget or whether Sentinel's EVM implementation met Office of Management and Budget (OMB) requirements. At the time of our audit, the FBI said its EVM data indicated that Phase 2 was on schedule and within budget, overall.

Additionally, we are concerned about the FBI's limited planning for streamlining the FBI's business processes to coincide with implementation of Sentinel. While Sentinel offers the FBI an opportunity to make its business processes, such as the collection of performance statistics more efficient, we found limited planning completed by the FBI in this area. As a result, the FBI needs to make several important decisions about the scope and functionality of Sentinel, such as Sentinel's role in automating records management.

Since deployment of Phase 1 in June 2007, the FBI has collected data on the number and demographics of Sentinel users.[5] According to that data, June 2007, the month Phase 1 was released, had the greatest number of users at 10,319. The number of users has declined every month from June 2007 through December 2007 but increased in January and February of

---

[4] 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. Periodic measurement of these variances gives project managers a timely perspective on a project's status. Please see page xii for a more detailed discussion of EVM.

[5] The Sentinel PMO measures Sentinel usage by the number of unique users who log into Sentinel at least once a month. FBI officials said that the PMO also measures weekly usage by the average number of unique daily users per week. These statistics are broken out by user type (supervisor or non-supervisor) for each field office and headquarters division.

2008. Over the same period the number of ACS users was relatively constant. A Sentinel Deputy Program Manager said the number of Sentinel users in June 2007 was artificially inflated because users, even those who do not normally use ACS, were curious to try Sentinel. FBI officials said that an additional reason for the high figure in June usage was that many FBI divisions mandated that all employees attend Sentinel training. Trainers were sent to all 56 field offices and headquarters over a 3-week period to conduct training just prior to the June deployment.

Sentinel PMO officials attributed the declining number of Sentinel users to the limited functionality of Phase 1, given that many users still need to use ACS to complete functions that are not currently available in Sentinel.

In addition to collecting user data, the FBI also established performance measures to measure the technical performance of Sentinel, such as the percentage of time that Sentinel was functioning and available for use by FBI employees. We found that most of these metrics were applicable to measuring Sentinel's performance at the end of Phase 4 and, in our judgment, few of the performance measures were useful to evaluate the value and satisfaction with Phase 1 deliverables. Because the FBI had not developed specific performance measures for Phase 1, it could not determine whether Phase 1 was meeting its phase-specific expectations.

Our previous three Sentinel audits included a total of 21 recommendations to help improve the FBI's management of Sentinel. During this audit, we concluded that the FBI has, in general, taken action to address the concerns expressed in our prior reports. Specifically, the FBI has made significant progress in staffing the Sentinel PMO and the Sentinel PMO has established improved controls to ensure that all changes to the Bill of Materials (BOM) received the required approval.[6] However, we could not determine what progress the FBI had made to one of the recommendations in our last report regarding the need to develop contingency plans and contingency triggers for highly rated risks because, at the time of our audit, the FBI was tracking only three risks and none of them were rated high enough to require a contingency plan or trigger. Because Sentinel is vital to the FBI's mission and because the requirements are very complex, we are concerned that the PMO has not identified any high risks that require a contingency plan or trigger. We believe the FBI could improve its risk

[6] A 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.

criterion and its categorization of risks, which would enhance the FBI's overall risk management as well as its contingency preparedness.

In this report, we make 10 additional recommendations to assist the FBI ensure the success of the Sentinel case management system and better manage project costs. Our report also contains detailed information on the results of our review of Sentinel's development and implementation. The remaining sections of this Executive Summary describe in more detail our audit findings.

Background

The Sentinel program 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 IT modernization project. The Virtual Case File was originally 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.[7] The cost of the original task order for Phase 1 of Sentinel was $57 million. According to the original 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. 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 three 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.

The FBI's initial plan called for implementing Sentinel's four phases over 45 months, with each phase providing distinct capabilities until the project was fully functional in December 2009. Originally, the FBI expected to complete each of the phases in 12 to 16 months. As discussed later in

[7] 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.

this report, however, the FBI modified the original four-phase approach based on its experience with the first phase, which experienced cost and schedule challenges. According to the revised schedule, the FBI expects to complete each of the remaining phases in 8 to 17 months.

Phase 1 introduced the Sentinel web-based portal, which provided access to data from the existing ACS system. Phase 1 also provided a case management workbox 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. Eventually, through incremental changes in subsequent phases, the portal will display data from a newly created investigative case management system.

Planning for Phases 2 through 4

After the FBI accepted delivery of Phase 1 of Sentinel, the FBI directed Lockheed Martin to develop a strategic plan to address the challenges encountered during Phase 1 development so that the lessons learned could be utilized when developing the remaining phases of the project. As part of the strategic planning process, the FBI and Lockheed Martin reexamined the remaining Sentinel system requirements, including the IT systems with which Sentinel would interface or replace. The strategic plan and its accompanying engineering change proposal (ECP) called for: (1) an incremental system development methodology, (2) a $30 million increase in cost, (3) a reconfiguration of the content and capabilities of the remaining phases, and (4) a 6-month extension in the amount of time required to complete the entire project.[8] In addition, the FBI added requirements for an enterprise portal.[9]

As of April 2007, the FBI had identified 43 IT systems that currently interface with ACS or had requested to interface with Sentinel. The original Sentinel requirements, released in July 2005, called for Sentinel to interface with only 35 other FBI systems. FBI officials reviewed the business needs of each of the interfaces and deleted some and added others. As of March 2008, the FBI decided that Sentinel would interface with 25 other FBI IT systems. The reduction in the number of interfaces was reflected in the

[8] An engineering change proposal (ECP) is the management tool used to propose changes to baselined performance requirements and baselined documentation describing different aspects of the computer system being developed.

[9] The Sentinel Enterprise Portal will allow users to access multiple FBI IT systems with a single sign-on. The portal will also provide a central location for links to other FBI applications.

estimated costs for Phases 2 through 4 in an ECP submitted by Lockheed Martin. The Sentinel PMO also reduced the number of systems that Sentinel will subsume or replace, a change that is also reflected in Lockheed Martin's ECP. In July 2005, the FBI planned for Sentinel to replace ACS and nine other IT systems. While Sentinel will continue to replace ACS, in January 2008 the FBI reduced to three the number of other systems that Sentinel will replace.

Revised Sentinel Capabilities

Lockheed Martin's ECP realigned the capabilities to be delivered in Phases 2 through 4 of the project. FBI officials stated that the revised plan for delivering Sentinel's capabilities was an improvement for several reasons. First, by not migrating data from each of ACS's three components in different phases of Sentinel, the new plan should eliminate some of the risk associated with data migration. In Phase 2, the new strategic plan calls for migrating data from a subset of the information contained in ACS – administrative electronic files – and then applying new workflows to this subset of cases. This will allow Lockheed Martin and the FBI to gain experience in migrating data from ACS to Sentinel before making a major transfer of data between the two systems. Also, by applying new workflows only to a small subset of FBI cases, the FBI will have the opportunity to refine its new workflows before adopting them for all FBI cases. In addition, the ECP increased the requirements satisfied by Phase 2, moving more risk to Phase 2 and alleviating some of the FBI's risk for Phases 3 and 4.

New System Development Methodology

After completion of Phase 1 of Sentinel, the Sentinel PMO and Lockheed Martin adopted an incremental development model for Phases 2 through 4. The FBI's Life Cycle Management Directive, version 3.0, describes the Incremental Model as one in which development occurs in an overlapping and iterative manner resulting in the delivery of portions, or increments, of the overall product. Under this model, future increments build on the capability of the increments already delivered.

Lockheed Martin's approach to the Incremental Model divides each phase of Sentinel into segments and then divides each segment into increments. For example, Lockheed Martin broke Phase 2 into four segments, the first of which has four increments. Each successive segment builds on the work completed in prior segments, but work on multiple segments may occur simultaneously. Similarly, work on two or more increments within a segment may occur concurrently.

One of the driving factors in the switch to the incremental development model was the FBI Chief Information Officer's (CIO) desire to deliver new capabilities to users approximately every 3-6 months. By comparison, in Phase 1 it took more than a year before the FBI delivered new capabilities to users. Under the Incremental Model, most increments

will enhance user capabilities while some will only provide infrastructure improvements that will not be apparent to users.

Revised Schedule and Costs

As a result of the time used for strategic planning following Phase 1, the reallocation of the remaining requirements, and the addition of requirements for an enterprise portal, Lockheed Martin and the FBI revised the schedule and cost estimates for the remaining phases of Sentinel. The revised schedule calls for Phase 4 to be completed in June 2010, 6 months later than originally planned. Based on the cost estimate contained in the Lockheed Martin ECP approved by the FBI in January 2008, the FBI expects Sentinel to cost a total of $451 million, approximately $26 million more than the $425 million originally planned. The value of the FBI's contract with Lockheed Martin, including all options, has increased from about $305 million to $335 million.

According to the Sentinel Program Manager, the level of risk for completing Phases 2 through 4 on time and within budget is the same for each phase and the risk reserve for the three phases is equal in percentage terms. The Sentinel Program Manager said the management reserve for each fiscal year is 11 percent of the total development, Sentinel PMO, and independent verification and validation (IV&V) costs of the project. However, he said that the adoption of the incremental development model led the Sentinel PMO to change how the risk reserve for the project is maintained.[10] The risk reserve is now based on the fiscal year rather than on which phase of the project is being completed. Both the amount of the management reserve and the PMO's maintenance of the reserve appear reasonable.

[10] A risk reserve, which is also referred to as a management reserve, is a budgeted amount to cover any unanticipated expenses.

FBI's Business Process Reengineering Effort Incorporated into Sentinel

In our judgment, to maximize the return on its investment in Sentinel, the FBI cannot merely automate its current business processes. Instead, it should take advantage of Sentinel's potential capabilities to streamline and reinvent its processes. The FBI has recognized this need and, in April 2005, launched a business process reengineering (BPR) effort. In Phase 2 of Sentinel, the FBI incorporated its BPR efforts into Sentinel, and the program is currently focusing on two major BPR efforts: (1) reducing the number of forms used in the FBI (known as "FD" forms); and (2) streamlining how the FBI collects data to demonstrate the progress it has made in addressing its strategic goals.[11]

In addition to reducing the number of FD forms, Sentinel BPR efforts are also addressing how the FBI collects metrics on its activities – a significant undertaking because agents demonstrate the progress they have made on cases or tasks assigned to them by entering data on FD forms. An FBI official stated that the most important inputs to Sentinel are data and the most important outputs are statistics. The goal of this effort is to ensure that the FBI collects all the required statistics, but that it does not collect the same piece of data twice.

The FBI expects Sentinel to transform the way it does business by allowing the FBI to move from a primarily paper-based case management system to an electronic system of records. In the current environment, all paper documents in a case file are considered to be records. Once Sentinel is fully implemented, most documents will be digitally signed and only exist in electronic form, making the electronic documents records that Sentinel's Records Management Application (RMA) will maintain as part of the official FBI case file.[12]

The FBI's enterprise-wide RMA must be able to handle all types of FBI records. However, the current focus of Sentinel's records management includes only investigative case records. Once completed, Sentinel will have much of the infrastructure to become the FBI's enterprise-wide RMA, but the FBI has not decided whether Sentinel will be the FBI's RMA or whether the

---

[11] Forms eligible for use throughout the FBI are defined by a form number that begins with "FD."

[12] An RMA is a software application that automates records management functions and manages electronic records through their life cycle.

Records Management Division will maintain a separate RMA for various non-investigative case records. If the FBI decides that Sentinel should become the FBI's enterprise RMA, more resources may be required to add additional capacity to Sentinel and to upgrade FBI hardware. Given that one of the FBI's strategic objectives is to automate its record management system, it must make a strategic decision soon about whether Sentinel will be the FBI's enterprise records management system or whether it will build a separate records management system.

Phase 2 Status

In April 2008, the FBI accepted from Lockheed Martin delivery of Phase 2, Segment 1. The four increments of Segment 1 delivered the initial version of the FBI enterprise portal, which will become the single point of entry for all FBINET users.[13] The increment deliverables also included capabilities that were originally scheduled for Phase 1, including patch management abilities for the underlying operating systems, improved software inventory reporting, and enhanced internal monitoring capabilities that should be useful in identifying system faults and degraded performance conditions. The segment also included testing and verification of the data migration program (see Appendix XV for a description of Phase 2, Segment 1 capabilities).

Funding

According to a senior FBI Finance Division official, fiscal year (FY) 2008 appropriations for Sentinel were $45 million less than required. The FBI had anticipated a $100 million recurrence (funding from the previous year's budget included in the base budget of the following fiscal year) for Sentinel, but received only $55 million. The FBI funded the remainder of its FY 2008 Sentinel costs with no-year funds carried over from prior year FBI appropriations and reimbursable funds from the Department of Justice Working Capital Fund.

The 2008 Consolidated Appropriations Act restricted the obligation or expenditure of funds for Sentinel until the Deputy Attorney General and the Department's Investment Review Board (DIRB) certified to the U.S. House and Senate Committees on Appropriations that Sentinel has appropriate program management and contractor oversight mechanisms in place and that Sentinel is compatible with the Department's enterprise architecture.

[13] FBINET is the FBI's centralized network management system, which provides access to various FBI administrative, financial, and investigative systems.

In January 2008, the DIRB granted Sentinel provisional certification, which allowed the FBI to obligate and expend funds only for the development of Segments 1 and 2 of Sentinel's second phase. At the time the DIRB granted Sentinel its provisional certification, one recommended item remained open – the delivery of a Full Operating Capability (FOC) Architecture and Design Document. In June 2008, the DIRB certified that Sentinel met the provisions of the Consolidated Appropriations Act of 2008, subject to 10 qualifications, including that Sentinel use the "to-be-completed FOC architecture to help generate new cost and schedule estimates for all future program work."

Earned Value Management

The EVM process helps manage project risks by producing reliable cost estimates, evaluating progress, and allowing the analysis of project cost and schedule performance trends. EVM compares the current cost and schedule status of a project to the established cost and schedule baselines. For any project using EVM, OMB requires an Integrated Baseline Review (IBR) to establish a performance management baseline (PMB) against which a project's performance can be measured.[14]

Under the incremental development approach, the FBI treats each segment as a separate project. Thus, a separate performance measurement baseline is required for each segment's scope of work and budget to ensure consistency between the two items. In lieu of an IBR for each segment, the Sentinel PMO conducts a Budget Baseline Review to validate segment cost, schedule, and scope. However, Sentinel's EVM System Description, which describes how EVM should be implemented for Sentinel and how that implementation will meet American National Standards Institute/Electronic Industries Alliance Standard 748-A (ANSI/EIA 748-A), has not been updated to reflect Sentinel's new approach to EVM.[15]

The Sentinel PMO reports the program's EVM data on a monthly basis, with reports issued about 1 month after the period covered. The EVM report for February 2008 indicated that Sentinel was under budget but behind schedule. In April 2008, the Sentinel Program Manager provided us with his current assessment of the project and explained that Segment 1 was

---

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

[15] We refer to this standard as ANSI/EIA 748-A, which is the criteria selected by the OMB for EVM systems.

completed on time and within budget. However, he also said Segment 2 had experienced some problems and that one increment was approximately 4 weeks behind schedule. According to the Sentinel Program Manager, the EVM results mirrored his assessment of the challenges in Sentinel's development.

On October 12, 2007, the Sentinel PMO granted Lockheed Martin authorization to proceed with Segment 1 development during the period from October 15, 2007, to April 15, 2008. The Sentinel Statement of Work (SOW) had to be revised due to the change to an incremental development approach, the addition of the enterprise portal, changes to the systems interfacing with Sentinel, and changes to the systems that Sentinel will subsume.

The original and revised SOWs contained requirements for EVM. However, the EVM requirements contained in the revised SOW are not consistent.

Phase 1 System Usage, Performance and Security

Since the deployment of Phase 1 in June 2007, the FBI and Lockheed Martin have evaluated the performance of Phase 1 by collecting input from Sentinel users and analyzing the technical performance of the system, such as the percentage of time Sentinel is available to users. In response to these evaluations, from June 2007 through February 2008, the FBI deployed 12 updates to Sentinel.

Phase 1 User Acceptance

Since deployment of Phase 1, the FBI has collected data on the number of Sentinel users as well as the demographics of those users. Sentinel user statistics showed that between June 2007 and February 2008 Sentinel usage decreased by 25 percent. In addition, the statistics showed variances in Sentinel usage across the FBI. To further understand the user data, the FBI solicited feedback from focus groups at field offices and conducted a Sentinel User's Conference in November 2007.

Sentinel user representatives at the focus groups and the Conference stated that the technical aspects of Sentinel affected overall usage, such as Sentinel's current functionality and design and the FBI's network. For example, they said that some actions, such as sending a lead to a large group of people, were easier to perform in ACS than in Sentinel. Users also

said that the current FBI network does not provide adequate bandwidth to smaller FBI offices, increasing network log in times to as much as 30 minutes when using Sentinel. The Sentinel user representatives also stated that some FBI employees, such as Support Services Technicians, require functionality that is currently only available in ACS, such as opening and closing cases. Once these users login into ACS, they see little benefit in logging into Sentinel to perform a subset of their work. In addition, Sentinel users at the conference also voiced concerns about the accuracy of Sentinel's search results.

The conference participants said that leadership from senior FBI management was critical to increasing Sentinel usage and ensuring Sentinel's overall success. They said executive level communication and support is a very effective way for the user community to understand FBI priorities and how Sentinel supports those priorities. Conference participants also said that Special Agent in Charge (SAC) support for Sentinel was inconsistent across field offices.

The Sentinel PMO and Lockheed Martin jointly conducted focus groups called Operational Impact Assessments at FBI field offices. The purpose of these assessments was to measure, evaluate, and report the potential effect of scheduled enhancements to Sentinel – both positive and negative – on Sentinel users. Each assessment included FBI personnel from various job functions. The following is a list of significant issues recorded during the three assessments we reviewed.

- Some functionalities, such as opening cases and setting leads, only exist in ACS and many ACS functions are not yet available in Sentinel.
- Many users are proficient in using ACS and are not familiar with using Sentinel, and ACS remains available.
- Some users do not want to invest time in learning and using Sentinel until it is complete.
- Sentinel takes too long to respond user queries for information.
- Users do not like switching back and forth between ACS and Sentinel to do their job.

Operations and Maintenance

When the FBI accepted delivery of Phase 1 of Sentinel, it entered the Operations and Maintenance (O&M) phase of the IT life cycle.[16] For May 2007 through September 2008, the FBI allocated $10.1 million for Phase 1 O&M activities. O&M activities include attending to any minor problems existing with Phase 1 upon deployment, user requests for improvements, the day-to-day maintenance of the system, and the detection and correction of system abnormalities. To address these issues, Lockheed Martin created Phase 1 updates, called "builds." From the time Phase 1 was deployed in June 2007 through February 2008, the FBI authorized 12 builds of Sentinel.

From a user perspective, Build 10, which added the Sentinel Web Application, may have been the most significant Sentinel update. According to Sentinel PMO officials, Build 10 addressed several user interface issues concerning the presentation of data that users identified during Phase 1 user acceptance testing or in early deployment feedback. The Sentinel Web Application also changed the underlying technology used to deliver data to users. Sentinel PMO officials stated that this change was implemented to reduce the amount of system maintenance needed and to improve user response times for searches.

Defect Reports, documentation of problems discovered during the development or testing of a new build, are the primary source for the changes included in each of the Sentinel builds. The Sentinel PMO also creates enhancement Defect Reports, which add capability deemed necessary by FBI users but were not included in Phase 1 as a deliverable. All Defect Reports receive a priority rating of one through four depending on the severity of the defect, with priority one defects requiring immediate attention. The 12 O&M builds of Phase 1 addressed a total of 456 Defect Reports, with 50 of these reports receiving the two highest priority levels.[17] Eighty-Nine percent of these Defect Reports received the lowest priority levels, indicating that the vast majority of the reports did not require immediate attention.

---

[16] The IT system life cycle includes the following components: planning, acquisition, development, testing, and operations and maintenance. See page 78 for a more detailed discussion.

[17] See Appendix IX for a definition of the four DR priority levels.

Technical Performance

To help ensure that Sentinel meets the contractual requirements of the program and that deliverables meet functional requirements, the FBI established performance measures and documented them in the Sentinel Measurement Plan. The plan defined the performance data to be collected, including seven Critical Performance Measures (CPM) and five O&M data elements.[18] The seven CPM data elements required by the Measurement Plan address technical aspects of Sentinel's performance such as the percentage of time the system is available to FBI users.

The Sentinel Measurement Plan requires Lockheed Martin to submit an evaluation of Sentinel metrics in a monthly Measurement and Defect Report. Lockheed Martin distributes this report to the Sentinel PMO and other FBI offices overseeing the performance of Sentinel. However, from June 2007 through February 2008 Lockheed Martin produced only four of the required nine Measurement and Defect Reports. According to a Sentinel PMO official, Lockheed Martin did not submit measurement reports from June 2007 through October 2007 because Lockheed Martin and the FBI could not agree on the metrics to be collected.

We reviewed the CPM and O&M metrics in the four reports Lockheed Martin submitted to determine whether Sentinel system performance was meeting technical expectations. In at least one of the four reports we reviewed, Sentinel did not meet four of the seven CPMs. A Sentinel PMO official stated that the CPMs reflect Sentinel's intended capability at the end of Phase 4, referred to as full operating capability (FOC), and the FBI did not expect Phase 1 to always meet the FOC thresholds. He stated that the objective is for Sentinel to show progress in meeting its FOC CPM thresholds as Sentinel progresses through the remaining phases. In our judgment, the seven CPMs are not useful for monitoring Sentinel's performance until Sentinel's completion, but the PMO has not established interim CPMs such as the measures used during Phase 1 testing to monitor the performance of Phase 1. We believe the FBI should develop interim measures to assess whether the current version of Sentinel meets technical expectations.

Also, in at least one of the four measurement reports we reviewed Sentinel did not meet the threshold for two out of five O&M performance

---

[18] CPM data elements are used to track system performance during development to gauge whether the specific program elements will be met once the system has been deployed. O&M data elements track system performance after the system has been deployed.

measures. We found that the PMO does not have a documented process for responding to measurement reports that indicate the system does not comply with all of the stated thresholds. An FBI official said that O&M metrics are just one of several indicators that may signal a potential performance problem and that the trend over several months may be a more important indicator of system performance.

Security Monitoring

A Plan of Action and Milestones (POA&M) is a management tool for correcting security weaknesses identified in an IT system. To ensure that POA&Ms contain the data necessary to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions, OMB issued guidance listing eight elements a POA&M should include for OMB-required reports. We found that the two POA&Ms vital to Sentinel's operation did not include the following four OMB required reporting elements: (1) estimated funding resources to resolve weaknesses, (2) key milestones with completion dates, (3) milestone changes, and (4) source of weakness.[19]

During our fieldwork, in February 2008 we discussed this issue with the FBI. In response to our findings, the FBI updated one of the two POA&Ms we reviewed to include: (1) estimated funding resources to resolve weaknesses and (2) milestone changes. The Sentinel Information System Security Manager said the FBI Accreditation Unit, which issues a template for all FBI POA&Ms, agreed to add the two elements to the template. In addition, he also said that the Sentinel Program Manager agreed to provide him with data on (1) estimated funding to resolve weaknesses, (2) key milestones with completion dates, and (3) milestone changes. However, even with these improvements Sentinel's POA&Ms do not fully comply with OMB guidance, and this may reduce the FBI's ability to manage Sentinel's security.

In addition to the missing reporting elements, we also found that both POA&Ms contained open findings with past due resolution. For one POA&M, 11 of the 20 open findings were past due by an average of 152 days. When POA&M findings are not addressed in a timely manner, the risk increases that Sentinel's sensitive data could be compromised. In response to our findings, the Information System Security Manager stated that Lockheed

[19] There are two Sentinel environments: (1) Herndon Secret Sentinel System (HS3), and (2) Sentinel Phase 1 (SP1). A POA&M is required for each environment.

Martin did not have a Security Engineering Team during Phase 1 to ensure that Lockheed Martin: (1) completed all of the security requirements scheduled for Phase 1, (2) performed Sentinel's system security verification, and (3) adhered to the schedule for correcting issues identified in the POA&Ms. To avoid a similar situation during Phase 2, Lockheed Martin has created and staffed a Security Engineering Team.

In addition to our concerns about the Sentinel POA&Ms, we also found that Lockheed Martin did not have a Security Administrator assigned to Sentinel. The Security Administrator is responsible for maintaining a daily checklist of activities specified in the Sentinel System O&M Manual and reporting any findings to the Operations Manager and Information System Security Officer. Because Lockheed Martin had not assigned a Security Administrator to Sentinel, the FBI's Information System Security Officer was performing the required monitoring tasks. However, in February 2008 Lockheed Martin hired a Security Administrator, and FBI personnel said that the Lockheed Martin Security Administrator would assume many of the system security monitoring duties being performed by the Information System Security Officer.

Actions Taken on Previous OIG Recommendations

The OIG's three previous reports on Sentinel contained 21 recommendations regarding the management of Sentinel. During this audit, we found that the FBI was, in general, taking action to resolve our recommendations from prior reports. As of June 2008, we closed 16 of our recommendations based on FBI corrective action. For example, we found that the FBI has made significant progress in staffing the Sentinel PMO and that the Sentinel PMO has implemented improved policies and procedures regarding changes to the Bill of Materials (BOM).

However, we could not determine what progress the FBI had made in addressing one of the recommendations in our last report regarding the need to develop contingency plans and contingency triggers for highly rated risks because, at the time of our audit, the FBI was tracking only three risks and none of them were rated high enough to require a contingency plan or trigger. We believe a change in the risk ranking criterion is the reason the Sentinel PMO was tracking so few open risks. According to Sentinel's revised Risk Management Plan, a risk will be tracked only if it will have a 10 percent or greater variance in the program's cost or schedule. Given that Sentinel is critical to the FBI's overall mission, we believe this variance threshold is too high. We also are concerned that a large number of

potential risks are not being actively managed as a result of the 10 percent threshold. In our judgment, improved risk criterion and categorization would enhance the Sentinel's overall risk management as well as its contingency preparedness.

Staffing

The Sentinel Program requires a highly skilled and integrated Sentinel PMO. The Sentinel Staffing Plan defines the staffing levels and skill needs of the Sentinel PMO. Due to the importance of the Sentinel PMO's oversight of Sentinel, we recommended in all three of our previous Sentinel audits that the Sentinel PMO complete hiring as soon as possible for the vacant Sentinel PMO positions. At the time of our audit, the Sentinel PMO had two vacancies – neither of which we consider critical - and was in the process of filling both positions.

Bill of Materials

In our August 2007 report, *Sentinel Audit III: Status of the Federal Bureau of Investigation's Case Management System,* we recommended that the FBI: (1) implement policies and procedures to ensure that all changes to the Bill of Materials (BOM) receive proper authorization and that the changes can be reconciled to the BOM submitted in Lockheed Martin's proposal, and (2) implement policies and procedures to ensure that materials contained in Lockheed Martin invoices can be reconciled to the BOM or an FBI approval for a change to the BOM.

During this audit, we found that the PMO has revised and strengthened its BOM Deviation Policy. Now all BOM changes, additions, and deletions must be documented and submitted by Lockheed Martin to the Contracting Officer's Technical Representative (COTR) using the Sentinel BOM Deviation Approval Submission Form. No changes can be made to the BOM until the form is received and approved by the COTR.[20] As an additional control, the Sentinel PMO matched material listed on Lockheed Martin's invoices to the approved BOM to verify that Lockheed Martin only purchased equipment for which it had authorization. We believe that the FBI has significantly

[20] Prior to delivery to the COTR, the BOM Deviation Approval Submission must be signed by representatives of Lockheed Martin's Engineering Review Board, Configuration Control Board, and finance office as well as representatives from the Sentinel PMO's Engineering Review Board, Configuration Control Board, and finance office. The COTR is the final approval official for all submissions.

improved its control over changes to the BOM and that these improved controls should provide the FBI with greater control over Sentinel's cost.

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 with the assistance of a Risk Review Board. 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.

Once the Risk Review Board Chair accepts a risk he assigns the risk to a Risk Owner, who is responsible for developing detailed mitigation plans, contingency plans and triggers, and assessments of the risk. In our August 2007 report, we expressed concern that the personnel assigned to manage risks may not have sufficient time or expertise to adequately develop and implement a strategy to reduce Sentinel risks. With the implementation of the revised Risk Management Plan, which utilizes risk owners and working groups, we believe that the FBI has taken meaningful steps to address our concern.

As of March 2008, the FBI identified and was managing only three open risks to the Sentinel program.

- If the Full Operating Capacity architecture does not contain a sufficient level of detail by the beginning of Phase 2, Segment 3, then Phase 2, Segment 3 development efforts may be adversely affected;

- The data migration complexity from phased-out legacy systems may have been underestimated, therefore some data may be lost, compromised, or the FBI may not be able to retire the ACS system if this issue cannot be resolved prior to starting Segment 4;

- Current deployment of FBI initiatives, including Enterprise Directory Service and Public Key Infrastructure on which Sentinel is dependent, do not support the revised roadmap.

The Sentinel Risk Management Plan, which was revised in November 2007, requires contingency plans and contingency triggers only for open

risks that have a risk exposure rating of "high" or "very high." The contingency plans must identify what actions will be taken when a specific trigger event occurs. Contingency triggers and plans are formulated by the risk owner and the related working group, and are recorded, reviewed, and revised by the Sentinel Risk Review Board, a board composed of Sentinel Project Management Office (PMO) officials who assess risks to Sentinel's cost, schedule, and performance. As of March 2008, the Board did not consider the three open risks as "high" or "very high", and therefore no contingency plans were required or developed for these risk areas.[21]

Conclusion and Recommendations

By clarifying Sentinel requirements, changing system development methodologies, and realigning the capabilities to be delivered in the remaining Phases 2 through 4, the FBI and Lockheed Martin have shown a significant willingness to incorporate lessons learned from the previous challenges encountered in developing Phase 1. In addition, the changes the FBI had made to Sentinel interfaces and its reassessment of the systems Sentinel will subsume also demonstrate a willingness to address shortcomings in the original Sentinel specifications.

Because of the strategic planning following Phase 1, the reallocation of the remaining requirements, and the addition of requirements for an enterprise portal, the FBI estimates that Phase 4 will be completed in June 2010, 6 months later than originally planned. As a result, the FBI now expects Sentinel to cost a total of $451 million, approximately $26 million more than the $425 million originally planned. The value of the FBI's contract with Lockheed Martin, including all options, has increased from about $305 million to $335 million.

By adopting an incremental development plan, the FBI divided Phase 2 into smaller segments that should deliver improved functionality to users more frequently. Each segment is now treated as a separate contract with separate deliveries. The FBI's Integrated Baseline Review for Phase 2 focused almost exclusively on Segment 1 of the phase, while the Full Operating Capability architecture for the project, which tells engineers what the final product they are building will be, has not been completed. The

[21] Contingency plans indicate the actions that should be performed when a specific "trigger" event occurs. A trigger is identified as a specific date, cost or schedule threshold, or pre-defined risk condition. Although it was not required, one risk had both a contingency trigger and a contingency plan.

PMO conducted the IBR for Phase 2, focusing on Segment 1 for which EVM, an integrated master schedule, and requirements data were tracked for cost, schedule, and performance. For each subsequent segment of Phase 2, the PMO conducted a Budget Baseline Assessment (BBA), the equivalent of a mini-IBR (containing cost, schedule, and performance requirements). The development work that was planned for Phase 2 may be pushed back into the operations and maintenance phase of the project or moved to a future phase. Sentinel's use of an EVM system that differs significantly from its EVM System Description increases our concern that the FBI may not be able to adequately monitor the progress of the project as a whole.

In Phase 2, for example, while the Sentinel PMO has spearheaded the elimination of hundreds of little-used forms, the FBI must still decide what data from approximately 350 forms will be entered into Sentinel and which forms will be replaced by Sentinel. In our judgment, these decisions are one of the primary tasks that the FBI needs to address in the immediate future. Similarly, we believe it is critical that the FBI use Sentinel as the driver for streamlining the way it records accomplishments, the number and type of statistics it collects, and how it collects statistics.

In addition, if the FBI completes Sentinel as currently envisioned, it will have the core of a new records management system in place. Given that one of the FBI's strategic objectives is to automate its records management system, it must make a strategic decision about whether it should build a new separate records management system or expand Sentinel's capabilities to allow Sentinel to become the FBI's enterprise records management system. The decisions the FBI makes concerning forms, statistics, and records management affect whether Sentinel simply automates the FBI's current work processes or whether it enhances the way the FBI conducts its work.

Since Phase 1 was deployed in June 2007, we found that the number of Sentinel users per month has decreased. We believe that this decrease is mainly due to Sentinel's current limited capabilities.

In addition, since June 2007 the FBI has authorized 12 new updated versions of Sentinel in response to issues found in previous versions of Sentinel. We believe that the processes necessary to provide timely and meaningful updates to Sentinel are in place at the Sentinel PMO and Lockheed Martin.

The OIG made 21 recommendations in our past 3 audits of the Sentinel program, and to date the FBI has addressed 16 of these 21 recommendations and agrees with the remaining 5 recommendations. In particular, the current audit examined the FBI's efforts to address recommendations in three specific areas: staffing the Sentinel PMO, controlling changes to the Bill of Materials, and managing risk.

With respect to the first issue, staffing in the Sentinel PMO has reached a level sufficient to close our recommendation. Similarly, the FBI has instituted new policies and procedures that, based on our testing, improved the FBI's control over changes to the Bill of Materials, giving the FBI better control over the cost of Sentinel. However, we could not determine whether the FBI had instituted our recommendation on contingency plans and contingency triggers for highly rated risks because none of the risks the FBI was tracking met the criteria requiring contingency plans or triggers. In our judgment, the revised Sentinel Risk Management Plan increases the threshold for what constitutes a highly ranked risk to the point where very few, if any, risks will need a contingency plan or trigger. Consequently, we believe the FBI should reevaluate its revised Risk Management Plan and lower the threshold for determining when a risk requires a contingency plan.

In this audit report, we made 10 additional recommendations to the FBI, including that the FBI identify the data that will be stored in Sentinel, the data collection process, and the FD forms Sentinel will replace. In addition, we recommend that the FBI decide what statistics will be stored in Sentinel and how those statistics will be collected. To provide a clearer roadmap of where the Sentinel project is headed, we also recommend that the FBI complete the FOC architecture and update Sentinel's EVM System Description.

INTRODUCTION

On March 16, 2006, the Federal Bureau of Investigation (FBI) announced that it had awarded a contract to Lockheed Martin Services, Incorporated (Lockheed Martin) to develop the Sentinel information and investigative case management system. 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 user-friendly, web-based access to information currently in the FBI's antiquated Automated Case Support system (ACS).[22] Phase 1 featured a personal workbox that summarizes a user's cases and leads.[23] It also provided 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 awarded up to an 11 percent award fee of the total development costs for meeting established goals in four areas: project management, cost management, schedule, and technical performance. The award fee will be allocated across the four areas based on risk. This type of contract and award fee structure is common for large government information technology (IT) projects.

The Sentinel project, which uses commercial-off-the-shelf (COTS) components, is intended to provide the FBI with a web-enabled electronic case management system that includes records management, workflow management, evidence management, search and reporting capabilities, and information sharing capabilities with other law enforcement agencies and the intelligence community. According to the FBI Director, "Sentinel will

---

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

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

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."[24]

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. 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 is the fourth OIG report on Sentinel. The previous three reports focused on the planning and development for Phase 1 of Sentinel, the FBI's processes and controls for managing information technology (IT) projects, and the contract with Lockheed Martin to develop Sentinel. This report examines the changes made to Sentinel's planning and development since completion of Phase 1, and the progress made by the FBI in resolving concerns identified in our previous audits.

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.[25]

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

---

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

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

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 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 the Aerospace Corporation (Aerospace) 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.[26] The IV&V report 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 Operating Capability and Full Operating Capability segments. The Initial Operating Capability segment assessed the

---

[26] 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.

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.[27]

The FBI issued a final report on the Initial Operating Capability at the end of April 2005.[28] 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 adapt to evolving investigative and intelligence business requirements over time. 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. 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

---

[27] U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project,* Audit Report 05-07 (February 2005).

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

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, 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.

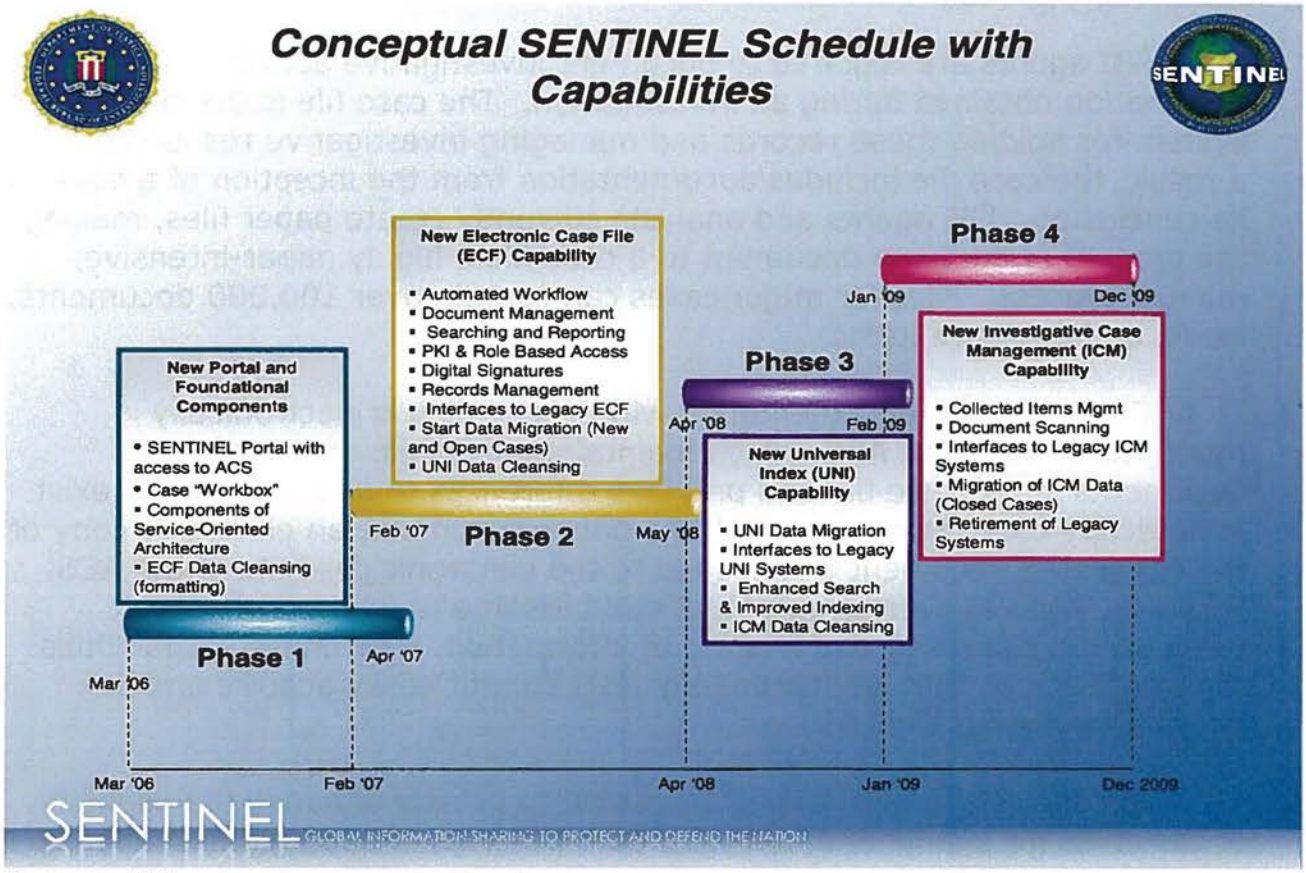
Currently, the documentation within case files is electronically managed through the ACS, which maintains electronic copies of most documents in the case file and provides references to documents that exist in hardcopy only. Upon approval of a paper document, an electronic copy of the completed document is uploaded to the electronic case file of the ACS. However, ACS is severely outdated, cumbersome to use, 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 program in four partially overlapping phases, each lasting approximately 12 to 16 months. 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 program. The following figure shows the FBI's original conception of the four phases and their general timeframes.

FIGURE A: CONCEPTUAL SENTINEL SCHEDULE WITH CAPABILITIES



Source: FBI

Phase 1 was to introduce the Sentinel web-based portal, which would provide access to data from the existing ACS. Eventually, through incremental changes in subsequent phases, the portal was intended to display data from a newly created investigative case management system. Phase 1 also was intended to provide a case management workbox 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.

Phase 2, the most ambitious and technically difficult of the phases, was to begin the transition to paperless case records and the implementation of electronic records management. A workflow tool would support the flow of electronic documents through the review and approval cycles, and a new security framework was to be implemented to support access controls and electronic signatures. Additionally, in Phase 2, the FBI planned to 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 was to 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 was to expand the number of attributes within the information management system allowing more precise and comprehensive searching within Sentinel and increasing the FBI's ability to "connect the dots."[29]

Phase 4 was to implement Sentinel's new case management and reporting capabilities, and consolidate the various case management components into one overall system. Shortly after the end of this phase, the legacy systems were scheduled to be shut down and the remaining cases in the legacy ACS electronic case file 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.

As the result of lessons learned during the development of Phase 1 of Sentinel, the FBI and Lockheed Martin replanned the remaining phases of Sentinel before development of Phase 2 began. The results of the re-planning effort are discussed in the Findings and Recommendations section of this report.

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

[29] 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.

projects, leverage technology, build institutional knowledge, and ensure that development is based on industry and government best practices. The LCMD is comprised of four integrated components: life cycle phases, control gates, project level reviews, and key support processes. (A diagram showing how these components relate to each other and a description of the life cycle phases, control gates, and the project level reviews mentioned throughout this report are contained in Appendix III.)

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 (Department) 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.[30] Properly executed, IBRs are an essential element of a program manager's risk-management approach. IBRs are

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

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 develop a new 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 IV.)

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.[31] 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 Project Management Office (PMO) dedicated to the Sentinel project.

However, at that time the OIG identified several concerns about the FBI's management of the Sentinel project, 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 ITIM processes.

In December 2006, the OIG released its second audit of the Sentinel project.[32] The second 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 some new concerns identified in the second audit merited continued monitoring. Specifically, the OIG found that the FBI had made progress in:

---

[31] U.S. 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 06-14 (March 2006).

[32] U.S. Department of Justice Office of the Inspector General. *Sentinel Audit II: Status of the Federal Bureau of Investigation's Case Management System*, Audit Report 07-03 (December 2006).

(1) establishing cost tracking and control processes, (2) implementing an 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 August 2007, the OIG released its third Sentinel audit.[33] The third report discussed: (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. The OIG found that the FBI resolved most of the concerns the OIG identified in its first and second Sentinel audits. However, the audit reported that some aspects of the OIG's concerns from the first two audits as well as some new concerns identified in the third audit warranted continued oversight. Specifically, the OIG found that the FBI had made progress in hiring experienced contractors to conduct IV&V evaluations throughout the Sentinel project.

Among the areas that merited continued monitoring by the FBI, the OIG, and other oversight entities were the: (1) completion of a system security plan, (2) completion of Sentinel PMO staffing, (3) completion of comprehensive training plans for the project, (4) determination of management reserve amounts for the remaining phases of Sentinel, (5) risk management and mitigation activities, and (6) project issue tracking and resolution activities.

In May 2006, the GAO released a report critical of the FBI's controls over costs and assets of its Trilogy project.[34] The GAO found that the FBI's review and approval process for Trilogy contractor invoices did not provide

---

[33] U.S. Department of Justice Office of the Inspector General, *Sentinel III: Status of the Federal Bureau of Investigation's Case Management System*, Audit Report 07-40 (August 2007).

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

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.[35] 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 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.

[35] U.S. Government Accountability Office, *Information Technology: FBI Following a Number of Key Acquisition Practices on New Case Management System but Improvements Still Needed,* Audit Report GAO-07-912 (July 2007).

FINDINGS AND RECOMMENDATIONS

FINDING 1: PLANNING FOR PHASES 2 THROUGH 4

At the conclusion of Sentinel's Phase 1 implementation in June 2007, Lockheed Martin developed a strategic plan to address the challenges encountered during development of the project's first phase and to incorporate the "lessons learned" in the project's remaining three phases. The major change in the Sentinel development plan was a modification of the previous 4-phase implementation strategy to include an incremental design approach that would result in more frequent delivery of smaller portions of the overall product. The plan also realigned Sentinel's deliverables in Phases 2 through 4. Based on this revised approach, the project is estimated to cost $30 million more and take 6 months longer to develop than originally planned. In addition to the changes suggested by Lockheed Martin, the FBI added a series of new requirements, including an enterprise portal that will allow users to access multiple FBI IT systems with a single sign-on. The portal will also provide a central location for links to other FBI applications, such as Strategic Information and Operations Center News Feed.

As we indicated in our previous audit, the FBI's move to a more incremental development approach for Sentinel appears prudent. We are concerned, however, with the limited amount of planning that has occurred in three areas: forms, statistics, and records management. At the time of our audit, the FBI did not have a plan to ensure that the data currently collected using nearly 400 different FBI forms will be stored in Sentinel. In addition, the FBI had not determined how it will streamline its case statistics to ensure uniformity, and it appears that Sentinel may be used to automate this task by consolidating the different methods used to collect similar data. Also, while Sentinel, as currently envisioned, will have many of the core attributes of an enterprise-wide records management system, the FBI had not decided whether Sentinel will be the FBI's enterprise record management system or whether it will seek to develop a new and separate records management system.

New Strategic Plan

To incorporate changes to the FBI's requirements for Sentinel and the lessons learned from Sentinel Phase 1 into the remaining phases of Sentinel, the FBI directed Lockheed Martin to develop a strategic plan to describe an approach that would address the challenges encountered in Phase 1. The strategic plan required a reconfiguration of the content and capabilities of the remaining phases and an incremental system development methodology, which resulted in a 6 percent increase in the project cost projection and an increase in the amount of time required to complete the project. In addition, the FBI added requirements for an enterprise portal.[36]

Requirements Clarification Process

To facilitate the reassessment of the capabilities to be included in the remaining phases of Sentinel, representatives from the FBI and Lockheed Martin met daily for 2 months to review the requirements not met by Phase 1, and to ensure that both parties had a mutual understanding of the requirements. This requirements clarification process assisted Lockheed Martin in developing an Engineering Change Proposal (ECP) that reconfigured the capabilities to be included in Phases 2 through 4 of Sentinel. The process also led the FBI to reduce the number of IT systems that will interface with Sentinel and to change the number of IT systems that Sentinel will replace.

Interfaces Reduced

In April 2007, the FBI's Assistant Deputy Director held a meeting with representatives of each of the FBI's four operational divisions, representatives from the Sentinel users group, the Sentinel PMO, and Lockheed Martin. The goal of the meeting was to reduce the number of interfaces Sentinel would be required to have with other IT systems. According to an FBI official, the FBI had identified 43 IT systems that currently interfaced with ACS or had system officials who requested that their system interface with Sentinel. FBI officials reviewed the business needs of each of the interfaces and revised the number of Sentinel interfaces accordingly. Some ACS interfaces were deleted because they were no longer used, and others were deleted because the information provided by the interfaces was captured or could be captured elsewhere. The reduction

[36] The Sentinel Enterprise Portal will allow users to access multiple FBI IT systems with a single sign-on. The portal will also provide a central location for links to other FBI applications.

in the number of interfaces was reflected in the estimated costs for Phases 2 through 4 in an ECP submitted by Lockheed Martin. The original Sentinel requirements, released in July 2005, called for Sentinel to interface with 35 other FBI IT systems. In 2007, 13 of these interfaces were eliminated and another 11 interfaces were added. As of March 2008, the plan was for Sentinel to interface with 33 FBI IT systems. (See Appendix V for a list of Sentinel interfaces.) This reduction in the number of interfaces reduces the cost and complexity of the project.

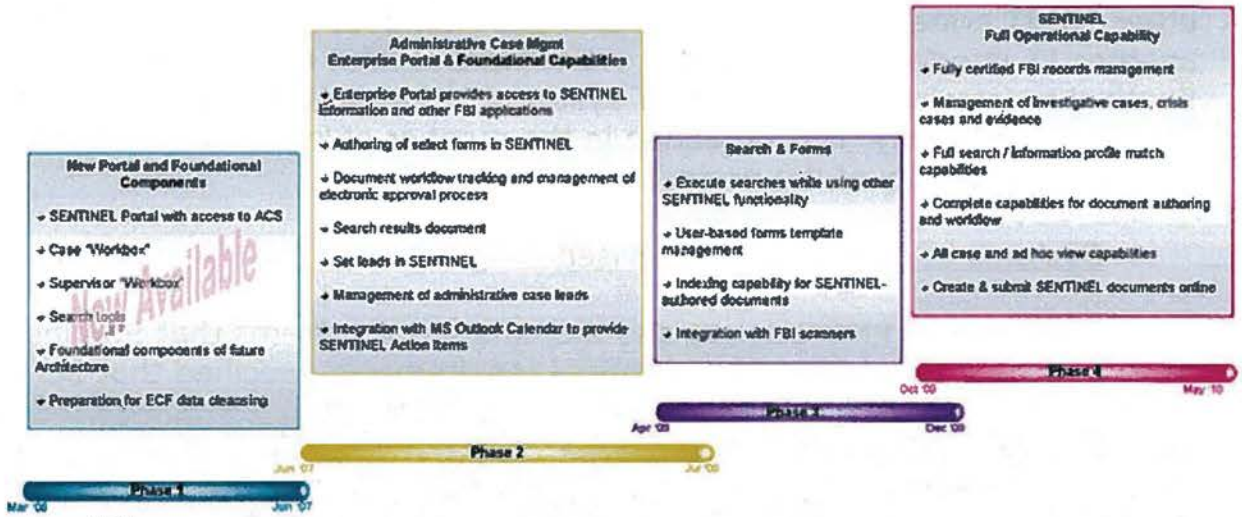
Systems to be Subsumed Revised

The Sentinel PMO also revised the number of systems that Sentinel will replace. The original July 2005 Sentinel requirements specified that Sentinel replace the following nine FBI IT systems: [redacted]. As of January 2008, Sentinel will subsume four systems: [redacted] (See Appendix VI for a description of the systems to be subsumed.) The FBI decided that Sentinel will not subsume Asset, Bank Robbery Statistical Application, Criminal Informant Management System, Data Extraction and Extension Project and Financial Institution Fraud because these systems were not used frequently or another FBI IT system included the functions performed by these systems.

Sentinel Capabilities

Another component of Lockheed Martin's ECP was the realignment of the capabilities to be delivered in Phases 2 through 4. The following figure outlines the capabilities planned for the remaining phases of Sentinel.

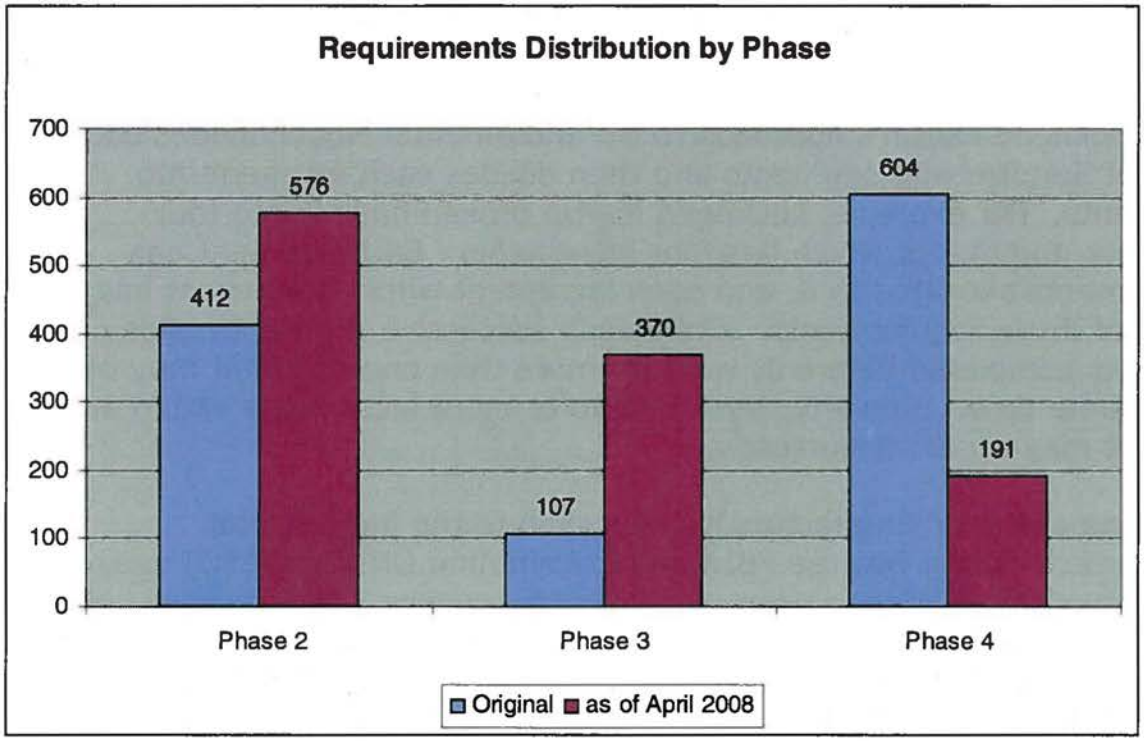
FIGURE A: REVISED SENTINEL SCHEDULE AND CAPABILITIES



Source: FBI

FBI officials said the new strategic plan for delivering Sentinel's capabilities is an improvement for several reasons. They stated that the new plan should eliminate some of the risk involved with data migration because the new plan does not require the majority of data from ACS's three modules to be migrated into Sentinel during Phase 2 as was the case in prior plans. Instead, only the data contained within administrative cases will be migrated during Phase 2. This will allow Lockheed Martin and the FBI to gain experience with creating and managing the migration of a small subset of FBI cases to Sentinel, rather than requiring data from all cases to be migrated into Sentinel at once. FBI officials said this would allow the FBI to refine new workflows that are developed by the organization as it moves to Sentinel from ACS before wide-scale changes are made. In addition, according to the FBI's analysis, the new plan increases the number of requirements satisfied by Phase 2, reducing the FBI's risk exposure created by the high number of requirements that were to be implemented at the end of the project. As shown in the following table, the new plan reduces the requirements satisfied by Phases 3 and 4 combined.

TABLE 1:



Source: FBI

Phase 2 includes two deliveries that were supposed to have been completed in Phase 1. The first delivery includes patch management capabilities for the underlying operating systems and to improve software inventory reporting. While this should improve the Sentinel infrastructure, it provides no new capability to users. The second delivery added tools to enhance Sentinel's internal monitoring capabilities. This should provide diagnostic information to the system operators for use in identifying system faults and degraded performance conditions. Based on the new strategic plan, Phase 2 will also include a new requirement – development of an FBI enterprise portal. This enterprise portal will be the single point of entry for all FBI system users. Sentinel is expected to be the first of many web-enabled applications or services of the enterprise portal.

New System Development Methodology

As part of the strategic planning process, the Sentinel PMO and Lockheed Martin adopted an incremental development model for Sentinel's Phases 2 through 4. The FBI's Life Cycle Management Directive, version 3.0, describes the Incremental Model as a software development model in which development occurs in an overlapping and iterative manner resulting in the

delivery of portions, or increments, of the overall product. Under this model, future increments build on the capability of the increments already delivered.

Lockheed Martin's approach to the Incremental Model divides each phase of Sentinel into segments and then divides each segment into increments. For example, Lockheed Martin broke Phase 2 into four segments, the first of which has four increments. Each segment has requirements allocated to it, and each increment within a segment has a subset of those requirements. While each successive segment builds on the segments completed before it, work on more than one segment may occur at the same time. Similarly, work on two or more increments within a segment may occur concurrently.

One of the driving factors in the switch to the incremental development model was the FBI Chief Information Officer's (CIO) desire to deliver new capabilities to users approximately every 3 to 6 months. Under the Waterfall Model used in Phase 1, the FBI did not deliver new capabilities to users for approximately 1 year. Under the Incremental Model, most increments will provide users with increased capabilities. However, some increments will enhance only the Sentinel infrastructure and not result in added user capabilities.

According to the FBI's Life Cycle Management Directive, version 3.0, the Incremental Model is especially appropriate for environments with significant long-term funding risk. In this situation, high-priority system features and functionality are incorporated in the early iterations when funding is more certain. Higher funding risk falls into the lower priority requirements. The Incremental Model relies on relatively stable and well-understood requirements that are defined early. It should be noted that changes made to requirements using the Incremental Model are especially difficult to accommodate and manage in the context of multiple baselines and overlapping phases.

Revised Schedule

As a result of the time used for strategic planning following Phase 1, the reallocation of the remaining requirements, and the addition of requirements for an enterprise portal, Lockheed Martin and the FBI revised the schedule for the remaining phases of Sentinel. In the revised schedule, Phase 4 is to be completed in June 2010, 6 months later than originally planned. The schedules for Phases 3 and 4 are dependent on the completion

of Phase 2 as well as the receipt of funding needed to complete the phases. Delays in funding would likely cause a delay in the completion of the project.

TABLE 2: SENTINEL DEVELOPMENT SCHEDULE

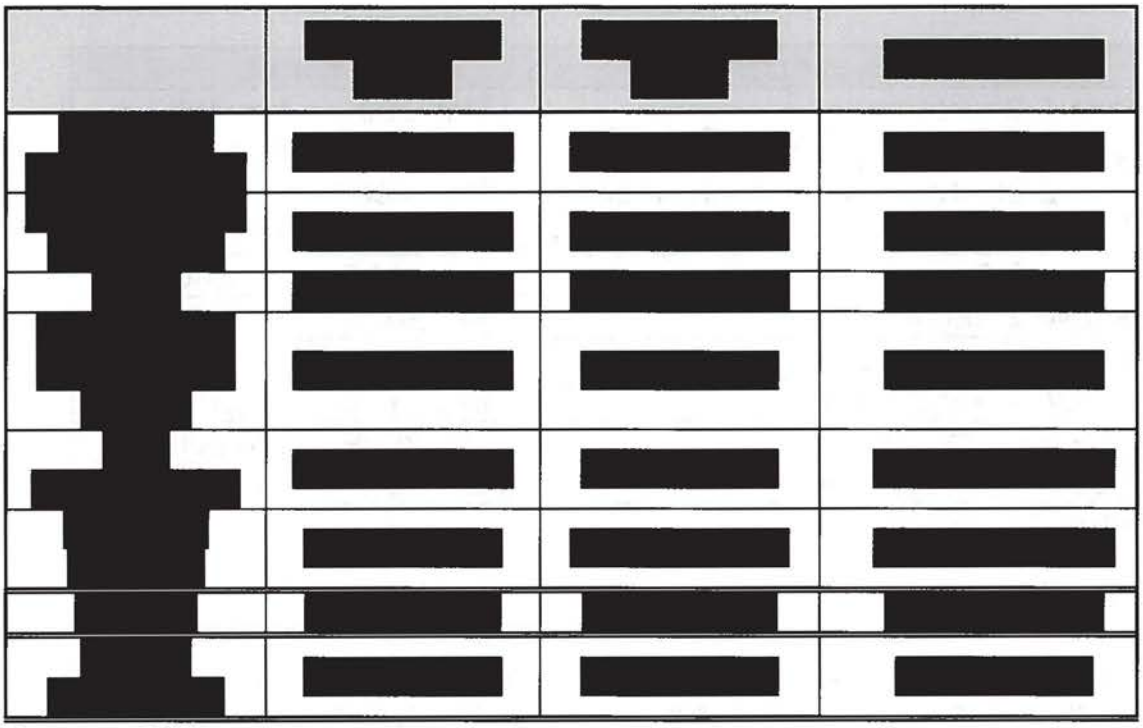
Contract Phase	Dates
Phase 1 Development	Mar 2006 – Jun 2007
Phase 1 Operations and Maintenance	May 2007 – Mar 2010
Phase 2 Strategic Plan Development	May 2007 – Sep 2007
Phase 2 Development	Oct 2007 – Jul 2009
Phase 2 Segment 1	Oct 2007 – Apr 2008
Phase 2 Segment 2	Jan 2008 – Jul 2008
Phase 2 Segment 3	Jun 2008 –Jan 2009
Phase 2 Segment 4	Dec 2008 – Jul 2009
Phase 3 Development	Apr 2009 – Dec 2009
Phase 4 Development	Oct 2009 – Jun 2010

Source: FBI records

Additional Costs

In October 2007, Lockheed Martin submitted an ECP that explained how it would implement the changes in the strategic plan and outlined the plan's impact on Sentinel's cost and schedule. Based on the cost estimate Lockheed Martin included within the ECP, the FBI expects Sentinel to cost a total of $451 million, $26 million more than the $425 million originally planned. The value of the FBI's contract with Lockheed Martin, including all options, increased from about $305 million to $335 million. The FBI Finance Division's Deputy Assistant Director attributed the additional costs to reengineering efforts that occurred after Phase 1 and the new strategic plan development. Table 3 shows the changes between the FBI's Sentinel spending plan in September 2006 and November 2007.

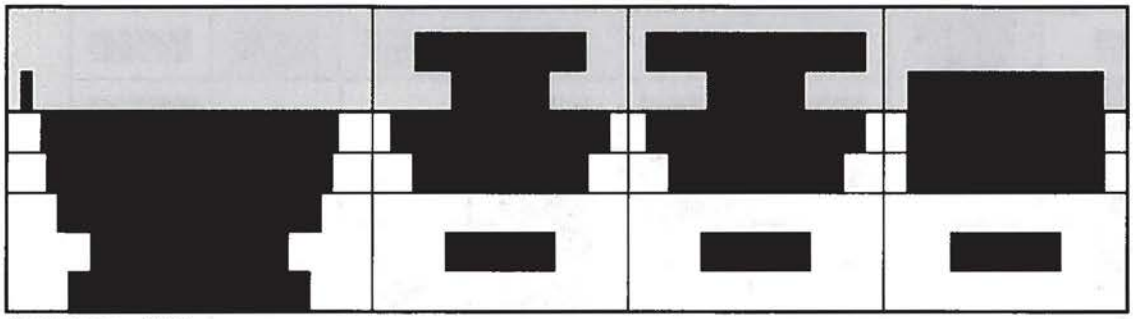
TABLE 3: SENTINEL SPEND PLAN BY CATEGORY SEPTEMBER 2006 AND NOVEMBER 2007



Source: FBI

The FBI estimates the development cost for Phases 2 through 4 will be approximately $191 million, an increase of almost $16 million. Although the new plan calls for Phase 2 to satisfy the majority of the remaining requirements, the FBI reduced the Phase 2 risk management reserve by approximately $10 million. According to the Sentinel system architect, the FBI needs less management reserve under the incremental development model because any potential problems will arise at the increment or segment level when they can be remedied more quickly and less expensively. Additionally, testing, which in the Incremental Model occurs at the end of each increment and segment, is much more frequent than in the Waterfall Model. The overall risk management reserve for Phases 2 through 4 has been reduced from 14.7 percent of development costs to 12.6 percent.

**TABLE 4: DEVELOPMENT COSTS AND RISK RESERVE
PHASES 2 THROUGH 4
NOVEMBER 2007 AND SEPTEMBER 2006 SPEND PLANS**



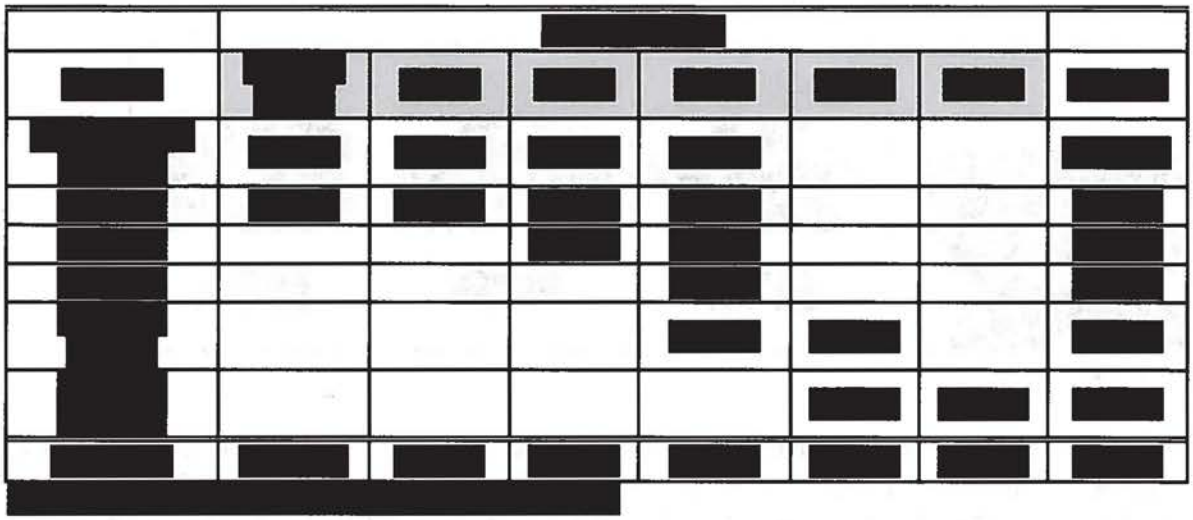
Source: FBI

According to the Sentinel Program Manager, the risk level for Phases 2 through 4 is the same, and therefore the management reserve is the same for each phase. However, due to the shift to an incremental development model, the Sentinel PMO changed the calculation of the risk reserve from Sentinel phase to fiscal year. The Program Manager said the management reserve for each fiscal year is 11 percent of the total combined amount of the development cost, the PMO cost, and the IV&V cost. He said that the shift to basing the management reserve on this combined amount – as opposed to just the development cost – was based on the concept that a schedule or cost challenge would affect all three cost components, not just the development cost.

Most of Sentinel costs occur in Phases 1 and 2, with combined total costs of $305,544,082, or 67.8 percent of the total planned cost of Sentinel. Of the four phases, Phase 2 has the greatest expected cost totaling $197,451,308. Table 5, below, depicts the Sentinel Spend Plan by fiscal year.[37]

[37] The status of Sentinel's progress is discussed in the next finding of this report.

TABLE 5: SENTINEL SPENDING PLAN BY FISCAL YEAR (IN MILLIONS)



FBI's Business Process Reengineering Effort Incorporated into Sentinel

In our judgment, to maximize the return on its investment in Sentinel the FBI cannot merely automate its current business processes. Instead, it must take advantage of Sentinel's potential capabilities to streamline and reinvent its processes. The FBI recognized this need and in April 2005 launched a Business Process Reengineering (BPR) effort. Originally, the FBI's BPR efforts were being conducted outside of Sentinel by the FBI's Deputy CIO. However, the FBI incorporated its BPR efforts into Sentinel in Phase 2. Sentinel PMO officials said that they are currently focusing on two major BPR efforts: (1) reducing the number of "FD" forms and (2) streamlining data captured for various metrics that demonstrate the FBI's level of performance.

The FBI utilizes various standardized forms to capture specific investigative and administrative data, such as documenting significant activities accomplished during a criminal investigation. Data from the forms can then be used to determine various statistics relating to performance, such as the number of arrest warrants issued or arrests made. Forms eligible for use throughout the FBI are defined by a form number that begins with "FD." As of May 2008, the FBI had 817 FD forms being utilized and no

central authority for approving or limiting the creation of new FD forms.[38] At the time, any senior FBI official could approve creation of a new FD form. Additionally, some of the 817 FD forms were not used very often and others captured duplicative information.

Sentinel's System Requirements Specification (SRS) only included the requirements for 22 "work items" or templates to be developed from current FBI FD forms and did not specify which of the 817 FD forms would be replaced by the 22 templates. However, in order for Sentinel to adequately capture all of the information used within the FBI, the templates created for Sentinel would have to incorporate data captured by the FD forms. In an effort to reduce the number of forms, the Sentinel PMO analyzed the content and usage of the 817 FD forms and found, for example, about 150 different consent forms. Because consent forms require a physical signature on a piece of paper, the Sentinel PMO removed all consent forms from the universe of forms that could potentially be eliminated by Sentinel. After further review, the Sentinel PMO found that 324 FD forms were used infrequently, if at all, and that other FD forms were duplicative. The Sentinel PMO led an effort to eliminate the forms that were rarely used or contained information that could be captured elsewhere.

With the elimination of the 324 FD forms, the Sentinel PMO reduced the number of FD forms from 817 to 493. Of the remaining 493, approximately 150 are consent forms, leaving 343 FD forms for which Sentinel must capture data. At the time of our audit, the Sentinel PMO had identified the following six templates that would be used in Sentinel:

- Electronic Communication (EC),[39]
- Payment,
- Collected Items Log,
- Lead Request,

[38] In addition to the FD forms, there are hundreds of forms approved for use at FBI headquarters and hundreds of forms approved for use at FBI field offices that do not have the FD designation.

[39] ECs are the primary type of document used by the FBI for internal communications.

- Report of Investigative Activity, and
- FDXXX (a "boilerplate" forms template).

With only 22 total templates and hundreds of FD forms, the FBI's challenge continues to be determining how to capture in the Sentinel templates the data currently entered into the hundreds of specialized forms. For example, a Sentinel PMO official stated that an EC or Report of Investigative Activity could be used to open a case, a function for which there are currently several FD forms. However, using ECs or Reports of Investigative Activity for this function could be confusing because the current specialized FD forms contain unique sections depending on the type of case that is being opened. For example, the FBI currently uses a specific FD form for civil rights cases. If, as a result of Sentinel, ECs or Reports of Investigative Activity are used to open cases, the FBI would have to update its policies and guidance to explicitly state what information an EC or Report of Investigative Activity opening a civil rights case must include. However, the need to constantly refer to guidance to fill out a FD form may prove to be cumbersome for Sentinel users.

Entering the same data in multiple IT systems or FD forms decreases operating efficiency. As a result, the Sentinel PMO is working to eliminate FD forms or consolidate FD forms that serve common purposes or include redundant information. For example, the FBI eliminated the FD-123, FD-123.1, and the FD-123.2, all of which were entitled "Request for Information Concerning Savings Bond Purchases."

After the completion of our fieldwork, the Sentinel PMO staff working on reducing the number of FD forms concluded that about 122 of the remaining 493 FD forms should be included in Sentinel.[40] As of May 2008, the FBI had not decided whether or not it was going to revise the System Requirements Specification (SRS) to include the additional 100 FD forms. Of the 22 FD forms in the SRS, only 6 are currently under development and none have been finalized or approved.

[40] The 122 FD forms include the 22 templates included in the current SRS.

Agent Statistics

In addition to reducing the number of FD forms, Sentinel BPR efforts are also addressing how the FBI compiles statistical data. The goal of this effort is to ensure that the FBI collects all of the statistics that are required and that the data used in creating the statistics are only collected once. The collection of statistics is vital to the FBI because it shows the progress being made on cases or other tasks. The FBI tracks agent activity by requiring the entry of certain data within the standardized forms for related accomplishments, such as making an arrest or initiating a wiretap. An FBI official stated that the most important inputs to Sentinel are data and the most important outputs are statistics.

According to an FBI official, agents record most of their accomplishments in one of two forms: an FD-515 (Accomplishment Report) or an FD-542 (Investigative Accomplishment Report). The FD-515 form is used to collect criminal statistics and the FD-542 form is used to collect statistics related to the National Security Branch. In addition to having two different forms to collect similar data, the FBI divisions treat similar accomplishments differently. For example, an agent who initiates a wiretap in a criminal case cannot claim an accomplishment on an FD-515 form. However, an agent who initiates a wiretap on a counterintelligence case can claim three accomplishments on an FD-542 form. Even within the National Security Branch we found that accomplishments were treated differently depending on the division. A Sentinel PMO official said that the FBI plans to track statistics through the FBI's Corporate Policy Office, who will also be responsible for forms approval. The Sentinel PMO is working with FBI management to base statistics on techniques (i.e., forms signed and warrants executed) that can be adapted to almost any type of case. We believe the PMO's efforts to use Sentinel as the driver for streamlining the way the FBI records its activities and collects statistics is a critical undertaking.

Records Management

Sentinel is expected to transform the way the FBI does business by allowing the FBI to move from a primarily paper-based case management system to an electronic system of records. However, the FBI has yet to decide whether Sentinel will be the FBI's primary records management application (RMA) or whether the FBI's Records Management Division will maintain a separate repository for all of the FBI's non- investigative records.[41]

The FBI maintains various types of records for investigative cases, travel, training, personnel, and other administrative issues. The FBI's RMA must ensure that accurate records of all activities are created, maintained, and disposed of in accordance with legal requirements.[42] Additionally, the system must provide timely and accurate responses to requests for information from government agencies that need FBI information. The system must also be responsive to requests for information under the provisions of the Freedom of Information and Privacy Acts.

The FBI's overall RMA must also be able to handle all FBI records. Currently, Sentinel focuses only on investigative case records. If Sentinel were to become the FBI's RMA, Sentinel would be required to meet all RMA rules for the various FBI records. For example, the FBI's Records Management Division has a required document retention period for project documents and other records. Major case files are retained for 20 to 25 years after closing, and personnel retirement records are maintained for 99 years. To become the FBI's RMA, Sentinel would have to be developed to ensure that all of these requirements are adequately captured. If the FBI decides to make Sentinel its RMA, an additional investment may be required to add additional capacity to Sentinel and to upgrade FBI hardware. Given

---

[41] A records management application is a software application that automates records management functions and manages electronic records through their life cycle.

[42] A record is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to education, financial transactions, medical history, and criminal or employment history that contains a name, or an identifying number, symbol, or other unique personal identifier such as a finger print, voice print, or a photograph.

A Privacy Act "system of records" is a group of records under the control of an agency from which information is retrieved using a name, an identifying number, symbol, or other unique personal identifier.

that one of the FBI's strategic goals is to automate its records management system, it must make a strategic decision about whether it should build a new separate records management system or expand Sentinel's capabilities to enable Sentinel to become the FBI's enterprise records management system.

Before Sentinel can become a system of records, it also must comply with National Archives and Records Administration standards. This requires that the FBI records officer certify that Sentinel meets these standards. The FBI has developed an Electronic Record Keeping Certification Manual to guide its system certification efforts. Sentinel PMO officials are also working with FBI Records Management Division officials to ensure that Sentinel attains electronic recordkeeping certification by the end of Phase 2, Segment 4, which is scheduled to be completed in July 2009.

During Phase 2, Segment 2, Increment 7, data from FBI administrative cases are to be migrated into Sentinel. The PMO's plan is to migrate to Sentinel all data related to administrative cases stored in the FBI's ACS system. However, according to a Records Management Division official, only about 20 percent of the administrative case data is stored in ACS. The remaining administrative case data consist of paper files, and currently there is no plan to import those files into Sentinel. This pilot migration will serve as a test and will allow for the FBI and Lockheed Martin to gain valuable experience in migrating data prior to the migration of all investigative case file data occurs.

Conclusion

By clarifying Sentinel requirements, changing system development methodologies, and realigning the capabilities to be delivered in the remaining Phases 2 through 4, the FBI and Lockheed Martin have shown a significant willingness to incorporate lessons learned from the challenges encountered in developing Phase 1. In addition, the changes the FBI made to Sentinel interfaces and its reassessment of the systems Sentinel will subsume also demonstrate a willingness to address shortcomings in the original Sentinel specifications.

While the Sentinel PMO has led the effort to eliminate hundreds of little-used FD forms, the FBI must still decide what data from approximately 350 FD forms will be entered into Sentinel and which FD forms will be replaced by Sentinel. In our judgment, these decisions are one of the primary tasks that the FBI needs to address in the immediate future.

Similarly, we believe it is critical that the FBI use Sentinel as the driver for streamlining the way it records accomplishments, the number and type of statistics it collects, and how it collects statistics.

In addition, if the FBI completes Sentinel as currently envisioned, it will have the core of a new records management system in place. Given that one of the FBI's strategic objectives is to automate its records management system, it must make a strategic decision about whether it should build a new separate records management system or expand Sentinel's capabilities to allow Sentinel to become the FBI's enterprise records management system. The decisions the FBI makes concerning forms, statistics, and records management affect whether Sentinel simply automates the FBI's current work processes or whether it enhances the way the FBI conducts its work.

Recommendations

We recommend that the FBI:

1. Decide what data will be stored in Sentinel, how that data will be collected, and what FD forms Sentinel will replace and adjust the Systems Requirement Specification if necessary.

2. Decide which statistics will be stored in Sentinel and how those statistics will be entered into Sentinel, and adjust the Systems Requirement Specification if necessary.

3. Decide whether Sentinel will serve as the FBI's enterprise-wide records management system, and adjust the Systems Requirement Specification if necessary.

FINDING 2: PHASE 2 STATUS

In April 2008, the FBI accepted delivery of the first of four segments that comprise Sentinel's Phase 2, an infrastructure update that should streamline the installation of future software upgrades. We found that while the FBI's EVM data indicated that Sentinel was on schedule and within budget at the time of our fieldwork, the document that governs Sentinel's EVM implementation had not been updated. In addition, other EVM documentation lacked sufficient detail for us to determine whether the changes to the EVM baselines were reasonable and justified. As a result, we could not verify that Sentinel was on schedule and within budget.

Segment 1 Completed

Phase 2 of Sentinel was divided into four segments. In April 2008, the FBI accepted delivery of Phase 2, Segment 1. The goal of Increment 1 was to deliver patch management capabilities for the underlying operating systems and improve software inventory reporting. This increment, while improving the Sentinel infrastructure by adding capabilities that should streamline the installation of future software upgrades, provided no new capability to the user.

In Increment 2, the FBI plans to add tools to enhance Sentinel's internal monitoring capabilities by improving the diagnostic information available to the system operators. This new information should be useful in identifying system faults and degraded performance conditions. These tools should also provide data regarding system response time metrics.

The capabilities included in Increments 1 and 2 were originally scheduled for delivery as a part of Phase 1. However these capabilities were delayed because of technical difficulties and schedule pressures, as well as the FBI's decision to delay the acquisition of certain software and licenses from Phase 1 to a timeframe closer to when they were actually going to be deployed in Sentinel's development.

Increment 3 is to include regression testing, modification, verification, and integration of data migration scripts and the installation and configuration of the data migration system into the FBI's test and design environment. Increment 4, the final increment of Phase 2, involves deployment of a new requirement, an FBI enterprise portal. This enterprise

portal is to become the single point of entry for all users of the FBI's IT network – FBINET.

Funding

According to a senior FBI Finance Division official, the FY 2008 appropriation for Sentinel was $45 million less than required. The FBI had anticipated for Sentinel a $100 million in funding from the previous year's budget included in the base budget of the following fiscal year, but received only $55 million. The FBI funded the shortfall by using "no-year" carryover funds from prior FBI appropriations and reimbursable funds from the Department of Justice Working Capital Fund.

The 2008 Consolidated Appropriations Act did not permit any funds to be obligated or expended for Sentinel until the Deputy Attorney General and the Department's Investment Review Board (DIRB) certified to the House and Senate Committees on Appropriations that Sentinel had appropriate program management and contractor oversight mechanisms in place and that Sentinel was compatible with the Department's enterprise architecture. In addition, $25 million was not made available for obligation until 60 days after the Appropriations Committees received a report from the FBI on the results of a completed integrated baseline review for Sentinel. That report was to be submitted to the Government Accountability Office who would review and provide its findings to the Appropriations Committees within 60 days of its receipt. In addition, funds could not be obligated until the Attorney General certified that existing Sentinel phases currently under contract for development had completed a majority of the work for that phase. As we discuss in the following section of this report, at the time of our audit, the Attorney General had made the certifications necessary to allow Sentinel to continue development.

Status Reporting

The FBI continues to implement EVM and IV&V as tools to help monitor Sentinel's development as well as identify areas of the project that require attention. EVM is a tool that provides an assessment on the completion of planned work. IV&V provides an assessment on particular issues or developments in the project's implementation. In addition, for Sentinel to receive continued funding, the 2008 Consolidated Appropriations Act requires the DIRB to certify that Sentinel has appropriate program management and contractor oversight mechanisms in place and that Sentinel is compatible with the Department's enterprise architecture.

Earned Value Management

EVM helps manage project risks by producing cost estimates, evaluating progress, and analyzing project cost and schedule performance trends. EVM compares the current cost and schedule status 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.

Integrated Baseline Review (IBR)

In August 2005, OMB issued a memorandum requiring that Integrated Baseline Reviews (IBR) be performed for any project that requires EVM to establish performance management baselines against which a project's performance can be measured.[43] Properly executed, IBRs are an essential element of a program manager's risk-management approach. IBRs are intended to provide government and contractor 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.

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

- Underlying performance measurement baseline rationales are reasonable.

- Managers have appropriately implemented required management processes.

On November 5, 2007, the Sentinel PMO performed the Phase 2 IBR and the Sentinel PMO and Lockheed Martin agreed to a baseline schedule of work. Under the incremental development approach, the FBI treats each segment as a separate project. Thus, a separate performance measurement baseline is required for each segment's scope of work and budget to ensure consistency between the two items. Currently, Lockheed Martin submits a Budget Baseline Request 30 days prior to the start of a segment. In lieu of an IBR for each segment, the Sentinel PMO conducts a Budget Baseline Review to validate segment cost, schedule, and scope. However, Sentinel's EVM System Description, which describes how EVM should be implemented for Sentinel and how that implementation will meet ANSI/EIA-748 standards, is not updated to reflect Sentinel's new approach to EVM.

The EVM System Description draft revision 1.0 stated that the purpose of the EVM System Description is to describe the Sentinel program's EVM System, clarify the criteria for applying EVM to the Sentinel program, describe the management information systems and tools supporting the EVM System, and provide evidence that the Sentinel program's EVM System complies with governing guidelines. According to the Sentinel EVM Specialist, the EVM System Description was not updated because other EVM activities have taken precedence. Without an EVM System Description that reflects Sentinel's current practices, we could not determine whether Sentinel was implementing EVM in a way that meets OMB's requirements.

In March 2008, a Joint EVM Audit Team consisting of representatives from the FBI, Department of Justice, and a contractor conducted an annual review of Lockheed Martin's implementation of the EVM process for the Sentinel program. Overall the audit team was pleased with the improvements in the project's EVM program and noted the program had implemented many of the lessons learned from Phase 1, and Lockheed Martin's Sentinel team was actively using EVM to manage the project. However, the EVM Audit Team reported that the Sentinel project had improperly allocated some management reserve funds and improperly used the project's undistributed budget. The findings were compounded by insufficient details or justifications for the changes described in the performance measurement baseline change logs. The logs should have

provided a historical timeline and rationale for baseline changes and their effects. For the management reserve and undistributed budget, the log should have described the scope of work transferred so the validity of the changes could be established. We believe that the inadequate logs gave the appearance that baseline changes were arbitrary.

We reviewed the Sentinel PMO's performance measurement baseline change log and had similar concerns about insufficient details or justifications for the changes recorded in the log. In addition, we found that none of the log entries referenced a Request for Change, a formal FBI document that includes the rationale for project changes as well as formal approval of the changes. We found that the Sentinel PMO was not using the log included in its EVM System Description, which requires a contract modification or Request for Change for each entry in the log. According to the EVM System Description, any changes to the performance measurement baseline log must go through the Sentinel PMO's change management process and an approved Request for Change must support every entry in the log.

Project Status Based on EVM

The Sentinel PMO reported the project's EVM data on a monthly basis, with reports issued about 1 month after the period covered. The EVM report for February 2008 indicated that Sentinel was under budget but behind schedule. In April 2008, the Sentinel Program Manager provided us with a more current assessment of the project and explained that Phase 2, Segment 1 was completed on time and within budget. It was noted, however, that Segment 2 experienced some problems. Segment 2, Increment 5 was approximately 4 weeks behind schedule due to other activities within Segment 2 that were behind schedule. According to the Sentinel Program Manager, the EVM results were consistent with the Sentinel PMO development trouble areas.

Revised Statement of Work Modified EVM Requirements

On October 12, 2007, the Sentinel PMO granted Lockheed Martin authorization to proceed (ATP) with Segment 1 development during the period from October 15, 2007, to April 14, 2008. The Sentinel Statement of Work (SOW) had to be revised due to the change to the incremental development approach, the addition of the enterprise portal, changes to the systems interfacing with Sentinel, and changes to the systems that Sentinel is to replace. The SOW was not finalized until January 29, 2008, over 3.5

months after the ATP was issued and after more than half the development period for Segment 1 had passed.

The original and revised SOWs contained requirements for EVM. However, the revised SOW eliminated some of the EVM requirements compared to the original SOW. For example, the revised SOW did not identify the deliverables that are due at IBR. In our judgment, this change in the SOW diminishes the Sentinel PMO's ability to oversee the development of Sentinel.

In addition, we noted that the EVM requirements contained in the revised SOW are not consistent. The revised SOW, which takes precedence over prior versions, stated that in addition to the common criteria contained in ANSI/EIA Standard 748, the contractor's EVM system, the contractor's earned value baseline, and the contractor's monthly earned value status reports should comply with the detailed requirements contained in the SOW's Attachment 1, *Earned Value Management System Requirements*. However, Attachment 1 of the revised SOW is a Lockheed Martin document entitled "PPM Directive." The attachment references FBI requirements that no longer exist:

> The Lockheed Martin Program Performance Management Process is the corporate process for monitoring and controlling program and project performance and assigning responsibilities for effectively implementing and maintaining program performance management. The *Sentinel SOW Attachment 1* [emphasis added] contained the contract specific EVM System Requirements levied by the customer.

In the event that there is ambiguity or conflict between ANSI/EIA Standard 748 and Attachment 1, the requirements of Attachment 1 were to take precedence. However, the directive refers to Attachment 1 of the previous July 2005 version of the SOW. Therefore, we could not determine what the revised SOW required of Lockheed Martin for EVM. We recommend that the FBI revise Attachment 1 of the current Sentinel's Statement of Work to clarify the requirements with respect to Attachment 1 of the July 2005 version of the Sentinel Statement of Work.

Enterprise Requirements and Assessment Unit

The Enterprise Requirements and Assessment Unit is a component of the FBI's internal oversight of its IT projects. The unit performs periodic

independent "health assessments" of mission critical or high risk IT projects. The assessments provide a risk-based look at a project's schedule and cost performance to determine the time and money required to complete the work remaining on a project. The assessments provide FBI managers with another tool to judge the schedule and cost progress of important FBI projects.

The Enterprise Requirements and Assessment Unit identified 235 Sentinel tasks with negative "slack" in the schedule. Slack is the amount of time that an activity may be delayed from its start without delaying the project finish date. When slack is negative, the task cannot be completed without delaying completion of the project. The Sentinel Program Manager said that Segment 2 had been 4 weeks behind schedule, but that 2 of the 4 weeks had been recouped. In its June 11, 2008, assessment, the FBI's Enterprise Requirements and Assessment Unit concluded that Segment 2 was approximately 18 days behind schedule due to an over-allocation of resources and the lack of an integrated Phase 2 schedule. When the schedule is leveled with adequate resources and time needed to eliminate the over-allocation of resources, the schedule is 122 days behind schedule.

In addition, the Enterprise Requirements and Assessment Unit reported that the Segment 2 schedule was rebaselined for a second time on April 23, 2008; however, as of that date, no documentation has been provided indicating who provided authorization for the update. The Enterprise Requirements and Assessment Unit reported that:

> it appears that when the baseline update was performed the entire project baseline was updated. The current Segment 2 schedule has 3,042 tasks with a different baseline start date from the previous version. Additionally the current schedule has 90,514 hours of Baseline Work, which represents a 33 [percent] reduction from the 134,538 hours of Baseline Work from the original [February 1, 2008] baseline.

Authorization for each change to the baseline is an important control for managing a project's cost, scope, and schedule. According to FBI officials, except for the rebaselining due to the change to an incremental development approach, there has been no other rebaselining in Phase 2. FBI officials stated that the PMO maintains baseline control at the control account level. Changes below the corresponding work breakdown structure level are generally considered at the discretion of the prime development and deployment contractor to manage provided (1) full disclosure of changes

are made to the PMO, and (2) no impact to cost or schedule is made at the government-controlled baseline level. Changes made to the government-controlled baseline level are currently made by a change request and are codified through contract modification.

Department Certification

As discussed in the funding section of this finding, the 2008 Consolidated Appropriations Act did not permit any funds to be obligated or expended for Sentinel until the Deputy Attorney General and the DIRB certified to the Appropriations Committees that Sentinel had appropriate program management and contractor oversight mechanisms in place and that Sentinel was compatible with the Department's enterprise architecture. In January 2008, the DIRB granted Sentinel provisional certification, which allowed the FBI to obligate and expend funds only for the development of Sentinel Phase 2, Segments 1 and 2. At the time the DIRB granted Sentinel its provisional certification, one recommended item remained open, the delivery of a Full Operating Capability (FOC) Architecture and Design Document. The DIRB specified that the Design Document should include the specific COTS or government off-the-shelf tools necessary to implement the architecture. In June 2008, the DIRB certified that Sentinel met the provisions of the Consolidated Appropriations Act of 2008, subject to 10 qualifications, including that Sentinel use the "to-be-completed FOC architecture to help generate new cost and schedule estimates for all future program work."

The FOC architecture was to be completed concurrently with the development of Phase 2, Segments 1 and 2. According to the Sentinel Deputy Program Manager of Systems, the development of the architecture is an engineering task focused on the development of a package of documentation that did not fit into the incremental "requirements, design, and test" process and as a result, was not assigned to a specific segment or increment. The bulk of the architecture work to the sub-component level was accomplished in Segment 1.

After the FOC architecture is developed and certified, the Sentinel PMO plans to perform reviews at the end of each segment to determine if the targets were met within each segment or if changes are required to meet system requirements specifications. The Sentinel PMO anticipates making small adjustments to the FOC architecture as the remaining phases are completed, but no major changes are anticipated.

Independent Verification and Validation

Inadequate implementation of any step in a disciplined systems development process 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 effect. One way to monitor the processes used in systems development is to implement an Independent Verification and Validation (IV&V) process. IV&V is an assessment or review of a project by an impartial party.

In September 2006, the FBI hired Booz Allen Hamilton (Booz Allen) to perform the IV&V evaluation for the Sentinel program. Since then, Booz Allen has participated in Sentinel program meetings and reviews. For Phase 1 O&M and Phase 2, Booz Allen provided written comments and recommendations on many project documents and produced 10 monthly reports. However, according to Booz Allen, Phase 2, Segment 1, Increments 1 and 2 were outside the scope of their review.

The 10 reports, as well as the briefings Booz Allen presented to the FBI, highlighted recent activities, upcoming events, and Booz Allen's view of the overall status of the project, including a discussion of the risks that could affect the project's recommendations and best practices. Between June 2007 and March 2008, Booz Allen made over 70 recommendations based on risks and other areas of concern it identified. (See Appendix VII for a list of IV&V issues and recommendations.) Booz Allen also reported several project management and oversight weaknesses in the areas of system architecture, design, testing, forms, data migration, design, security, and EVM. Booz Allen concluded that these weaknesses increased the risks associated with Sentinel's cost, schedule, and performance baselines.

Full Operating Capability Architecture

In February 2008, Booz Allen noted that it previously reported that during Phase 1 the incomplete system design contributed to the challenges in deploying Phase 1 and that the Web Application (WebApp) design was not completed until a substantial amount of coding was started. Even within an incremental development approach – within an O&M environment – a design document would have aided in the development process. Booz Allen recommended that the Sentinel PMO develop detailed design documentation or artifacts that described the design for the WebApp.

Booz Allen also noted that any delay in the delivery and acceptance of the FOC architecture may delay the delivery of Segment 2, Increment 5. The delivery date of the FOC architecture documents – the Design Concept Description Architecture and System Design Document – was moved back from March 22, 2008, to April 14, 2008. Consequently, the FOC architecture would not have been delivered until after Increment 5 began.

According to Booz Allen, the Sentinel PMO acknowledged that there were gaps in the architecture and design, and that the Sentinel PMO was taking steps to address these gaps. Specifically, the Sentinel PMO was conducting In-Progress Reviews of the FOC architecture with Lockheed Martin to ensure that Lockheed Martin understood the FBI's expectations and concerns about gaps in the architecture and that Lockheed Martin took the appropriate actions to ensure the development of a sound and complete design. Booz Allen believed the Sentinel PMO was taking the appropriate steps to ensure that a high quality FOC architecture was developed, but noted that the FBI will need to actively manage the steps Lockheed Martin takes to address the FBI's concerns.

Testing

In July 2007, Booz Allen noted that the overall Phase 1 performance evaluation of the Sentinel system for 5,000 simultaneous log ons and 2,000 active concurrent users was inconclusive. The performance testing of the Sentinel system during Phase 1 included a low to moderate workload. Because Phase 1 testing did not include a high workload, the Phase 2 incremental deliveries, which should increase the number of Sentinel users, could result in users experiencing longer times to receive search results. Booz Allen recommended that the Sentinel PMO conduct performance testing with realistic workloads for Phase 2. Also, in Februrary 2008 Booz Allen recommended that the Sentinel PMO allocate time in the baselined schedule to adjudicate and resolve any high-priority issues identified during user acceptance testing prior to formal acceptance of the increment.

Forms

In December 2007, Booz Allen recommended that the Sentinel PMO establish: (1) a formal Forms User Group to effectively complete the three tracks related to the streamlining of FD forms and (2) a timeline and target

and date for the Forms User Group to deliver the outputs from the three tracks along with their recommendations for Sentinel.[44]

Data Migration

In December 2007, Booz Allen noted that the Sentinel PMO's overall data migration approach called for the migration of ACS legacy data into Sentinel just prior to the associated functionality being implemented in Sentinel. Booz Allen found the Sentinel PMO's approach viable and recommended that the future versions of the Sentinel Data Migration Plan present data migration plans for segments in future phases, not just the present segments currently under development or segments that will be developed in the near future. For example, if one case classification holds a large quantity of data and requires extensive cleansing, the overall approach for delivering a set of functions to users may change as a result.

In March 2008, Booz Allen concluded that without a complete data migration plan, which covered all types of FBI cases, the likelihood of completing all of the data migration by May 2010 decreased with the currently allocated schedule and funds. Booz Allen recommended that the Sentinel PMO include additional items on the FOC roadmap (e.g., estimated date, forms, reports, and case classifications).

Design

In November 2007, Booz Allen reported that Phase 1 O&M Build 1.10 would deploy the new Sentinel WebApp, replacing the Portlet Factory framework that was used to build the Phase 1 system. The WebApp was expected to address existing maintainability issues (i.e., the need for weekly reboots to prevent system failures and unplanned outages) and improve response times for search functions. Delivery of the WebApp to the production environment was delayed 19 days, due in part to delays in the free and open source software approval and the inability to complete the targeted level of software coding in the anticipated timeframe.

[44] Track 1 concentrates on FD forms that should be deleted in their entirety from the forms inventory. Track 2 concentrates on the modification and/or consolidation of forms. Track 3 concentrates on the identification of forms in the near future that will become Sentinel templates in their current state.

Security

In July 2007, Booz Allen reported that the 12 audit reports submitted for Phase 1 Deployment Acceptance Review provided administrators only with a very high level depiction of Sentinel system activity. Because Phase 1's reporting capability lacked the automation and flexibility to generate more detailed reports, system administrators had to manually audit the details in the original logs to discover the root causes of variances between different audit logs and the correlations between entries. Booz Allen reported that the rigidity in reporting coupled with the intensive manual analysis required and limited administrator staffing increased the risk that a security incident would go undiscovered and fail to be addressed in a timely manner.

Earned Value Management

In October 2007, Booz Allen noted that as Sentinel increments are tested, deficiency reports would be developed to document parts of the increment that are neither working appropriately nor meeting the requirements. During testing, priority 1 or 2 deficiency reports should be resolved prior to completion and acceptance of the increment. Booz Allen questioned whether the completion dates of increments and segments were static or if they could be extended to address items that arise during development and testing. For example, Increment 3 can be scheduled to be completed at the same time as Segment 1. However, if Increment 3 had an open priority 1 deficiency report, the FBI would have to decide whether Segment 1 would end as planned and, if so, whether the Segment Acceptance Review would still occur but with a lien (a weakness requiring correction) to cover the open priority 1 deficiency. Booz Allen recommended that the Sentinel PMO document and clarify in the Life Cycle Process Program Methodology whether segment and increment finish dates are static or whether they are flexible depending on an assessment of what is actually completed. Booz Allen noted that the resolution of these issues could have a significant impact on Sentinel's EVM metrics.

In July 2007, Booz Allen reported that an effective EVM System not only addresses accurate historical status, but also uses data to generate independent estimates of the cost and schedule to complete a project. These independent estimates would allow the Sentinel PMO to validate forecasts provided by Lockheed Martin. Change control was an area in which the Booz Allen summarized lessons learned and observations from Phase 1 that must be addressed in Phase 2 to maximize the potential of the EVM System as a predictive tool. Booz Allen recommended that the Sentinel

PMO document corrections to EVM data in a detailed Errata Report to facilitate traceability.

Conclusion

The FBI succeeded in dividing Sentinel's remaining three phases into smaller, more manageable segments that should result in more frequent deliverables to Sentinel users. We found that the IBR focused almost exclusively on Phase 2, Segment 1 and that the FOC architecture, which should tell engineers what end state to build to, has not been completed. Because of this, the potential exists for development work that was planned for Phase 2 to be extended into the O&M phase of the project or moved to a future phase. If the work is extended into future phases, the risk is that by the end of Phase 4 there will be no where to shift development tasks and as a result the schedule may continue to get extended, the FOC Sentinel product may be revised to fit the work accomplished, or additional funds may be needed to complete the project. Additionally, Sentinel's use of an EVM system that differed significantly from its EVM System Description only exacerbates this concern.

Recommendations

We recommend that the FBI:

4. Complete the Sentinel FOC architecture.

5. Update the EVM System Description.

6. Provide better descriptions and justifications for EVM baseline changes.

7. Revise Attachment 1 of the current Sentinel Statement of Work to clarify the requirements with respect to Attachment 1 of the July 2005 version of the Sentinel Statement of Work.

FINDING 3: PHASE 1 SYSTEM PERFORMANCE, SECURITY, AND USAGE

According to Sentinel PMO data, the number of unique Sentinel users decreased each month since Sentinel's implementation in June 2007 through December 2007. Sentinel officials attributed the decline in the number of Sentinel users to initial user curiosity and the limited functionality of Sentinel's Phase 1. Through February 2008, the FBI had authorized 12 updates to Phase 1 of Sentinel to address minor problems, user requests for improvements, routine maintenance, and the correction of system abnormalities. In addition to collecting user data, the FBI also established performance measures to evaluate the technical performance of Sentinel, such as the percentage of time that Sentinel is functioning and available for use by FBI employees. However, we found that most of these metrics were applicable to measuring Sentinel's ultimate performance at the end of Phase 4.

Phase 1 User Acceptance

Since the deployment of Phase 1 in June 2007, the FBI has collected data on the number and demographics of Sentinel users. To further understand the user data, the FBI established focus groups at field offices and conducted a Sentinel User's Conference.

Sentinel User Statistics

According to data collected by the Sentinel PMO, June 2007, the month Phase 1 was released, had the greatest number of unique users with [redacted] As shown in Table 6, the number of unique users declined every month from June 2007 through December 2007 but increased from December 2007 through February 2008.

TABLE 6: UNIQUE SENTINEL USERS
JUNE 2007 – FEBRUARY 2008

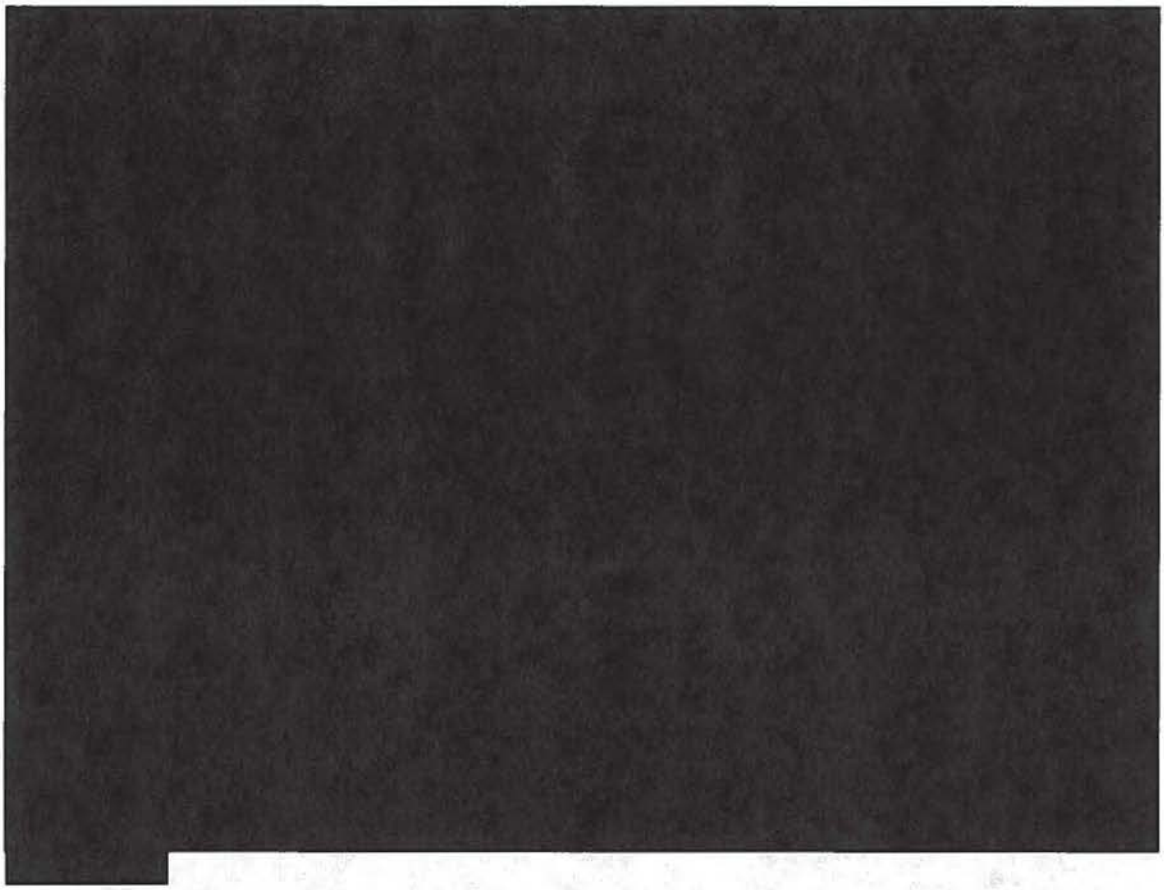


Table 7 compares the variance in the number of unique users for ACS and Sentinel from June 2007 to January 2008. During that period, the number of Sentinel users decreased by 30 percent while the number of ACS users decreased by 2 percent.

The FBI's Deputy Program Manager for Organizational Change Management said that the June 2007 number was artificially inflated because employees, even those who do not normally use ACS, were curious to try Sentinel when it was deployed. He also said that there was a mandate from the FBI CIO requiring personnel to sign in simultaneously in an effort to perform load and performance testing. FBI officials said that an additional reason for the increase in June usage was that many FBI divisions mandated that all employees attend Sentinel training. Trainers were sent to all 56 field offices and headquarters over a 3-week period to conduct training just prior to the June deployment. Sentinel PMO officials said they believed the limited functionality of Phase 1 of Sentinel was the cause of the declining number of

Sentinel users over the first 6 months of its implementation. They noted that portions of the user community must use ACS to complete functions that are not currently available in Sentinel. Rather than log on to Sentinel to perform functions Sentinel was capable of performing and then log on to ACS to perform the remainder of their work, these users appeared to be using ACS to perform all of their work. We agree with the Sentinel PMO's assessment that Phase 1's limited functionality caused the decline in usage and kept Sentinel from being more popular with FBI personnel.

TABLE 7: PERCENTAGE OF MONTHLY ACS UNIQUE USERS AND MONTHLY SENTINEL UNIQUE USERS COMPARED TO SENTINEL DEPLOYMENT MONTH (JUNE 2007 THROUGH JANUARY 2008)[45]

The Deputy Program Manager for Organizational Change Management stated that the FBI engaged in two activities since late 2007 which he believes encouraged personnel to use Sentinel and increased the number of unique users per month. The FBI sent information cards to all FBI squads

[45] The February 2008 ACS numbers were not available at the time of our audit, so we performed our analysis through January 2008.

that describe the current and planned functionality of Sentinel.[46] Also, since October 2007 a joint FBI and Lockheed Martin team has conducted Organizational Impact Assessments at various FBI field offices. Additionally, the FBI held a Sentinel User's Conference in November 2007 to obtain feedback on Sentinel functionality from end users.

Organizational Impact Assessments

As of January 2008, a joint Sentinel PMO and Lockheed Martin team conducted Operational Impact Assessments at three FBI field offices. The purpose of these assessments was to measure and evaluate the potential effect of scheduled changes to Sentinel – both positive and negative – on Sentinel users. Each Operational Impact Assessment included 16 to 24 representatives from various job functions, but the format and focus varied. For example, two of the assessments focused on Sentinel's potential long-range capabilities while the third focused on prioritizing Sentinel's future capabilities. The Sentinel PMO plans to conduct an Operational Impact Assessment at all 56 FBI field offices before Sentinel is completed. We believe these assessments can be a meaningful tool to ensure Sentinel meets the needs of the Sentinel user community.

During all three assessments, the Sentinel PMO and Lockheed Martin team solicited user feedback on Sentinel's current limitations and discussed what capabilities users needed next from Sentinel. The following is a list of prevailing issues recorded during the three Operational Impact Assessments.

- Some functionality (open cases, set leads) only exists in ACS and many ACS functions are not yet available in Sentinel.
- ACS is still available and many proficient ACS users are not accustomed to using Sentinel.
- Some users do not want to invest time in learning and using Sentinel until it is complete.
- Sentinel takes too long to respond to user queries for information.
- Users do not like switching back and forth between ACS and Sentinel to do their jobs.

[46] FBI field offices are divided into squads that have specific subject matter responsibilities, such as the drug squad and the counterterrorism squad.

Usability Conference

In addition to the decline in usage, Sentinel user statistics also indicated large variances across the FBI by field offices and headquarters divisions. For example, during August 2007 54 percent of the potential users in the St. Louis Field Office logged onto Sentinel at least once.[47] During the same period, only 11 percent of the potential users in the Albuquerque Field Office used Sentinel at least once. At FBI Headquarters, 27 percent of the Cyber Division's potential users logged onto Sentinel at least once, while only 5 percent of the Directorate of Intelligence's potential users logged onto the system.

To understand this disparity and improve Sentinel usage, the Sentinel PMO held a Usability Conference in November 2007. Representatives from 10 field offices and FBI headquarters divisions, selected from both high- and low-usage offices, provided feedback and voiced their level of satisfaction with Sentinel through a series of focus group discussions. Sentinel program designers, developers, and human performance analysts used the conference to understand the human and system factors behind Sentinel usage and to identify potential improvements for future versions of Sentinel. Based on the conference's findings, we believe three broad areas have most affected Sentinel usage: (1) technology, (2) position requirements, and (3) leadership.

Technology

Sentinel user representatives said that technical limitations of Sentinel and the FBI's network had a significant impact on Sentinel usage. With regard to Sentinel, they said that Sentinel's current limited functionality, design, and performance discouraged use of the system. For example, Sentinel does not allow some users to perform their jobs without using ACS. Once these users log in to ACS, many of them choose to use ACS for all of their tasks rather than log in to Sentinel to perform a subset of their tasks.

Conference participants also cited several design issues that they believed limited Sentinel usage. For example, they said it was easier to send a lead to a large group of people in ACS rather than in Sentinel. In ACS, it is common practice to select multiple leads and assign those leads to multiple offices. Sentinel currently requires users to assign each lead

[47] For the purpose of this analysis, the FBI defined a potential user as a person who logged onto ACS at least once during the four Wednesdays in August 2007.

individually. Future versions of Sentinel will allow multiple leads to be assigned to multiple offices.

The Sentinel users at the conference also voiced concerns about the accuracy of Sentinel's search results and the record count of the search results. Sentinel PMO officials agreed that the number of returned records Sentinel indicated did not always match the number of records displayed. Sentinel PMO officials agreed that the business rules on which Sentinel operates have caused its count of the number of records returned in a search to not match the actual number of records returned. Sentinel PMO officials acknowledged that this and other issues could affect Sentinel's credibility and discourage its use.

The user representatives also said that the FBI network on which Sentinel resides did not provide adequate bandwidth to smaller FBI offices, increasing network log in times to as much as 30 minutes. As a result of these long login times and the limited functionality of Sentinel, users at remote offices said they choose to use only ACS.

Position Requirements

Conference participants said that Sentinel's benefits vary significantly according to a user's job requirements. The primary functions of Phase 1 were lead assignment and follow up, functions which the Sentinel PMO agreed benefit Supervisory Special Agents (SSA) and Special Agents more than most other positions. However, personnel in other roles, such as Support Services Technicians (SST), require functionality that is currently only available in ACS. For example, SSTs open and close cases, a task that can currently only be done in ACS. Since SSTs have to log into ACS to perform their jobs, they found it easier to use ACS exclusively rather than switching between the two systems. In addition, SSTs must access multiple computer systems to do their jobs, so at this point Sentinel complicates their jobs rather than simplifying them. For example, they must use either Web-Based ACS (WACS) or ACS to upload documents and to open or close cases, and they rely on the Investigative Data Warehouse to conduct searches

Leadership

Conference participants stated that leadership and support from senior FBI managers was critical to increasing Sentinel usage and ensuring Sentinel's overall success. They said they could not remember any recent examples of visible leadership from the Director and other executives

regarding Sentinel and its high priority within the FBI. The conference participants said that executive level communication and support would be very effective in conveying how Sentinel supports the FBI's priorities.

The conference participants also stated that the level of support given by Special Agents-in-Charge (SAC) for Sentinel in the FBI's 56 field offices was inconsistent, with some SACs showing significant support and others seemingly discouraging its use. For example, in the St. Louis and Salt Lake City Field Offices, two of the offices with the highest Sentinel usage rates, the SACs mandated the use of Sentinel. Specifically, the SACs required SSAs to use Sentinel to assign and manage leads. In addition, they required agents to use Sentinel to view leads assigned to them. Overall, the conference participants viewed these mandates as a reasonable and effective way to increase Sentinel usage. However, the conference participants noted that such mandates should be targeted to positions that receive the most benefit from Sentinel's current functionality.

Operations and Maintenance (O&M) Activities

After the FBI accepted from Lockheed Martin delivery of Phase 1 of Sentinel, Phase 1 entered the Operations and Maintenance (O&M) phase of the IT life cycle. So far, the activities performed during Phase 1's O&M have addressed low priority deficiencies existing at the time of delivery, user requests for improvements, and system maintenance. While the Sentinel PMO provided oversight, Lockheed Martin is responsible for most of the technical work in the O&M phase, including system maintenance, resolution of issues identified by Sentinel users, and the ongoing detection of system abnormalities.

Phase 1 Updates

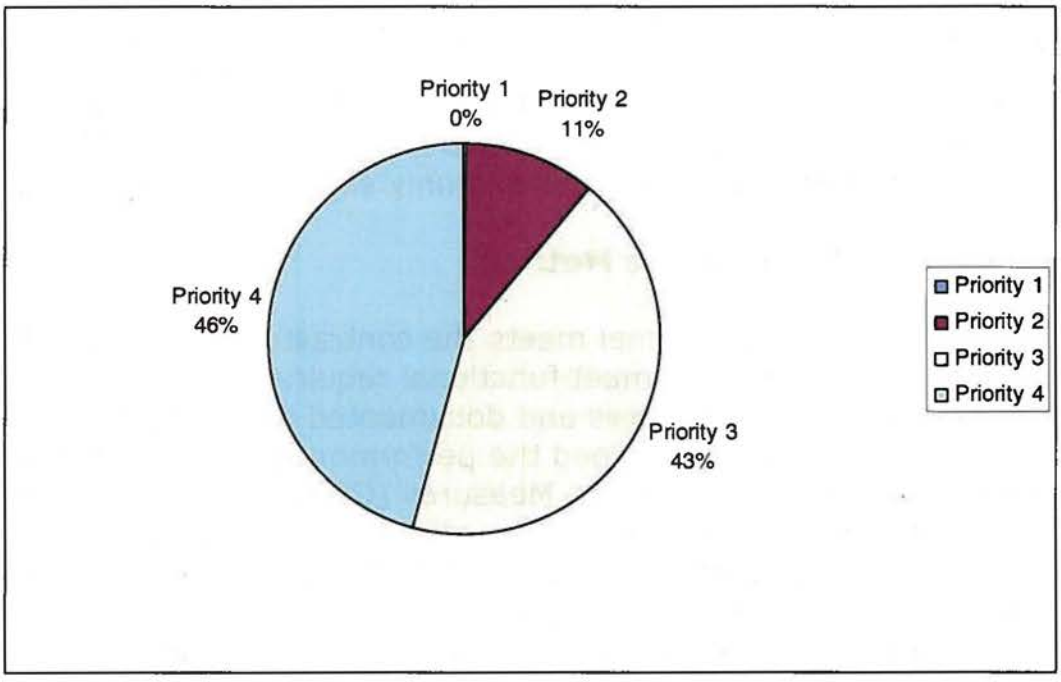
To address issues identified in the O&M Phase 1 of Sentinel, the FBI has authorized the release of updated versions of Phase 1, called builds. From June 2007 when Phase 1 was deployed through February 2008, the FBI released 12 builds. (Appendix VIII describes the major functions included in Builds 1 through 12.) From a user perspective, Build 10, which added the Sentinel Web Application, may have been the most significant Sentinel update. According to Sentinel PMO officials, Build 10 addressed several user interface issues concerning the presentation of data that users identified during Phase 1 user acceptance testing or in early deployment feedback. The Sentinel Web Application also changed the underlying technology used to deliver data to users. Sentinel PMO officials stated that

this change was implemented to reduce the amount of system maintenance needed and to improve user response times for searches.

The Sentinel Joint Engineering Board (JEB) – a governance board comprised of both FBI and Lockheed Martin personnel – manages changes to Sentinel and decides which technical problems and functionality updates each build will address. To aid in this decision making process, the JEB assigns one of four priority rankings and one of five severity rankings to Defect Reports. Defect Reports (DR) are the primary source for the changes included in each of the Sentinel builds. (See Appendix IX for the criteria used to assign these rankings.)

The 12 builds we reviewed addressed 456 DRs. Of these, 89 percent received a priority 3 or 4 rating and 11 percent received a priority 1 or 2 rating. Priority 1 and 2 DRs require immediate attention. Table 8 summarizes the DRs by their priority rating.

TABLE 8: PHASE 1 O&M BUILDS BY DEFECT REPORT PRIORITY RATING



Source: OIG analysis of FBI data

The Sentinel PMO tracked the functional area of each DR addressed in O&M Builds. (See Appendix X for a description of each functional category and a summary of the total number of DRs addressed in O&M Builds by

functional area.) The software development and COTS integration functional areas constituted 74 percent of the DRs addressed by the 12 builds we analyzed. We believe that this was the result of the COTS integration, requirements deferment, and design issues that Sentinel encountered during Phase 1 development. The Sentinel PMO and Lockheed Martin have since engaged in re-planning the remaining Sentinel development phases. We believe that this re-planning should help to mitigate the risk that these issues will resurface in subsequent phases of Sentinel's development. We also believe that the Sentinel PMO and Lockheed Martin have a procedure in place, executed by the JEB, which provides a timely and meaningful way of resolving DRs.

O&M Costs

Through the use of a contract modification, the FBI awarded Lockheed Martin the O&M of Phase 1 for the period of May 2007 through May 2010. At the time of our audit, the FBI had allocated $10.1 million to Phase 1 O&M activities for the period ending September 30, 2008. The FBI forecasts that Phase 1 O&M in future years will cost an additional $8.5 million.

As discussed in finding two, the Sentinel PMO is using earned value management (EVM) to manage Sentinel's cost and schedule performance. As part of that effort, the Sentinel PMO also collected EVM data on Phase 1 O&M activities. Through the February 2008 reporting period, EVM data indicated that O&M was within budget and only slightly behind schedule.

Phase 1 System Performance Metrics

To help ensure that Sentinel meets the contractual requirements of the program and that deliverables meet functional requirements, the FBI established performance measures and documented them in the Sentinel Measurement Plan. The plan defined the performance data to be collected, including seven Critical Performance Measures (CPM) and five O&M data elements (a description of each CPM data element and whether Sentinel is operating within the threshold for each data element respectively is provided in Appendix XI).[48] The seven CPM data elements required by the Measurement Plan address technical aspects of Sentinel's performance such as the percentage of time the system is available to FBI users.

[48] CPM data elements are used to track system performance during development to gauge whether the specific program elements will be met once the system has been deployed. O&M data elements track system performance after the system has been deployed.

The Sentinel Measurement Plan requires Lockheed Martin to submit an evaluation of Sentinel metrics in a monthly Measurement and Defect Report. Lockheed Martin distributes this report to the Sentinel PMO and other FBI offices overseeing the performance of Sentinel. However, as shown in Table 9, from June 2007 through February 2008 Lockheed Martin submitted only four of the required nine Measurement and Defect Reports.

TABLE 9: PHASE 1 MEASUREMENT AND DEFECT REPORTS

Data Collected (Month/Year)	Report Issued
June 2007	NO
July 2007	NO
August 2007	NO
September 2007	NO
October 2007	NO
November 2007	YES
December 2007	YES
January 2008	YES
February 2008	YES

Source: OIG analysis of FBI data

A Sentinel PMO official stated that Lockheed Martin did not submit measurement reports from June 2007 through October 2007 because the FBI did not require these reports from Lockheed during the re-planning period between Phases 1 and 2.

We reviewed the CPM and O&M metrics in the four reports Lockheed Martin submitted to determine whether Sentinel system performance was meeting technical expectations. In at least one of the four reports we reviewed, Sentinel did not meet four of the seven CPMs. A Sentinel PMO official stated that the CPMs reflect Sentinel's intended capability at the end of Phase 4, referred to as full operating capability (FOC), and the FBI did not expect Phase 1 to always meet the FOC thresholds. This official also stated that the objective is for Sentinel to show progress in meeting its FOC CPM thresholds as Sentinel progresses through the remaining phases. In our judgment, the seven CPMs are not useful for monitoring Sentinel's performance until Sentinel's completion, and the PMO has not established interim CPMs, such as the measures used during Phase 1 testing, to monitor the performance of Phase 1. We believe that interim measures could be helpful in assessing issues of concern to Sentinel users.

Each CPM data element in the Sentinel Measurement Plan has been linked to a Sentinel requirement in the Sentinel System Requirements Specification (SRS), which provided the requirements for the Sentinel system. These requirements were defined in more detail in the Phase 1 System Specification, which defined the functional and performance system requirements and criteria for verification and acceptance of the Sentinel system for Phase 1. We found that three of the seven CPM thresholds in the Sentinel Measurement Plan were different than the thresholds in the Phase 1 System Specification. (Appendix XI discusses which thresholds were consistent and which were not.) For the period we reviewed, if Phase 1's performance was measured using the System Specification thresholds, it would meet six of the seven thresholds.

While we agree it may be useful to measure Sentinel CPM metrics against its FOC thresholds in order to get an early warning of potential areas of performance problems, we believe it is also beneficial for Sentinel to measure CPM metrics against its current phase thresholds. Without consistent threshold criteria, system performance measurement is not a useful tool. Since the Phase 1 System Specification defines requirements for Phase 1 functionality, we believe that the Sentinel Measurement Plan should include those thresholds for CPM data elements.

Also, in at least one of the four measurement reports we reviewed, Sentinel did not meet the threshold for two out of five O&M performance measures.[49] Most significantly, problems identified by users were not resolved within the specified time.[50] We found that the PMO does not have a documented process for responding to measurement reports that include measures outside of their threshold. A Sentinel PMO official said that measurement report metrics are just one of several indicators that may signal a potential performance problem and that the trend over several months may be a more important indicator of system performance.

---

[49] O&M metrics are used to determine whether the performance of the currently deployed version of Sentinel is meeting performance requirements and identify areas which need to be addressed that do not meet the requirements. (Appendix XII describes the five O&M data elements and identifies whether Sentinel exceeded the threshold during the period of our review.)

[50] After the end of our audit fieldwork, an FBI official stated that the FBI had formulated a more accurate problem response time tracking method.

Plans of Action and Milestones (POA&M)

A Plan of Action and Milestones (POA&M) is a management tool for correcting security weaknesses identified in an IT system. A POA&M details the resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. These plans are designed to be used by CIOs, program officials, and other agency employees responsible for tracking the progress of corrective actions. To ensure that POA&Ms contain the data necessary to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions, OMB issued guidance listing eight elements a POA&M should include for OMB-required reports. We reviewed the POA&Ms for two Sentinel environments to determine whether the POA&Ms contained the required reporting elements and data, and whether the FBI resolved the findings contained in the POA&Ms by the scheduled completion dates.[51] (See Appendix XIII for a list and description of OMB required reporting elements, and a description of the Sentinel Phase 1 (SP1) and Herndon Sentinel Secret System (HS3) environments.)

We determined that the HS3 POA&M did not meet the OMB reporting requirements. As shown in Table 10, the HS3 POA&M did not contain four of the eight required reporting elements. We believe that these were material omissions of reporting elements. If not monitored as prescribed by OMB, the HS3 POA&M findings and their associated risks could result in increased program cost or the extension of the program schedule.

[51] We reviewed the Herndon Secret Sentinel System (HS3), and Sentinel Phase 1 (SP1) environments. HS3 is the environment used for developing Sentinel. SP1 is the environment that houses the version of Sentinel accessible to Sentinel users.

TABLE 10: HS3 POA&M DATA ELEMENTS

OMB Required Data Element	Contained in current HS3 POA&M?
Type of Weakness	YES
Identity	YES
Estimated Funding Resources Required to Resolve the Weakness	MISSING
Scheduled Completion Date for Resolving the Weakness	YES
Key Milestones With Completion Dates	MISSING
Milestone Changes	MISSING
Source of Weakness	MISSING
Status	YES

Source: OIG analysis of FBI data

The Sentinel Information System Security Manager stated that based on our findings, two of the four missing reporting elements will be added to the next version of the HS3 POA&M: (1) estimated funding resources to resolve weaknesses and (2) milestone changes.

Similarly, we determined that the SP1 POA&M did not meet the OMB reporting requirements. As shown in Table 11, the SP1 POA&M did not contain four of the eight required reporting elements and we believe that these were material omissions. If not monitored as prescribed by OMB, these SP1 POA&M findings and their associated risks could result in breaches to Sentinel's security and damage to its infrastructure and the information contained within Sentinel.

TABLE 11: SP1 POA&M DATA ELEMENTS

OMB Required Data Element	Contained in First SP1 POA&M Reviewed?	Contained in Updated SP1 POA&M?
Type of Weakness	YES	YES
Identity	YES	YES
Estimated Funding Resources Required to Resolve the Weakness	MISSING	YES
Scheduled Completion Date for Resolving the Weakness	YES	YES
Key Milestones With Completion Dates	MISSING	MISSING
Milestone Changes	MISSING	YES
Source of Weakness	MISSING	MISSING
Status	YES	YES

Source: OIG analysis of FBI data

After our fieldwork had ended, the FBI provided an updated version of the SP1 POA&M.[52] As shown in Table 11, the updated version contained two of the four OMB required reporting elements that we previously identified and presented to the FBI as missing: (1) estimated funding resources to resolve weaknesses and (2) milestone changes.

The Information System Security Manager believed that the only reporting elements missing from the HS3 and SP1 POA&Ms were (1) estimated funding resources to resolve weaknesses and (2) milestone changes. He said the FBI Accreditation Unit, which is responsible for the FBI's POA&M template, had agreed to add these two elements to the FBI POA&M template. While we believe the FBI is taking important steps to ensure its POA&Ms meet OMB guidance, we noted that two OMB required reporting elements were still not included in the POA&M documents: (1) key milestones with completion dates and (2) source of weakness.

[52] SP1 is now referred to by the FBI as the Sentinel Production System (SPS). However, we refer to this environment by its previous name, SP1, throughout this report for consistency.

We also determined that the SP1 POA&M contains 20 open findings. The resolution of 11 of the 20 open findings is past due by an average of 152 days. We noted that 8 of the 11 overdue findings have not closed because they have not been validated by the FBI Certification Unit. When POA&M findings are not addressed in a timely manner, there is an increased risk of compromising Sentinel security. This could result in the degradation of Sentinel system performance or the compromise of the system's integrity, risking damage to the Sentinel infrastructure and data. In our judgment, the overdue POA&M findings are a significant condition because they are directly related to the Sentinel production environment which thousands of FBI employees rely upon to conduct their jobs.

In response to our findings, the Information System Security Manager stated that Lockheed Martin did not complete all of the security requirements scheduled for Phase 1, did not perform Sentinel's system security verification, and did not adhere to the schedule for correcting issues identified in the POA&Ms because Lockheed Martin did not have a Security Engineering Team. To avoid a similar situation during Phase 2, Lockheed Martin created a Security Engineering Team. Until Lockheed Martin could staff that team, Sentinel PMO personnel provided staff assistance to Lockheed Martin. According to the Information System Security Manager, Sentinel PMO personnel and the Lockheed Martin Security Engineering Team have the responsibility of monitoring completion of Sentinel security requirements by Lockheed Martin. We believe a fully staffed Lockheed Martin Security Engineering Team will enhance the FBI's ability to correct security issues on schedule.

Security Monitoring

The Systems Operations and Maintenance Manual contains a list of daily Sentinel system monitoring tasks assigned to the Security Administrator. It is the responsibility of the Security Administrator to maintain a daily checklist of his or her activities, and to report any findings to the Operations Manager and Information System Security Officer.

During our audit, we found that Lockheed Martin did not have a Security Administrator for Sentinel. The FBI's Information System Security Officer stated that he administered the required monitoring tasks instead of a Lockheed Martin Security Administrator. The Information System Security Officer said that every week he ensured that the system was properly audited and that the results were submitted to the Sentinel PMO.

Additionally, the Systems Operations and Maintenance Manual includes the Security Administrator Reporting Instructions, which serve as an instruction guide for the Security Administrator to obtain information related to conducting security audits and management of the Sentinel program. The instructions in this document are applicable to monitoring and audit reporting for software that comprises Sentinel.

In Phase 1, ACS remains the system of record for all automated case records and Sentinel has a limited amount of system and operational data that requires auditing. For Phase 1, Sentinel is responsible for auditing all security configurations, access, and account information as well as a subset of the functional data. The functional data audited in Phase 1 includes several COTS software components, database tables that contain sensitive information, and user query strings. A partial list of the associated reports includes:

- system privileges and modifications to user rights;
- attempts to access Sentinel using an incorrect role;
- new user accounts;
- stale and unused accounts; and
- unauthorized attempts to view, modify, or delete audit logs.

In February 2008, Lockheed Martin hired a Security Administrator. FBI personnel said that the Lockheed Martin Security Administrator would assume many of the system security monitoring duties currently being performed by the Information System Security Officer. The lack of a Security Administrator to execute required daily system monitoring tasks and meet the requirements of the Security Administrator Reporting Instructions represented a significant risk to Sentinel's system security. Without personnel to vigilantly monitor Sentinel's system security, Sentinel is vulnerable to undetected security breaches. This vulnerability increases the risk that Sentinel's production environment and sensitive data could be seriously damaged. We are pleased to see that this position has been filled.

Audit Reporting and Reduction Tools

There are several requirements in place for Lockheed Martin and the Sentinel PMO to manage, control, and prevent unauthorized or inadvertent

modifications to Sentinel as it is being developed. This includes requirements for an audit tool that can provide historical references of changes to the system as well as documenting user activity when system changes are made. The Sentinel audit tool supports aggregating, correlating, and reporting security related events and is used by FBI personnel to monitor the Sentinel production environment. The use of an integrated Sentinel auditing tool is an essential part of security management. The Information System Security Officer stated that, as of January 9, 2008, no major issues have been identified through the audits.

At the time of our audit, 3 of the 20 open findings in the SP1 POA&M related specifically to security audit reporting and security audit reduction. One of the three findings had a risk rating of "high", and the resolution of two of the findings was overdue by an average of 248 days.[53] The Information System Security Manager stated that Lockheed Martin provided a security audit reporting and reduction capability in Phase 1, and based on the SP1 audit reporting and reduction requirements and configuration of the tools, the FBI Accreditation Unit agreed to a validation process that would close the related POA&M finding with a "high" risk rating.[54] Additionally, Phase 2, Segment 2, Increment 10, scheduled for deployment in July 2008, will introduce additional audit reporting and reduction capabilities and toolsets. These toolsets will further augment and enhance audit reduction and reporting capabilities toward satisfying security audit requirements.

Conclusion

While the number of Sentinel users declined each month during the first 6 months of Sentinel's implementation, the Sentinel PMO has undertaken several efforts to better understand the decline in Sentinel usage, including what features Sentinel users would like to see in future releases of Sentinel. We agree with the Sentinel PMO's assessment that Phase 1's limited functionality has caused the decline and kept Sentinel from being more popular with FBI personnel. We also believe that the Sentinel PMO has taken significant steps to ensure that user input will help determine the order in which new features are added to Sentinel. While the 12 updated versions of Phase 1 addressed technical issues, they also helped address users' immediate needs for improvements to Sentinel. In our

---

[53] SP1 POA&M findings are each assigned a risk rating of "low," "medium," "high," or "very high".

[54] This POA&M finding is scheduled to be closed by May 9, 2008. The other two POA&M findings are awaiting FBI Certification Unit accreditation for closure.

judgment, the Sentinel PMO and Lockheed have implemented a structured method for determining the content of each update to Phase 1.

In addition to collecting user data, the FBI has also established performance measures to measure the technical performance of Sentinel, such as the percentage of time that Sentinel is functioning and available for use by FBI employees. However, we found that most of these metrics were applicable to measuring Sentinel's performance at the end of Phase 4. We believe that interim performance measures could be helpful in assessing issues of concern to Sentinel users.

Finally, we are concerned that the Sentinel PMO is not collecting all of the information required by the OMB for Sentinel's POA&M, and we believe that the FBI's POA&M template should be updated to conform to OMB's requirements.

Recommendations

We recommend that the FBI:

8. Amend the Measurement Plan to reflect the addition of Phase 1 System Specification CPM thresholds, and update the Measurement Plan as the CPM thresholds change in subsequent versions of the System Specification.

9. Update the POA&M template and all open POA&M findings on the HS3 and SP1 POA&Ms to include all of the reporting elements required by OMB.

FINDING 4: ACTIONS TAKEN ON PREVIOUS OIG RECOMMENDATIONS

The FBI generally has taken steps to resolve our concerns regarding the management of Sentinel and to address the 21 recommendations we made in previous Sentinel reports. Based on FBI actions, we have closed 16 of the 21 recommendations. The FBI agrees with the remaining five recommendations and is working on implementing them. For this review, we specifically followed up on the two recommendations that remained open from our most recent Sentinel report. We found that the FBI made significant progress in staffing the Sentinel PMO and that the Sentinel PMO implemented improved policies and procedures to ensure that all changes to the Bill of Materials (BOM) receive the required approval. However, we could not determine whether the FBI addressed our recommendation to create contingency plans and establish contingency triggers for highly rated risks because none of the current open risks met the FBI's threshold requiring such action. Nevertheless, we believe the FBI can improve its risk criterion and its categorization of risks, which would enhance the FBI's overall risk management as well as its contingency preparedness.

In our March 2006 report, *The Federal Bureau of Investigation's Pre-Acquisition Planning For And Controls Over the Sentinel Case Management System,* we made seven recommendations. We have closed four of these recommendations based on FBI improvements. The remaining three recommendations relate to the FBI's need to complete certain planning documents, the staffing of the Sentinel PMO, and Sentinel training. The FBI has made efforts to address these recommendations, including:

- continuing to work on completing its system security plan and completing its IV&V plan, which partially closes this recommendation;

- filling 77 of 79 positions within the Sentinel PMO, with 2 of the vacancies tentatively filled; and

- continuing to work on a comprehensive Sentinel 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. All five recommendations have been closed following FBI corrective action.

In our August 2007 report, *Sentinel Audit III: Status of the Federal Bureau of Investigation's Case Management System,* we made nine recommendations, seven of which have been closed. For the two open recommendations, we recommended that the FBI: (1) collect and report EVM data for both the performance measurement baseline approved at the integrated baseline review and the revised performance measurement baseline, and (2) develop and implement effectiveness measures for all risk mitigation plans.

In performing the fieldwork for our current audit, we found that the FBI was meeting the requirements in its revised Sentinel Risk Management Plan for the development of contingency plans and triggers. However, as discussed later in this finding, we continue to have concerns regarding the FBI's implementation of its Risk Management Plan. We will continue to monitor the FBI's implementation of its Risk Management Plan during future audit work.

Staffing

The Sentinel Program requires a highly skilled and integrated Sentinel PMO. The Sentinel Staffing Plan defines the staffing levels and skill needs of the Sentinel PMO for the Phase 1 contract award.

Due to the importance of the Sentinel PMO's oversight of Sentinel, we recommended in all three of our previous Sentinel audits that the Sentinel PMO complete hiring as soon as possible for the vacant Sentinel PMO positions. Since our August 2007 report, the number of planned positions increased from 76 to 78 positions in the Sentinel Staffing Plan.[55] The revised staffing plan also reallocated positions among units within the Sentinel PMO. At the time of our audit, the Sentinel PMO had two vacancies and was in the process of filling both positions.

As of January 2008 the Sentinel PMO Organization Chart identified 79 total planned Sentinel PMO staff, one more than the current staffing plan. In addition, as shown Table 12, the organization chart and staffing plan showed

[55] According to the Sentinel Staffing Plan V2R1 dated October 10, 2007.

different allocations of staff among the Sentinel PMO components. The Sentinel PMO Organization Chart lists two positions not required by the Sentinel PMO Staffing Plan and eliminates one position included in the Sentinel PMO Staffing Plan resulting in the addition of one position. According to the Sentinel Staffing Plan, the plan will be updated, as required, to reflect changes in the Sentinel PMO staff's roles and responsibilities.

TABLE 12: SENTINEL PMO STAFFING REQUIREMENTS

Organizational Units	PMO Staffing Plan	PMO Org Chart	Difference
Program Leadership	3	3	0
Direct Reporting Staff	8	7	-1
Systems Development	25	26	+1
Operations and Maintenance	4	4	0
Training and Communications	8	8	0
User Representation and Policy	12	12	0
Program Support	18	19	+1
Total	**78**	**79**	**+1**

Source: FBI

We believe that the Sentinel PMO Organization Chart should accurately reflect the Sentinel PMO Staffing Plan and that the staffing plan should be updated whenever there is a need to add or reallocate Sentinel PMO personnel. Without an organization chart that matches the Sentinel PMO Staffing Plan, it is impossible to determine the number of vacancies at the Sentinel PMO. The Chief of the Program Support Unit said that the Sentinel PMO updates the staffing plan annually or after significant changes to the Sentinel PMO's staffing level.

As of January 2008, the Sentinel PMO had on board 77 of the 79 of the personnel identified in the FBI's Sentinel PMO Organization Chart.[56] Table 13 summarizes the Sentinel PMO's staffing level as of January 2008 and shows the progress the FBI has made in fully staffing the Sentinel PMO

[56] We used the Sentinel PMO Organization Chart to determine the planned and actual staffing levels because, at the time of our audit, the Sentinel Staffing Plan did not reflect the staffing changes at the Sentinel PMO.

since May 2007. (For a more complete description of Sentinel PMO staff and their duties, see Appendix XIV.)

TABLE 13: SENTINEL PMO STAFF ON BOARD

Organizational Units	Staff on Board, May 2007	Staff on Board, January 2008
Program Leadership [a]	10	3
Direct Reporting Staff		7
Systems Development	28	26
Operations & Maintenance	3	4
Training & Communications [b]	5	7
User Representation & Policy [b]	4	11
Program Support [c]	20	19
Total [d]	70 (76)	77 (79)

Source: FBI

Notes:

(a) In our August 2007 report, we identified Program Leadership and the Direct Reporting Staff jointly as the Sentinel PMO Front Office.
(b) Since our August 2007 report, the Training and Communications Unit has replaced the Transition Unit, and the User Representation and Policy Unit has replaced the Organizational Change Management Unit.
(c) Since our August 2007 report, the Program Support Unit has replaced the Business Management Unit and the Program Integration Unit.
(d) The number in parentheses is the total planned staff. As noted previously, the number and allocation of planned staff in the current Sentinel Staffing Plan and the current Sentinel PMO Organization Chart vary. For the planned level of staffing in January 2008, we used data from the Sentinel PMO Organization Chart. In January 2008, the PMO had 77 staff on board and 2 vacancies, for a total of 79 positions.

As shown in the previous table, as of January 2008 the Sentinel PMO had two vacancies, a SSA and an Intelligence Support Specialist (ISS), both of which are government employee positions. An FBI official said the vacant SSA position had not been filled because the position was not authorized until November 2007. According to the FBI, an agent was scheduled to fill this position at the end of March 2008. The vacant ISS position is a temporary duty position, typically filled by an ISS from a field office who serves in the Sentinel PMO for approximately 1 year and then returns to the

field office. The ISS position had been filled until January 2008, at which time the ISS's temporary assignment ended.

Since May 2007, the Sentinel PMO has made significant progress in fully staffing the Sentinel PMO, and we believe that neither of the two current vacancies is critical to the immediate operation of the Sentinel PMO. However, we will continue to monitor staffing levels of the PMO in our future reports.

Bill of Materials

In our August 2007 report, *Sentinel Audit III: Status of the Federal Bureau of Investigation's Case Management System,* we recommended that the FBI: (1) implement policies and procedures to ensure that all changes to the BOM receive proper authorization and that the changes can be reconciled to the BOM submitted in Lockheed Martin's proposal; and (2) implement policies and procedures to ensure that materials contained in Lockheed Martin invoices can be reconciled to the BOM or an FBI approval for a change to the BOM.

Since our previous audit, the Sentinel PMO has revised its BOM Deviation Policy. Now all BOM changes, additions, and deletions must be documented and submitted by Lockheed Martin to the Contracting Officer's Technical Representative (COTR) using the Sentinel BOM Deviation Approval Submission Form. The form must clearly identify the BOM item in question and any change to the cost, model, or schedule. No purchases or changes can be made to the BOM until the form has all the necessary approval signatures and the request is received and approved by the COTR.[57] The COTR stated that these revised policies will help increase the amount of management control the FBI has over the Sentinel BOM.[58] Lockheed Martin invoiced material is matched against the BOM to verify that Lockheed Martin only purchased equipment for which they had authorization.

---

[57] Prior to delivery to the COTR, the BOM Deviation Approval Submission must be signed by representatives of Lockheed Martin's Engineering Review Board, Configuration Control Board, and finance office as well as representatives from the Sentinel PMO's Engineering Review Board, Configuration Control Board, and finance office. The COTR is the final approval official for all submissions.

[58] The revised policies are the BOM Deviation Policy and the Invoice Policy and Procedure.

According to the Sentinel PMO Auditor, this process incorporates the BOM Deviation and Change Policy and Procedures. Authorization of BOM changes must come from the Sentinel PMO Program Manager and COTR. This process also serves to notify Sentinel PMO management whether BOM deviations or engineering changes are within targeted PMO budget limits since cost impact is also reviewed by the Sentinel PMO cost analyst. The Sentinel PMO budget analyst and EVM personnel are also kept informed as part of the BOM change management process. We verified that the Sentinel PMO is implementing many of its new control processes by observing the Sentinel PMO auditor as he reviewed documentation supporting charges on Lockheed Martin invoices, independently calculated the amount of the invoices, and matched material in Lockheed Martin invoices to the current version of the BOM to verify that Lockheed Martin was authorized to purchase equipment. We believe that the FBI has significantly improved its control over changes to the BOM and that these improved controls should provide the FBI with greater control over Sentinel's cost.

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 with the assistance of a Risk Review Board (RRB).[59] The most significant risks identified by the board are examined at monthly Program Management Review sessions and other Sentinel oversight meetings in accordance with the FBI's LCMD.[60]

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

---

[59] According to the Sentinel Risk Management Plan, the Sentinel Risk Review Board will include the following Sentinel representatives: 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.

[60] In addition to the risk management processes cited above, the following individuals 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).

the life of the program. In addition to documenting the risk management approach, which is described below, the plan specifies:

- the risk process;
- the roles and responsibilities of the Program Manager, the PMO team, and development contractors;
- how risks should be tracked throughout the project lifecycle;
- how mitigation and contingency plans are implemented;
- executive level risk reporting; and
- the relationship between the Risk Management Plan and Lockheed Martin's Risk/Opportunity Management Plan (ROMP).

Risk Management Approach

Anybody involved with the management or oversight of Sentinel may identify a potential risk that Sentinel may encounter.[61] Any risks generated by persons outside of the PMO are communicated to Sentinel PMO management or the Sentinel PMO risk coordinator. Sentinel PMO personnel enter all proposed risks into a Risk Review Database. The relevant Sentinel PMO unit chief or the unit's designated risk lead then reviews the proposed risks. The unit chief or risk lead can either accept the proposed risk as submitted, request more information from the submitting stakeholder, or request additional assistance from Sentinel PMO personnel with more expertise in the risk area. Once a Unit Chief accepts a proposed risk, the Risk Coordinator forwards the proposed risk to the RRB.[62] The Program Manager, who chairs the RRB, in consultation with the entire RRB, can accept the risk, reject the risk, or defer the risk to a subsequent RRB meeting, asking that the submitting stakeholder refine the risk and better evaluate how to mitigate the risk.

---

[61] Stakeholders include the Sentinel PMO, the FBI, Lockheed Martin, and other law enforcement personnel.

[62] Risks submitted by Deputy Program Managers do not require a unit chief's review before being presented to the RRB.

Once the RRB Chair accepts a risk, he assigns the risk to a Risk Owner. The Risk Owner is responsible for developing detailed mitigation plans, contingency plans and triggers, and assessments for assigned risks. If needed, a Risk Owner may form a working group to assist with these tasks. The RRB uses the plans developed by the Risk Owner or working group to assign an "impact severity" and "probability of occurrence" rating to each risk.[63] The RRB can assign one of four ratings to risk for impact severity and probability of occurrence: (1) Very High, (2) High, (3) Medium, and (4) Low. Based on those two ratings, the RRB then computes the Risk Exposure rating for the risk, which is used to prioritize each risk. (See Appendix XVI for the Risk Exposure Matrix.)

Once the open designation is assigned to a risk, it is given a tracking number by the RRB and then analyzed and updated by the Risk Owner and working groups. Open risks are also ranked by the RRB so that the highest priority risks get immediate attention. Recommendations are brought to the RRB by the working group for review and approval. Throughout the life of the risk, the Risk Owner and the associated working group provides updates to the RRB and, if required, executes contingency plans and contingency triggers. In our August 2007 report, we expressed concern that personnel assigned to manage risks may not have sufficient time or expertise to adequately develop and implement a strategy to reduce Sentinel risks. With the implementation of the revised Risk Management Plan involving Risk Owners and working groups, we believe that the FBI has taken meaningful steps to alleviate our concern.

Risk Tracking

Sentinel risks are tracked throughout the life of the program. Once risks have been identified and assessed, as described above, they are reviewed, categorized, revised, and potentially closed during the RRB meetings.

Risks accepted by the RRB are tracked in a risk register, which includes the following data elements:

- description of the risk,
- impact on the program should the risk occur,

[63] See Appendix XVI for a description of the matrices and guidance used by the RRB to assign impact severity and probability of occurrence ratings to each open risk.

- phase of Sentinel affected by the risk,
- person responsible for managing the risk,
- OMB risk category,
- severity of the risk as rated by the RRB,
- probability the risk will occur as rated by the RRB,
- strategy to mitigate the risk,
- risk status,
- contingency trigger, and
- contingency plan.

The risk register identifies open risks in rank order based on the risk exposure level as designated by the FBI. As of March 2008, the FBI had identified and was managing three open risks to the Sentinel program. These risks are listed below from highest to lowest in order of importance, as ranked by the RRB and adjudicated by the Sentinel PMO Program Manager.

- If the FOC architecture does not contain a sufficient level of detail by the beginning of Phase 2, Segment 3, then Phase 2, Segment 3 development efforts may be adversely affected.
- The data migration complexity from phased-out legacy systems may have been underestimated, therefore some data may be lost, compromised, or the FBI may not be able to retire the ACS system if the issue cannot be resolved prior to starting Segment 4.
- Current deployment of FBI initiatives, including Enterprise Directory Service and Public Key Infrastructure on which Sentinel is dependent do not support the revised roadmap.

A risk mitigation strategy is a list of and schedule for all tasks required to fully mitigate the risk. Risk mitigation strategies may include the following information:

- description of the mitigation activity,

- schedule of activities with completion dates, and
- completion of mitigation activities.

The Sentinel Risk Management Plan, which was revised in November 2007, requires the FBI to develop mitigation strategies for all open risks. The revised plan requires contingency plans and contingency triggers for open risks that have a risk exposure rating of "high" or "very high." The contingency plans must identify what actions will be taken when a specific trigger event occurs. Contingency triggers and plans are formulated by the Risk Owner and the related working group, and are recorded, reviewed, and revised by the RRB. As of March 2008, the FBI developed mitigation strategies for all three of its open risks, as required by the Risk Management Plan. None of these risks were rated "high" or "very high" and, therefore, did not require contingency plans or triggers.[64]

We reviewed the risk registers generated by the RRB beginning in October 2007. Table 14, below, shows the number of open risks by risk register.

[64] Contingency plans indicate the actions that should be performed when a specific "trigger" event occurs. A trigger is identified as a specific date, cost or schedule threshold, or pre-defined risk condition. Although it was not required, one risk had both a contingency trigger and a contingency plan.

TABLE 14: OPEN RISKS BY RISK REGISTER

Risk Register Date	Number of Open Risks
10/25/07	18
11/08/07	18
11/21/07	10
12/06/07	9
1/10/08	7
1/17/08	7
1/31/08	6
2/14/08	6
2/28/08	6
3/13/08	5
3/27/08	3

Source: FBI

As shown in the table above, the number of open risks recorded in the Sentinel risk registers during the period of our review decreased significantly over time. Although we believe the Sentinel PMO is following its risk tracking procedures, we are concerned about the relatively low number of open risks – particularly because we believe that Phase 2 is the most challenging of the remaining phases. For example, Phase 2 is scheduled to deliver more requirements than either Phases 3 or 4. We attribute the decrease in the number of open risks to the criterion contained in the revised Risk Management Plan, which went into effect in November 2007. As Table 14 shows, the significant decline in the number of open risks began after the Risk Management Plan was revised.

The specific change to the Risk Management Plan that we believe caused the decline in the number of open risks is the criterion for a risk. According to the revised Risk Management Plan, a risk will only be tracked in the risk register if the RRB determines the risk will have a 10 percent or greater variance in the program's cost or schedule. This 10 percent threshold correlates to a risk exposure of "high" or greater.[65] Given that Sentinel is critical to the FBI's mission, we believe this variance threshold is too high and are concerned that a large number of potential risks are not being actively managed as a result.

[65] Risk exposure is the product of total loss if a risk occurs multiplied by the probability that a risk will occur.

The Sentinel Program Manager agreed that the program was not actively managing enough risks. He attributed the relatively low number of risks on the risk registers to an attitude among Sentinel PMO personnel that views a high number of open risks as reflecting negatively on the management of the program. The previous version of the Sentinel risk management plan required the Sentinel PMO to develop a "contingency trigger" and a contingency plan for each risk the Risk Review Board rated as having a probability or severity rated as medium or higher. We recommend that the FBI revise the Sentinel Risk Management Plan to use the risk criteria contained in Version 1 of the Risk Management Plan.

Risk Closure

There are several conditions under which a risk may be closed. Under one condition, the RRB Chair agrees that the mitigation plans have been successfully completed and then the Sentinel PMO identifies the risk as 'closed-complete.' Under a second condition, risks are closed and tagged as 'watch' items after closure. Watch items are periodically reviewed by the RRB to prevent recurrence of a risk in future phases. A risk may also be closed if it developed into an 'issue.' An issue is a risk that has a 100 percent possibility of occurring or is presently occurring at the time of assessment. Open risks that are classified as issues are marked by Sentinel PMO personnel as 'closed' in the risk tracking database and tracked separately. As of March 2008, the risk register contained 41 closed risks. Of these 41 closed risks, 14 were classified as issues, 5 were marked as watch items, and 22 were closed. In our previous report, we had recommended that the Sentinel PMO track issues separately. During this audit, we found that it was doing so.

Conclusion

The FBI has a broad range of management controls and processes that aid it in managing the development of Sentinel. In our past 3 audits of the Sentinel Program, we made a total of 21 recommendations aimed at strengthening those controls. To date, the FBI has addressed 16 of these 21 recommendations and agrees with the remaining 5 recommendations.

During this audit, we examined the progress the FBI has made in implementing our recommendations in three specific areas: staffing the Sentinel PMO, controlling changes to the BOM, and managing risk. Sentinel PMO staffing has reached a level sufficient to close our recommendation that the FBI fully staff the Sentinel PMO. Similarly, the FBI has instituted new policies and procedures that, based on our testing, improved the FBI's

control over changes to the BOM, giving the FBI better control over the cost of Sentinel. However, we could not determine whether the FBI had instituted our recommendation on contingency plans and contingency triggers for highly rated risks because none of the risks the FBI was tracking met the criteria requiring contingency plans or triggers. In our judgment, the revised Sentinel Risk Management Plan increases the threshold for what constitutes a highly ranked risk to the point where very few, if any, risks will need a contingency plan or trigger. In our judgment, the FBI should reevaluate its revised Risk Management Plan and lower the thresholds for identifying a risk to enhance the Sentinel's overall risk management as well as its contingency preparedness.

Recommendation

We recommend that the FBI:

10. Revise the Sentinel Risk Management Plan to use the risk criteria contained in Version 1 of the Risk Management Plan.

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, Memorandum M-02-01, 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),
- Department of Justice Order 2880.1b,
- FBI Life Cycle Management Directive,
- Department of Defense Program Manager's Guide to the Integrated Baseline Review Process,
- 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 one area where the FBI was not in compliance with the laws and regulations referred to in OMB Memorandum M-02-01 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. As discussed in the Findings and Recommendations section of this report, we found the following internal control deficiencies.

- The FBI POA&M template does not meet OMB reporting requirements.
- The Phase 2 integrated master schedule has not been developed.
- The FOC architecture, which tells engineers what end state to build to, has not been completed.
- Sentinel's use of its EVM system differs drastically from its EVM System Description.

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

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to: (1) determine if Phase 1 of the Sentinel project met technical and performance expectations; (2) evaluate the FBI's planning for and implementation of Phase 2 of the Sentinel project, including cost and schedule performance; and (3) assess the FBI's progress in resolving concerns identified in the OIG's previous Sentinel audits.

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 the 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, and the Department of Justice. We also interviewed officials from contractors supporting the Sentinel 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. We obtained from the FBI, and used in our report computer-processed data related to the requirements distribution, by phase, and the number of unique Sentinel and ACS users. We used the data for informational purposes. Therefore, we did not verify its accuracy.

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, post-Phase 1 activity, and planning and progress toward completion of Phase 2. Additionally, we interviewed FBI officials responsible for contract implementation.

To update issues identified in the OIG's August 2007 Sentinel audit report, we interviewed responsible FBI and contractor officials

and reviewed plans and procedures for cost tracking, risk management, contingency planning, IV&V, Sentinel PMO staffing. We also reviewed, management of the Bill of Materials, Phase 1 schedule, cost, and performance, and Phase 2 planning and management. We also interviewed FBI officials and obtained the updated status on issues relating to EVM.

APPENDIX II

ACRONYMS

ACS	Automated Case Support
BOM	Bill of Materials
BPR	Business Process Reengineering
CIO	Chief Information Officer
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off The Shelf
CPM	Critical Performance Measure
CPU	Central Processing Unit
DIRB	Department Investment Review Board
Department	Department of Justice
DR	Defect Report
EVM	Earned Value Management
FBI	Federal Bureau of Investigation
FOC	Full Operating Capability
FY	Fiscal Year
GAO	Government Accountability Office
HS3	Herndon Secret Sentinel System
IBR	Integrated Baseline Review
IT	Information Technology
IV&V	Independent Verification and Validation
JEB	Joint Engineering Board
LCMD	Life Cycle Management Directive
O&M	Operations and Maintenance
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PMO	Program Management Office
POA&M	Plans of Action and Milestones
RMA	Records Management Application
SAC	Special Agent In Charge
SP1	Sentinel Phase 1
SRS	System Requirements Specifications
SS	System Specification
SST	Support Services Technician
UNI	Universal Index
VCF	Virtual Case File

APPENDIX III

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 through many of the life cycle phases, control gate reviews, and project level reviews multiple times.

Phases

The LCMD 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 and 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 needs, 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 complete system testing of the entire system once completed.
6. Development and Test	Produces and tests all system components, assembles and tests all products, and plans for system testing.
7. Implementation and Integration	Executes functional, interface, system, and integration testing; provides user training; and accepts and transitions the product to operations.
8. Operations and Maintenance	Maintains and supports the product, and manages and implements necessary modifications.
9. Disposal	Shuts down the system operations and arranges for the orderly disposition of system assets.

Source: FBI

FBI LCMD CONTROL GATE REVIEWS

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

Source: FBI

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 three FBI IT Decision Boards 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).

- 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.

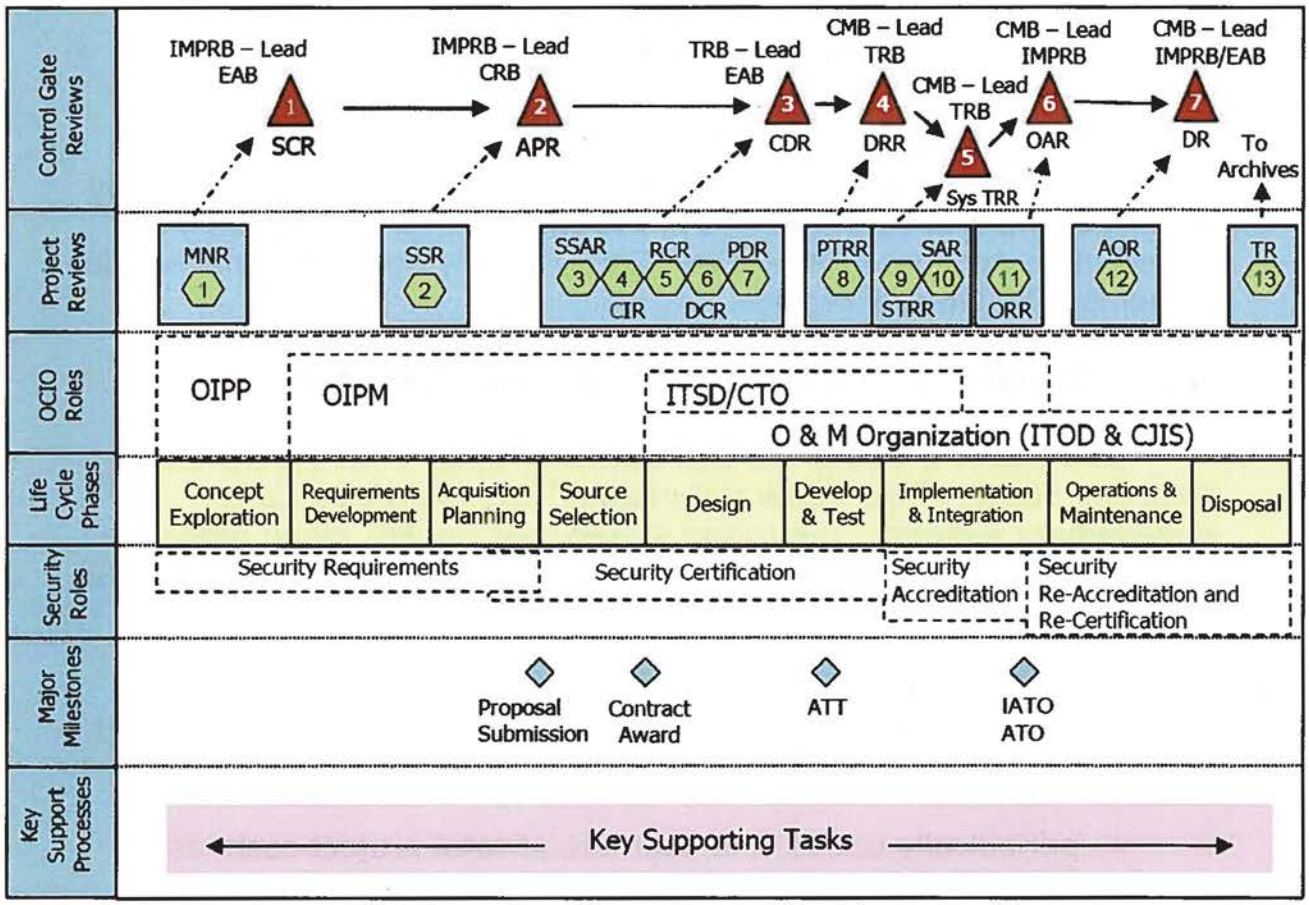
PROJECT LEVEL REVIEWS

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.

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.

Source: FBI

FBI'S LCMD IT SYSTEMS LIFE CYCLE



LEGEND

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

APPENDIX IV

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:

- 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 Management Project*, which encompassed Sentinel's predecessor, the Virtual Case File (VCF). The OIG recommended the FBI take the following steps:

- Replace the obsolete ACS system as quickly and as cost effectively as feasible.
- Reprogram FBI resources to meet the critical need for a functional case management system.
- Freeze the critical design requirements for the case management system before initiating a new contract and ensure that the contractor fully understands the requirements and has the capability to meet them.

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

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

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

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

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

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

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

External Reports on FBI Case Management Efforts

In 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.[66] 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

[66] 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.

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 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 May 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 unallowable costs. These costs included first-class travel and other excessive airfare costs, incorrect charges for overtime hours, and charges for which the contractors could not document costs incurred. The GAO found unsupported and questionable costs in the amount of $10 million. The GAO also found that the FBI failed to establish controls to maintain accountability over equipment purchased for the Trilogy project. According to the GAO, poor property management led to 1,200 missing pieces of equipment valued at $7.6 million.

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 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 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 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.

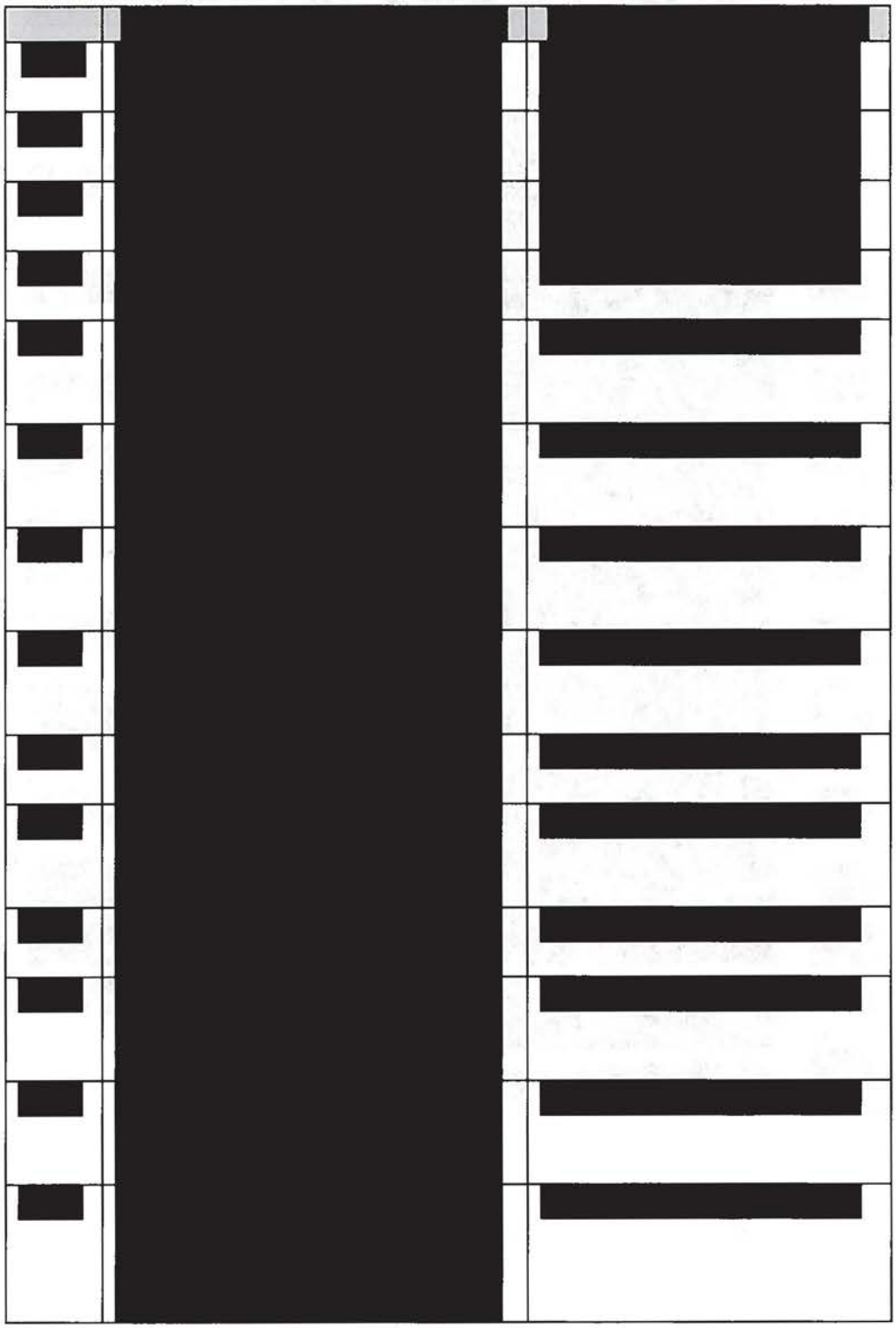
In December 2002, the OIG issued a report on *The FBI's Management of Information Technology Investments*, which included a case study of the Trilogy project. The report made 30 recommendations, 8 of which addressed the Trilogy project. The report's focus was on the need to adopt sound investment management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

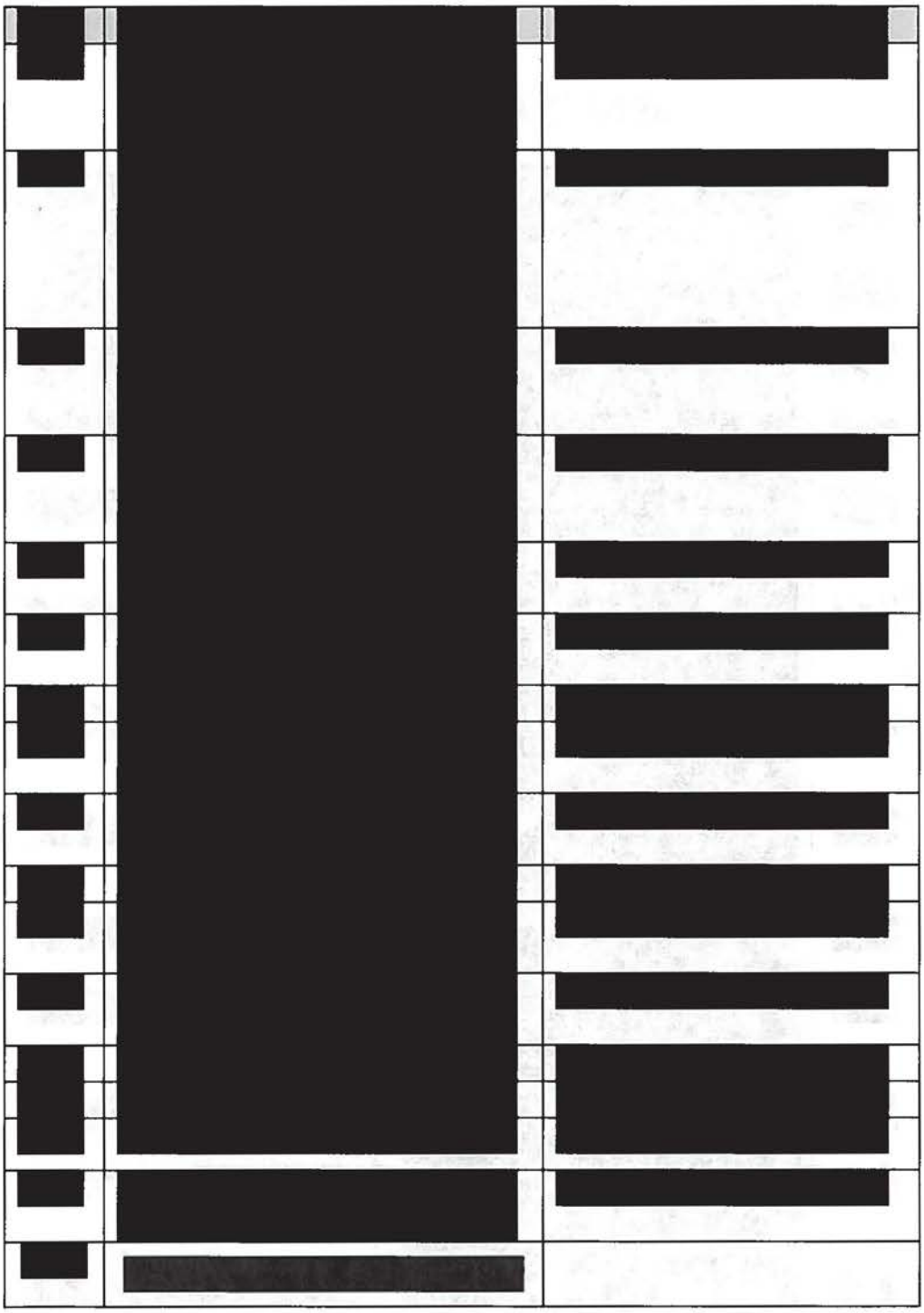
- defining and developing IT investment boards,
- following a disciplined process of tracking and overseeing each project's cost and schedule milestones over time,
- identifying existing IT systems and projects,
- identifying the business needs for each IT project, and
- using defined processes to select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

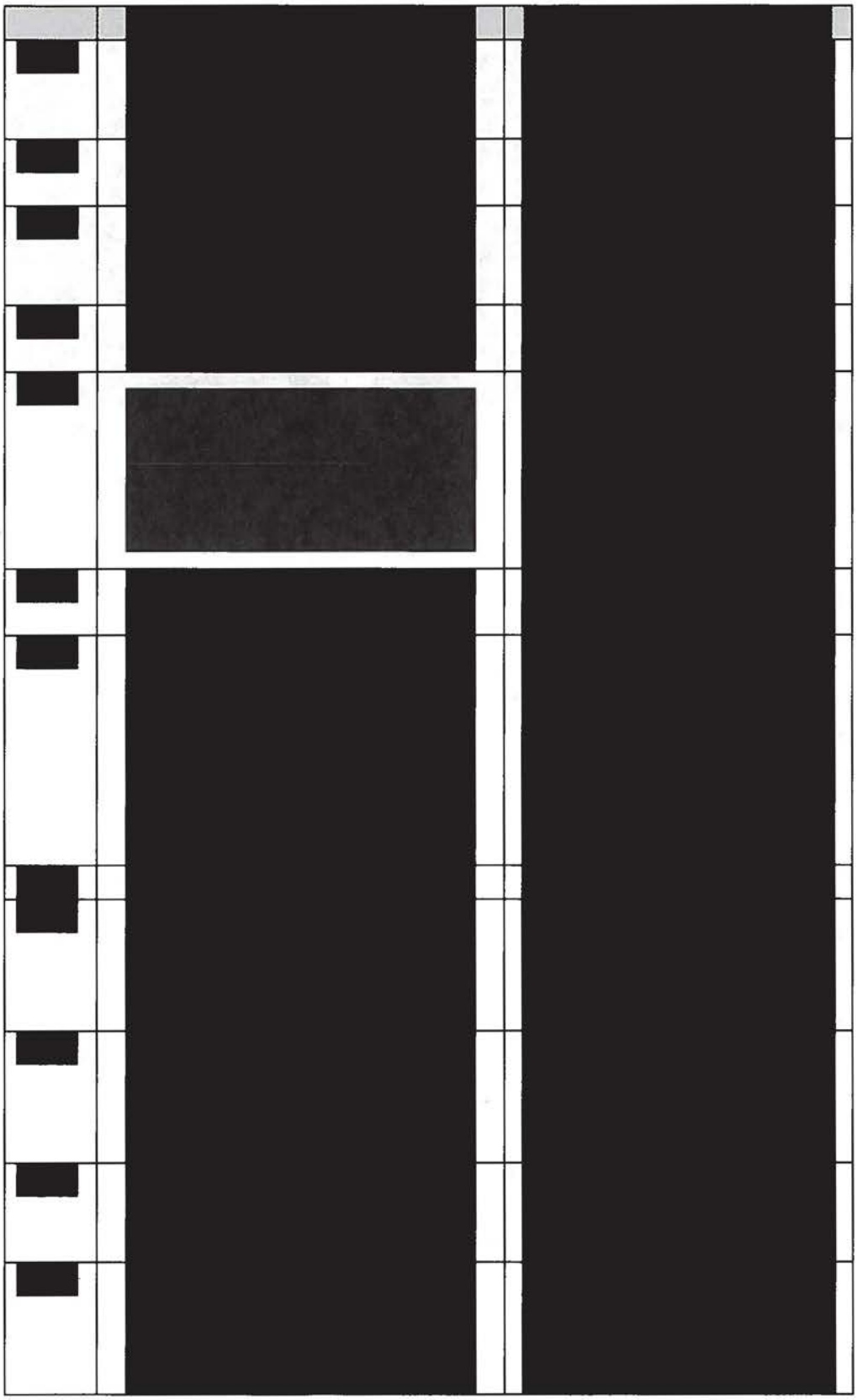
The audit found that the lack of critical IT investment management processes for Trilogy contributed to missed milestones and led to uncertainties about cost, schedule, and technical goals.

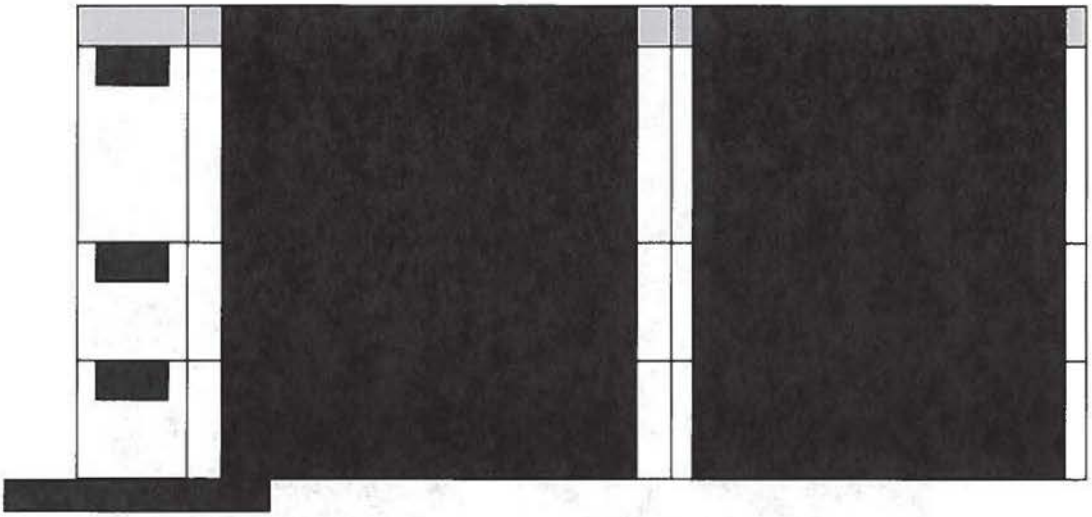
APPENDIX V

SENTINEL INTERFACES









APPENDIX VI

SENTINEL PLANNED SUBSUMED SYSTEMS

1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]
5	[redacted]		[redacted]
6	[redacted]		[redacted]

	[redacted]	[redacted]	[redacted]
7	[redacted]		[redacted]
8	[redacted]	[redacted]	[redacted]
9	[redacted]	[redacted]	[redacted]

Source: FBI

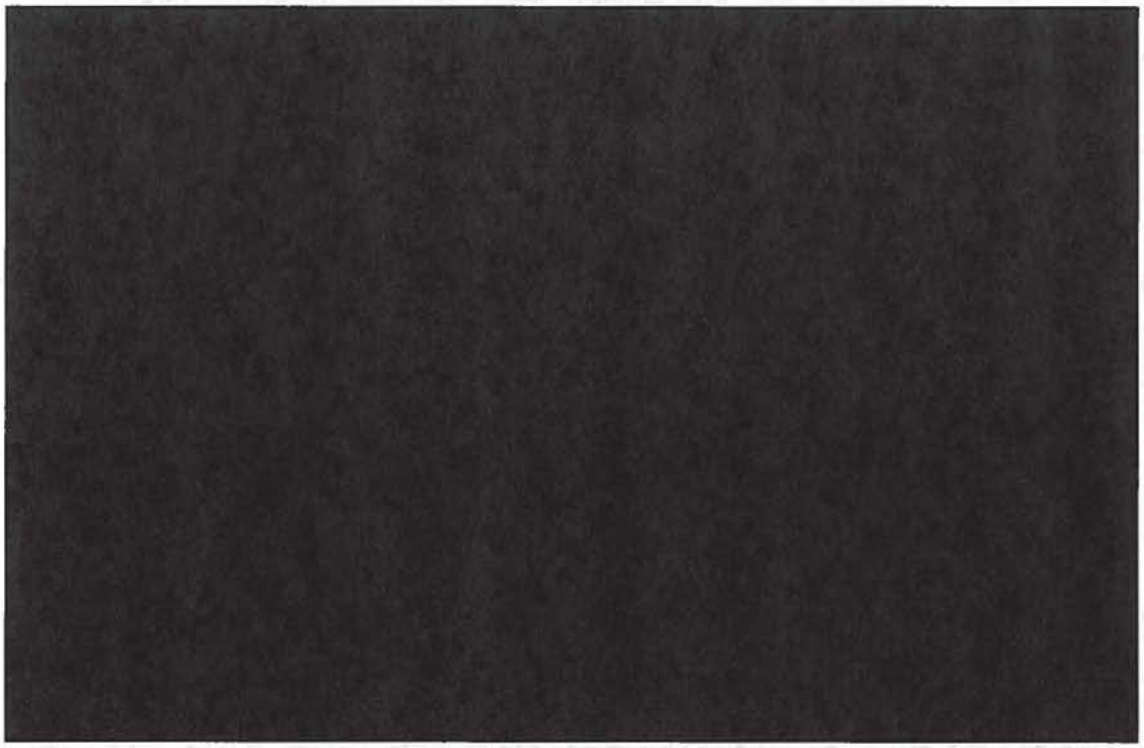
APPENDIX VII

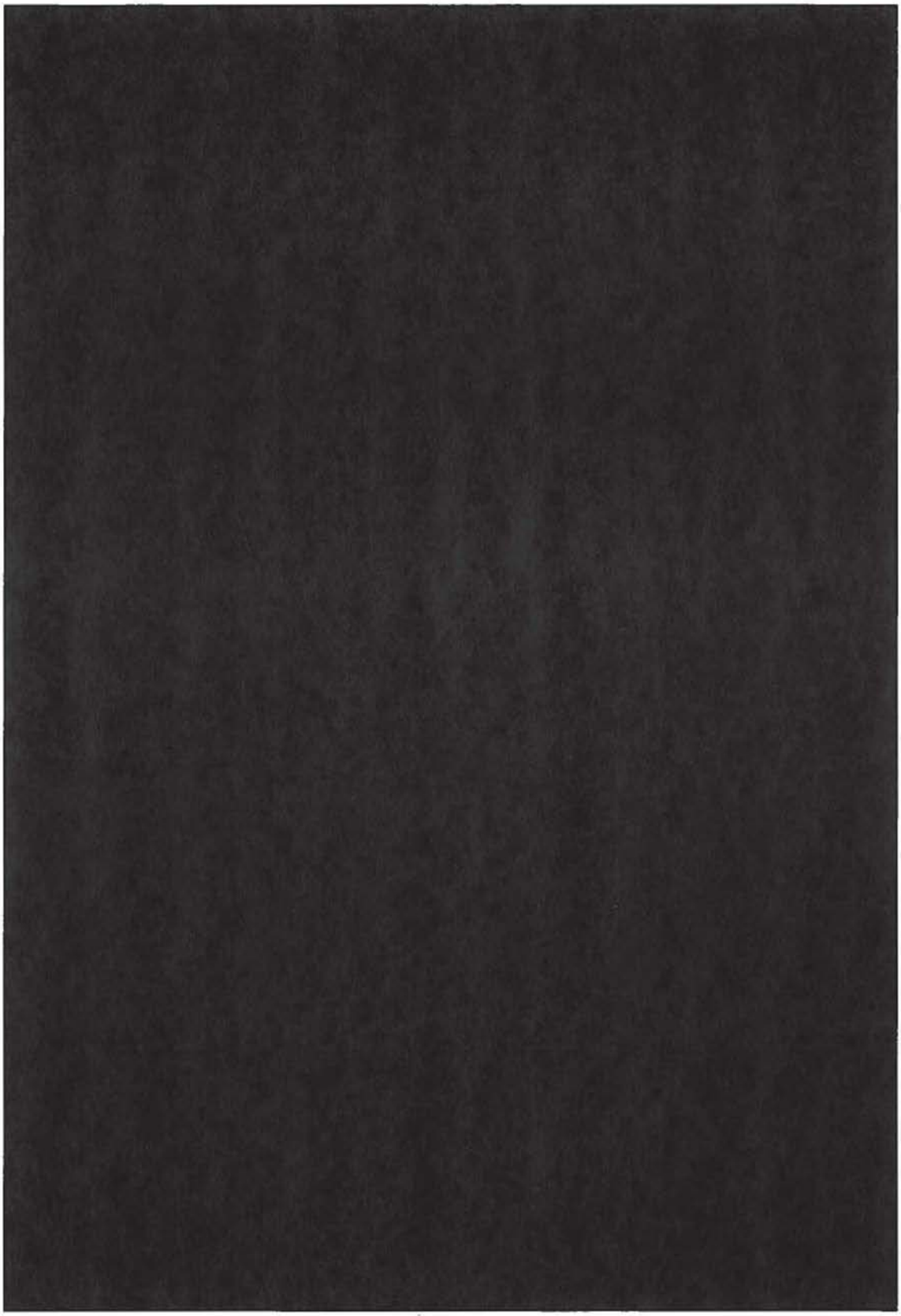
INDEPENDENT VERIFICATION AND VALIDATION ISSUES AND RECOMMENDATIONS

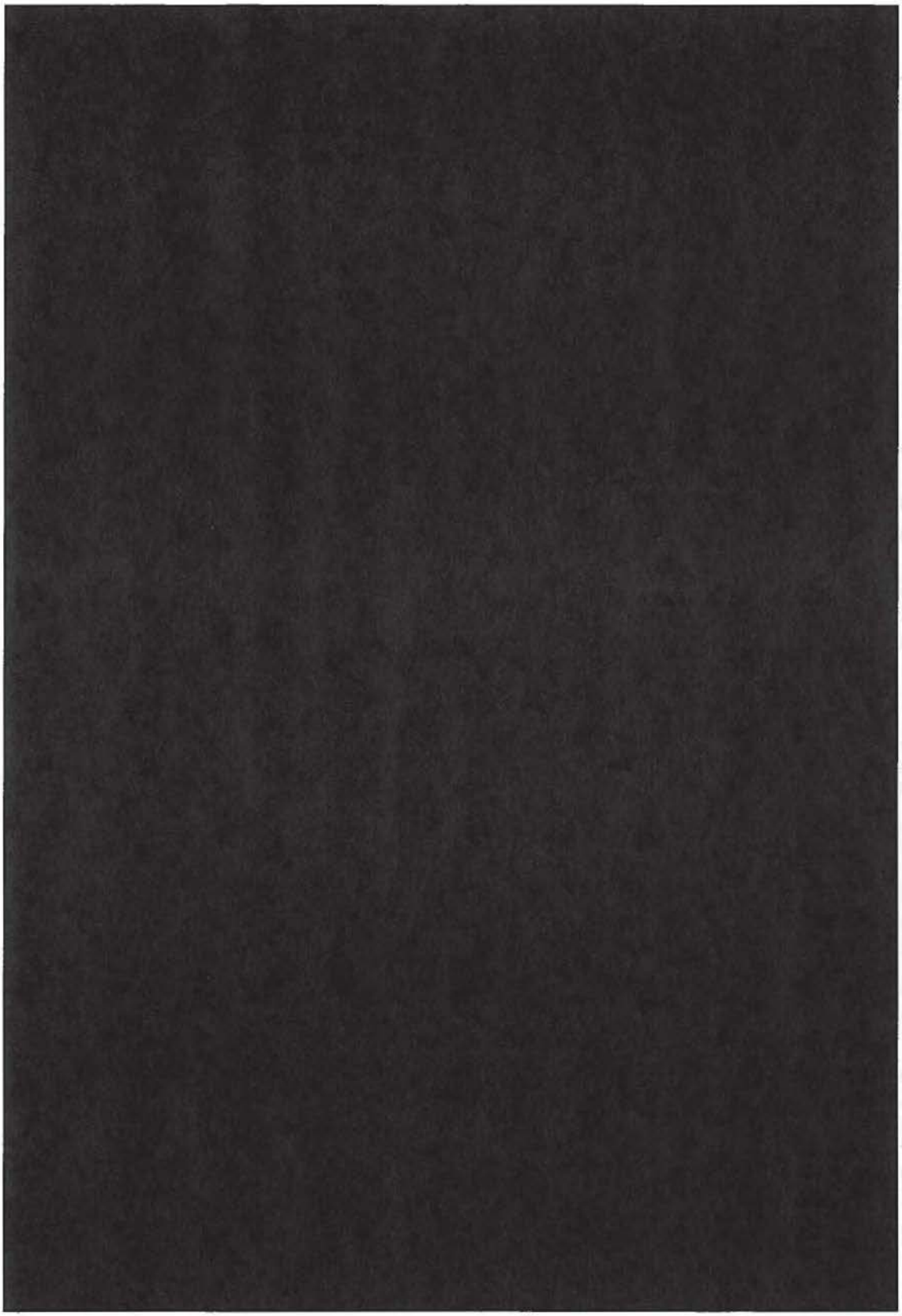
Phase 1 Operations and Maintenance and Phase 2

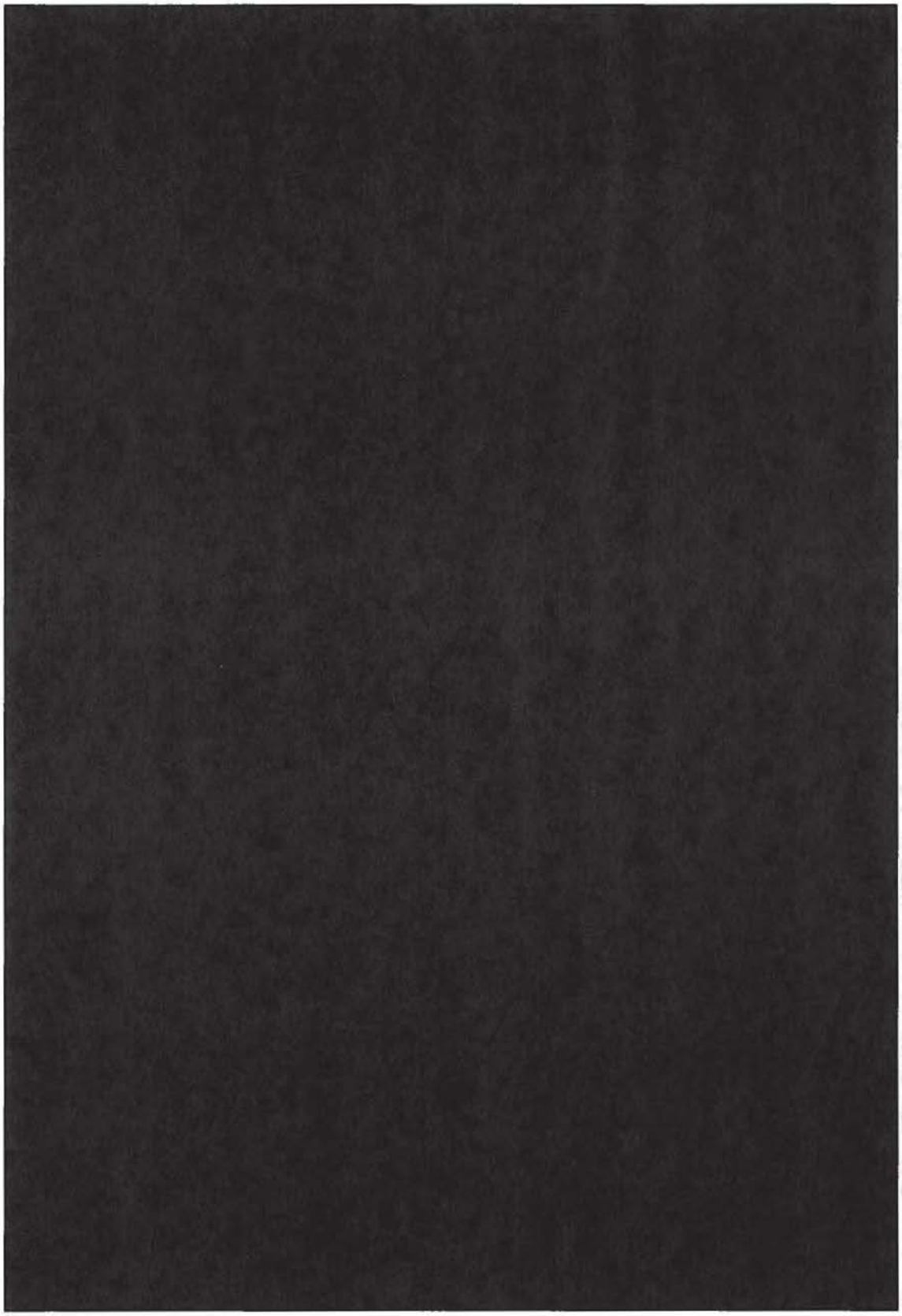
According to the IV&V contractor, a recommendation can have a status of: (1) open – a recommendation that has not been acted upon by the Sentinel Team; (2) inactive – a closed recommendation that the Sentinel Team has chosen not to implement; and (3) implemented – a closed recommendation that the Sentinel Team has executed the recommended action; (4) a closed recommendation indicates that the IV&V contractor no longer reported the recommendation as active but did not specify whether it was closed by implementation or by becoming inactive. Some recommendations have been closed because the issue or risk has been eliminated as a certain stage of the project has passed or the IV&V contractor identified another means that minimized or eliminated the issue of concern.

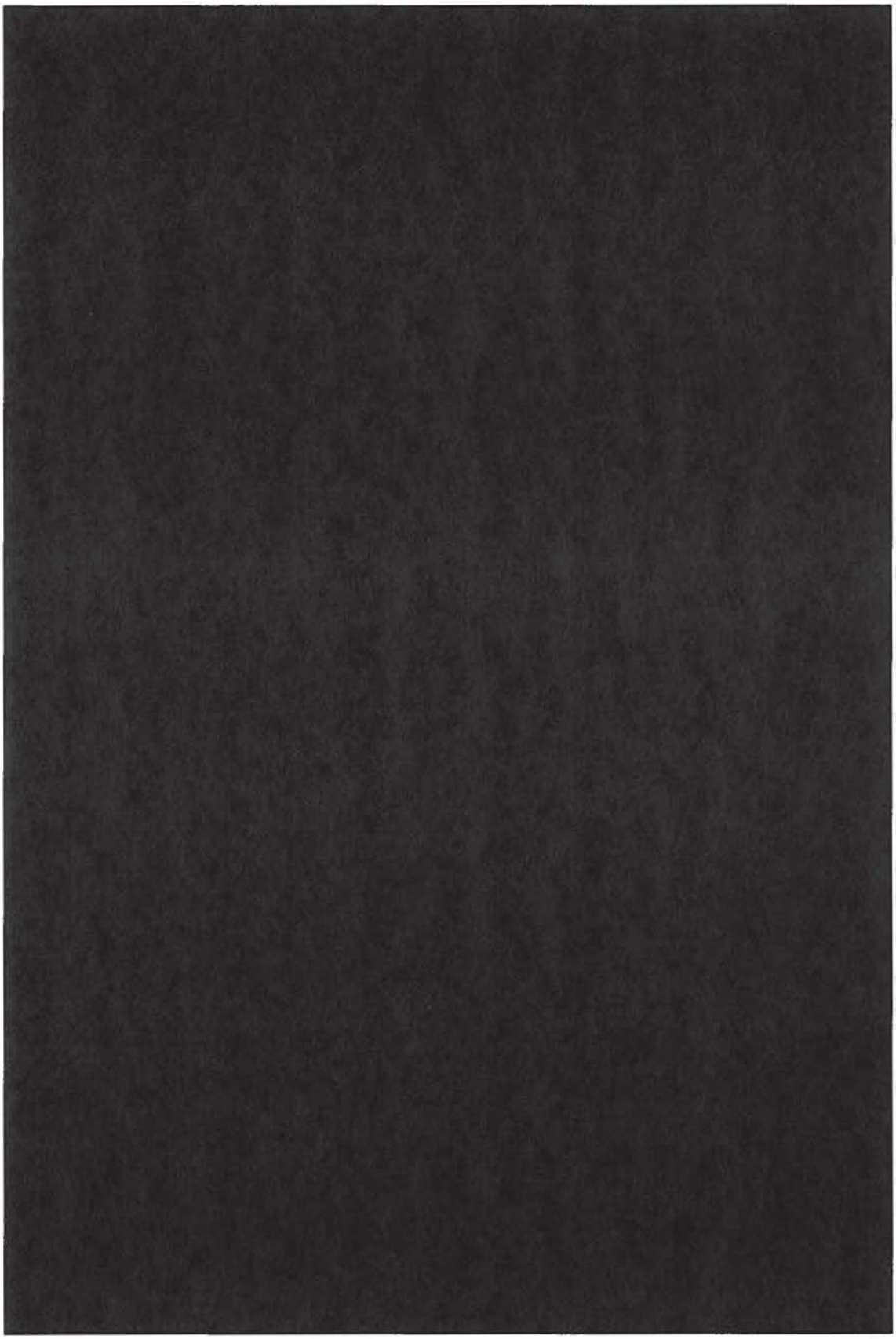
IV& V IDENTIFIED RISKS AND ISSUES

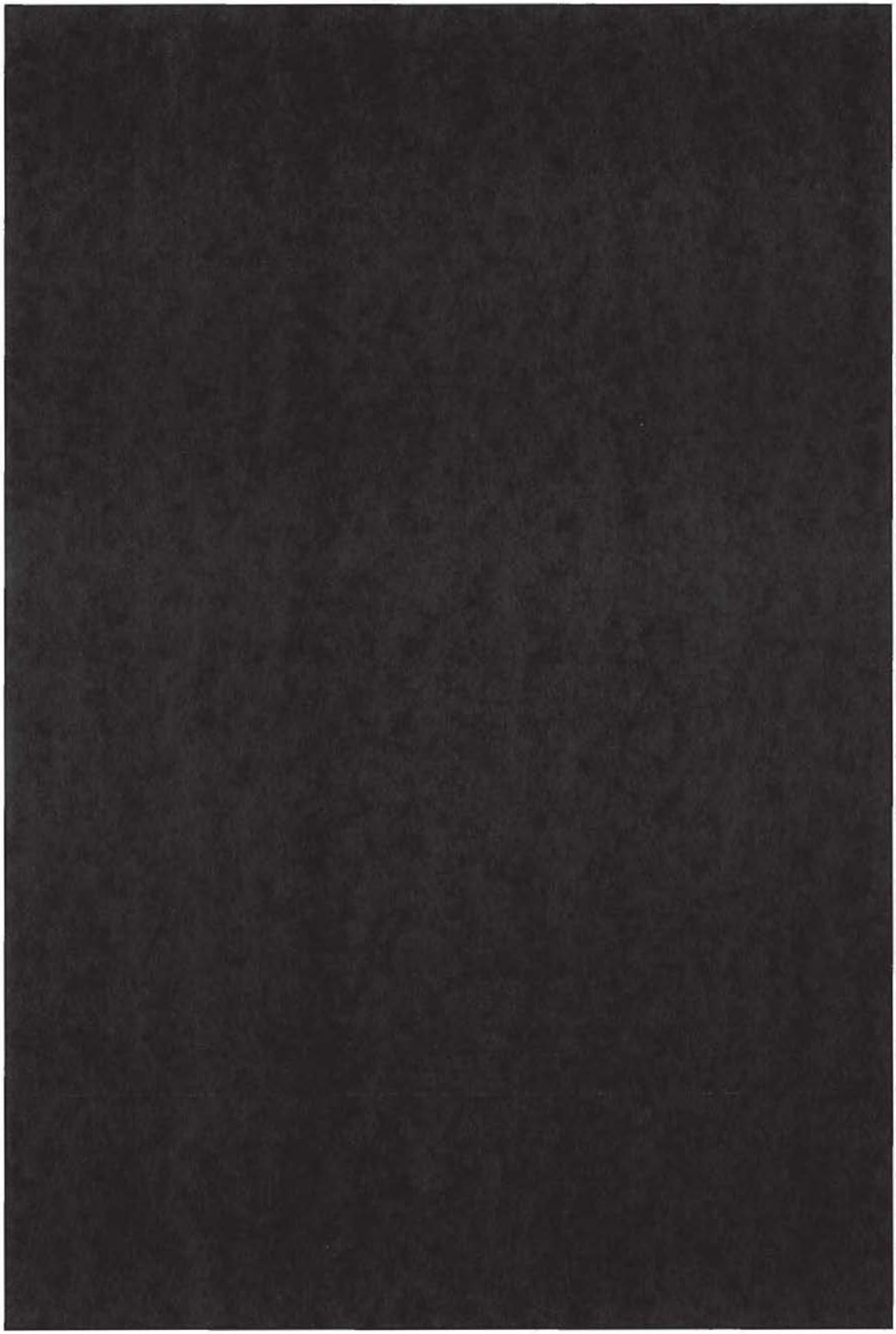


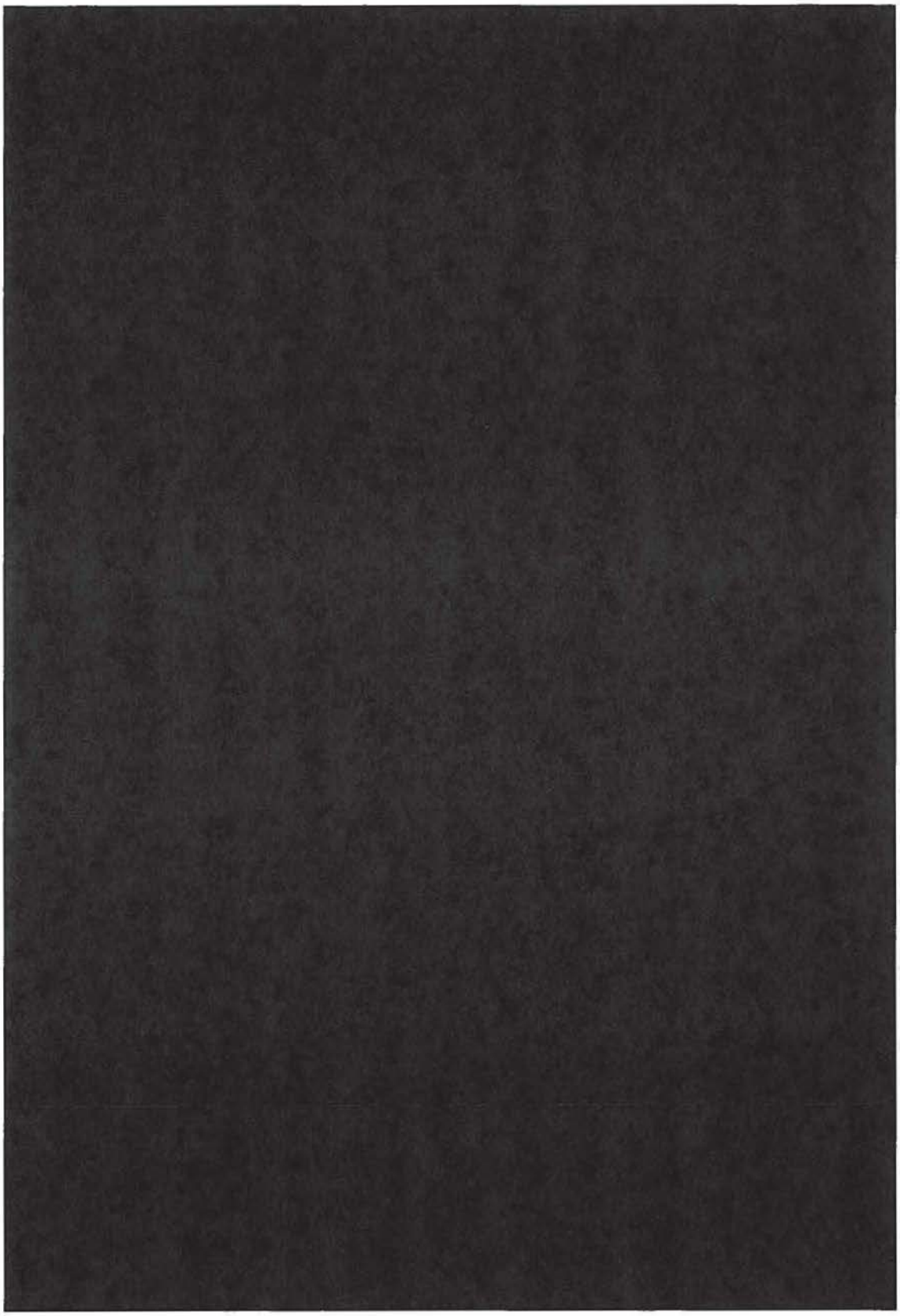


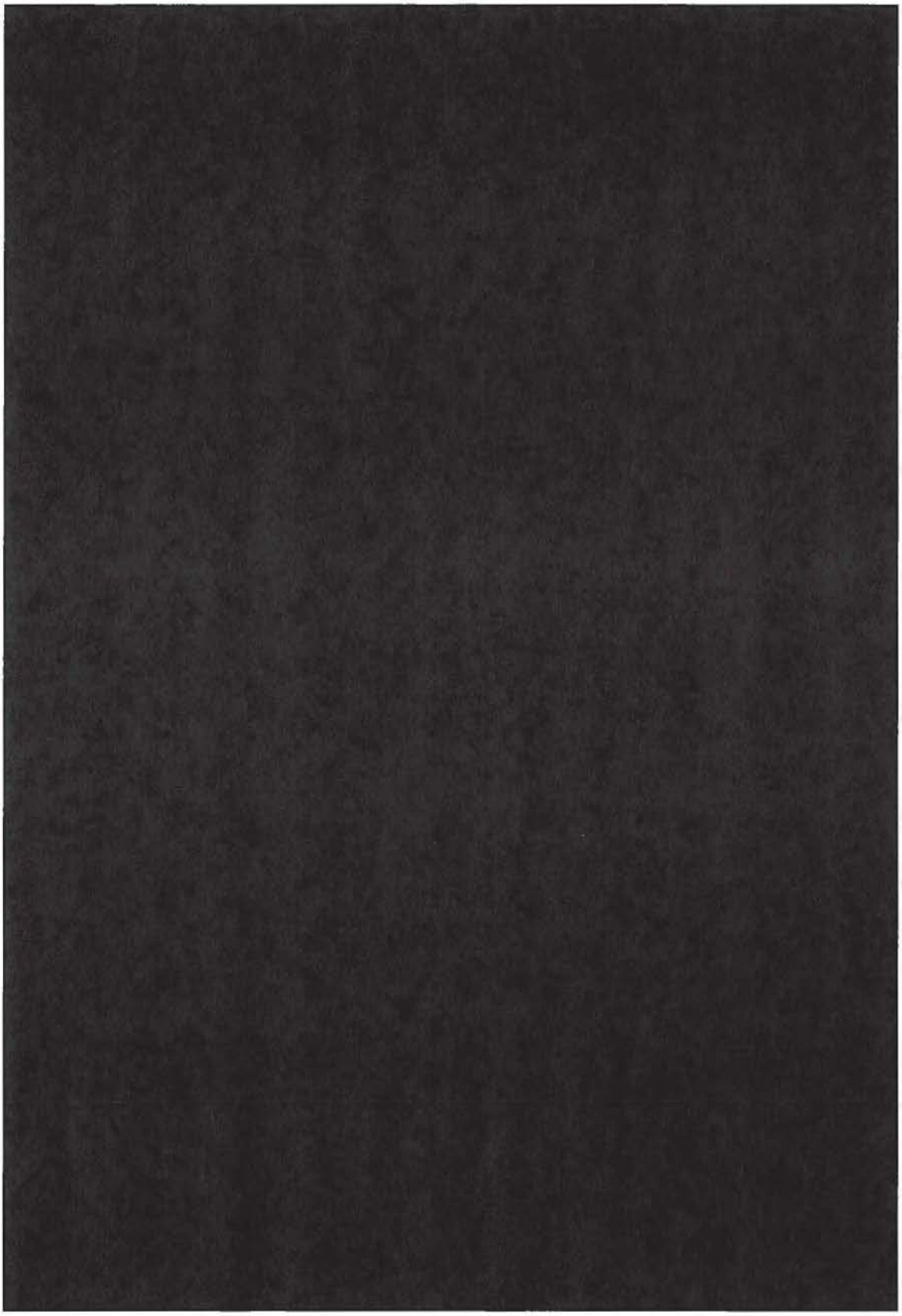


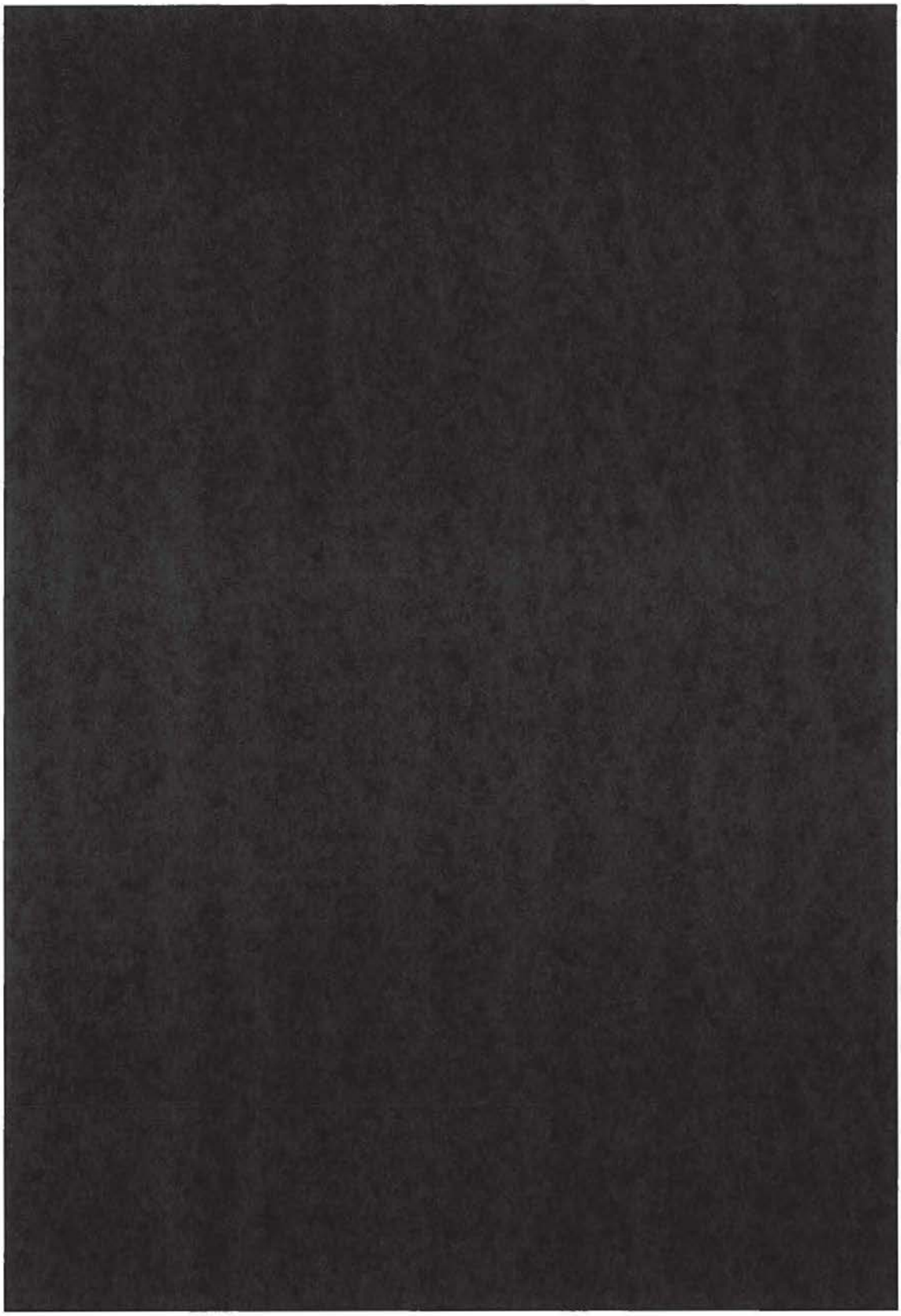


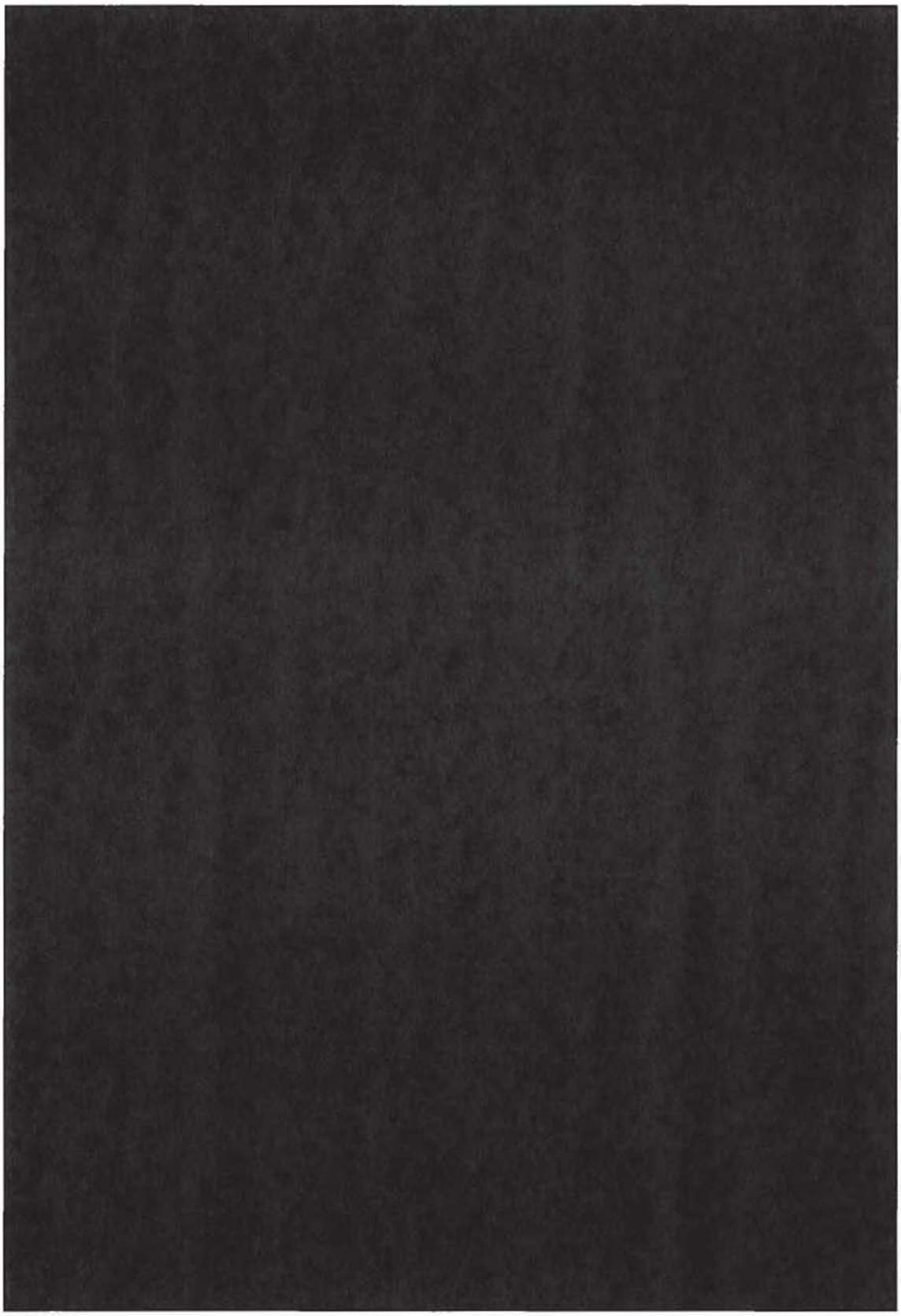


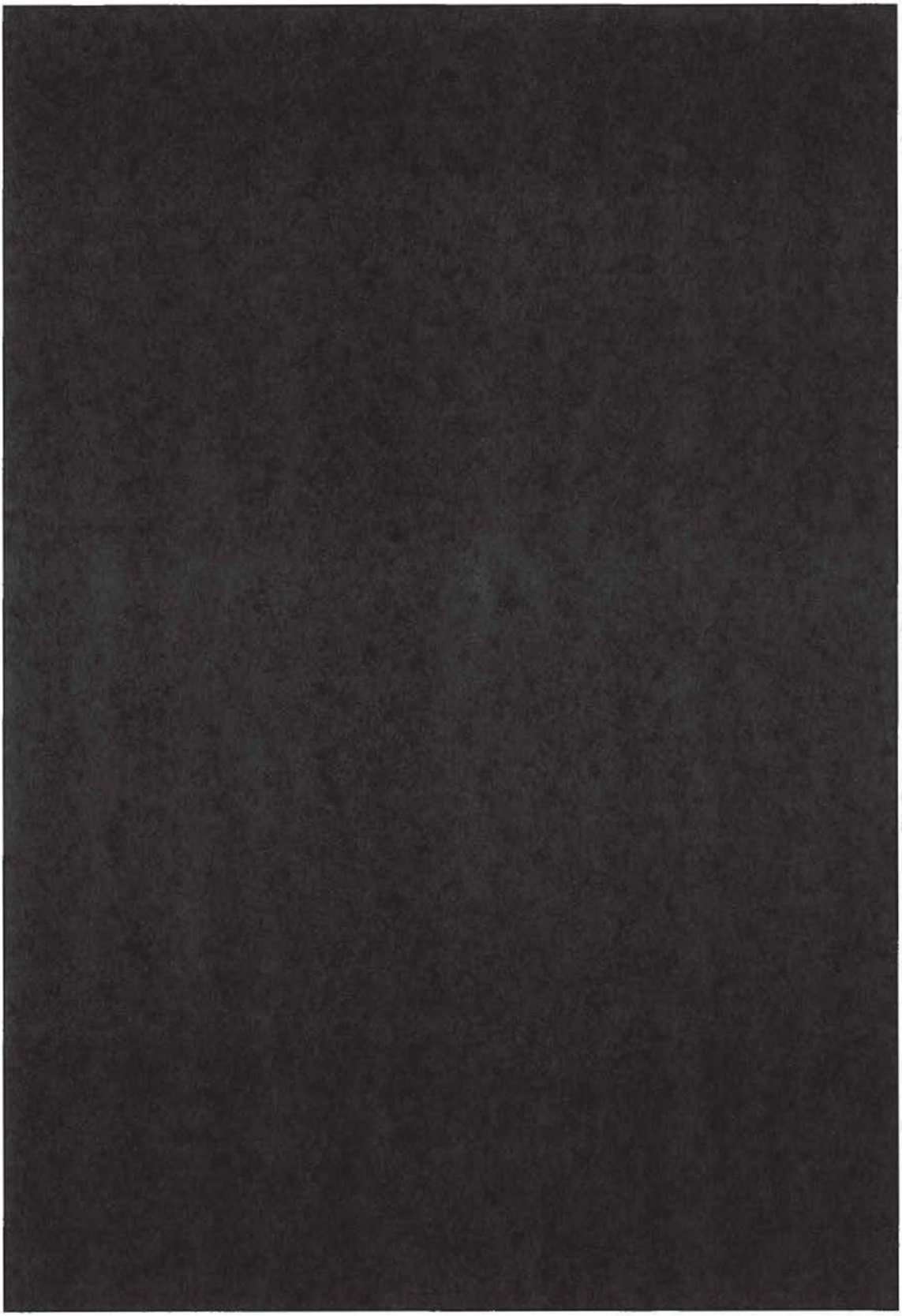


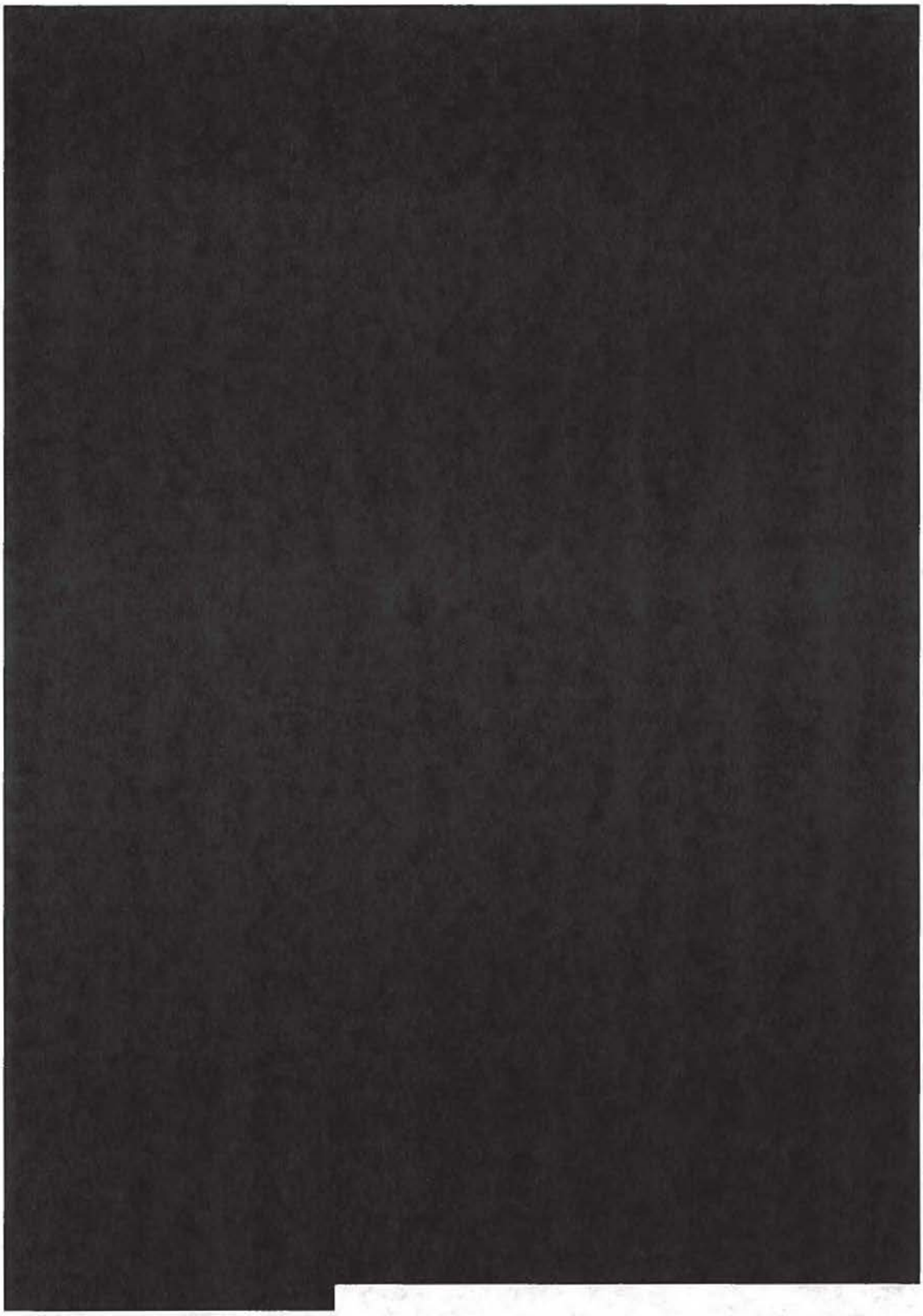






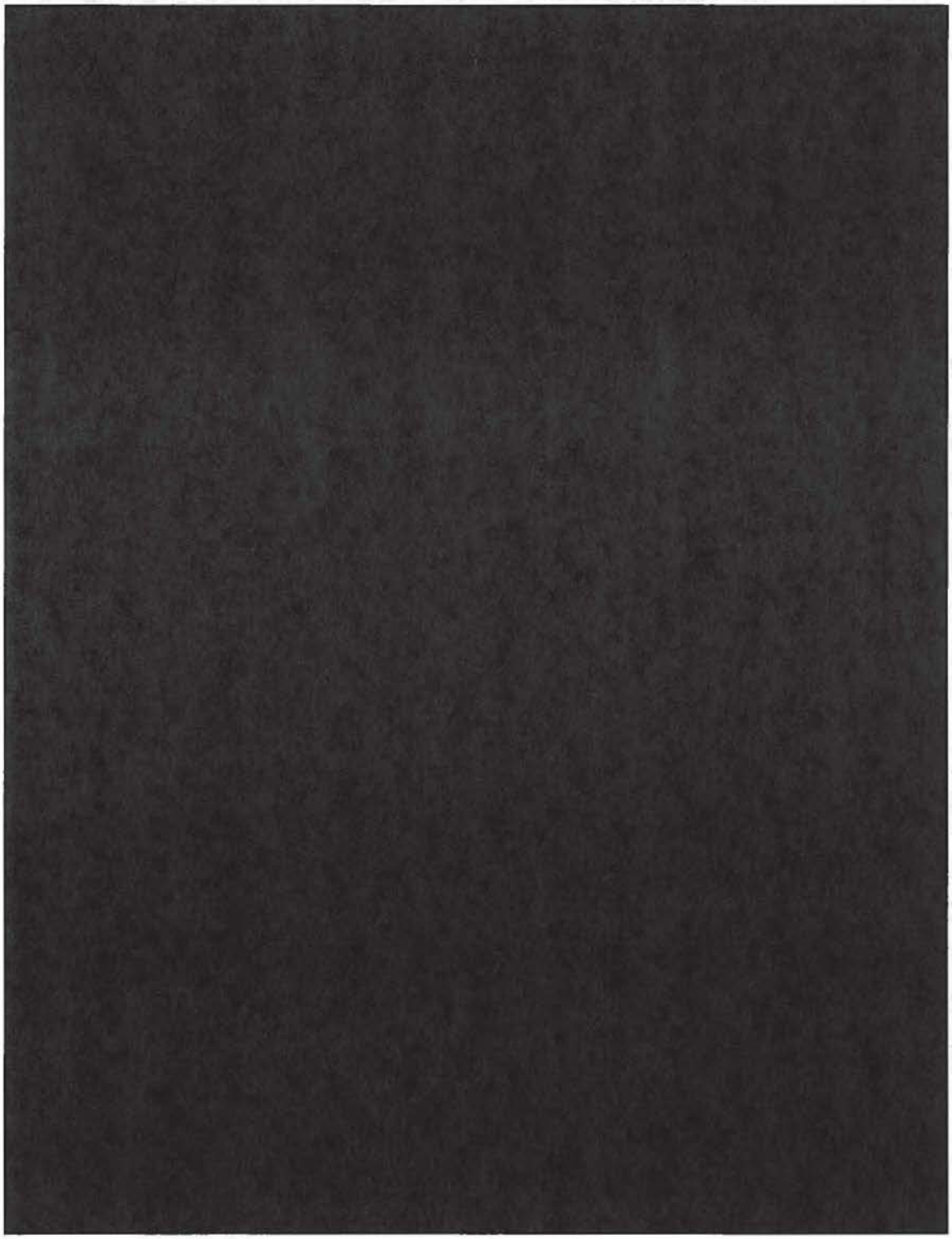


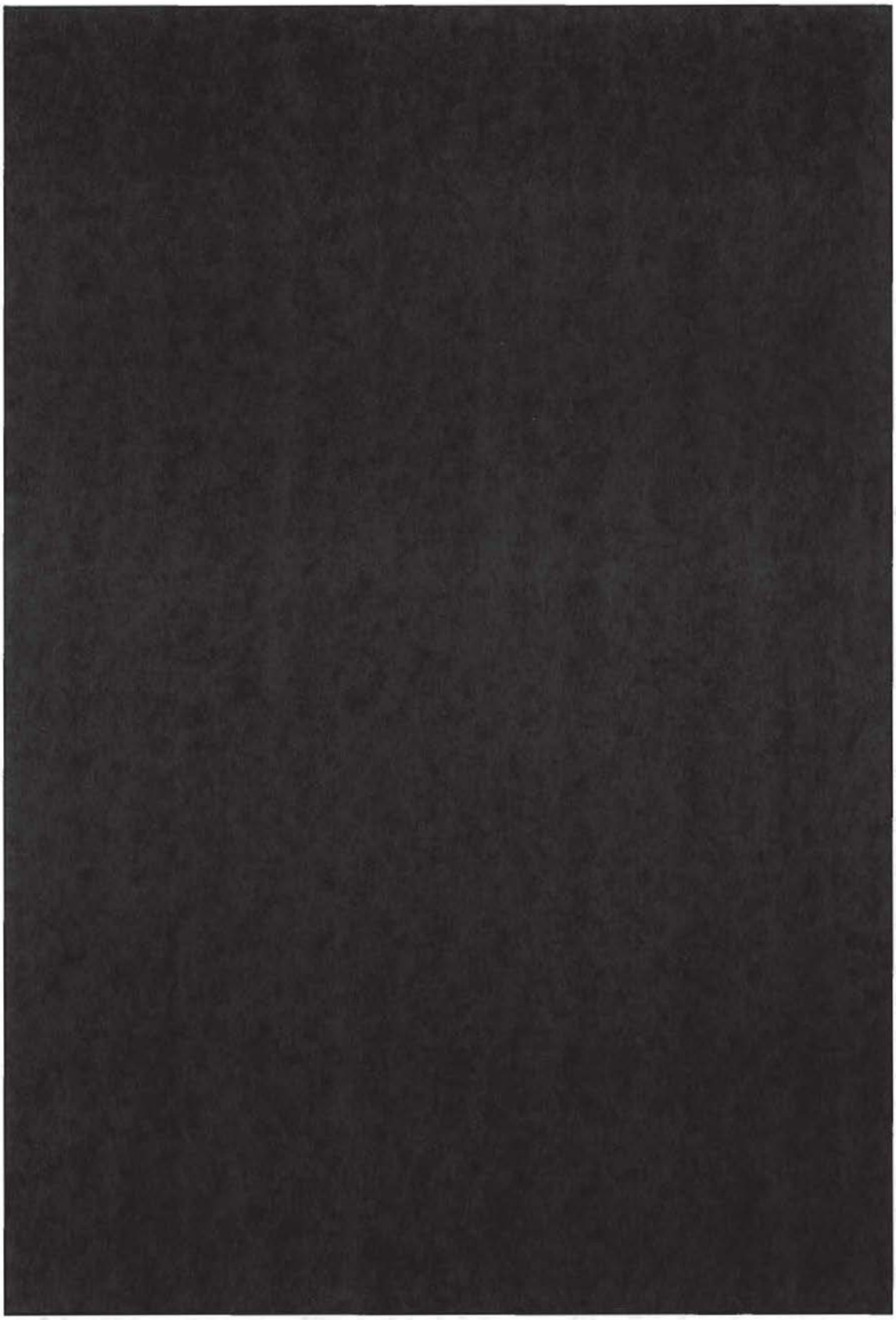


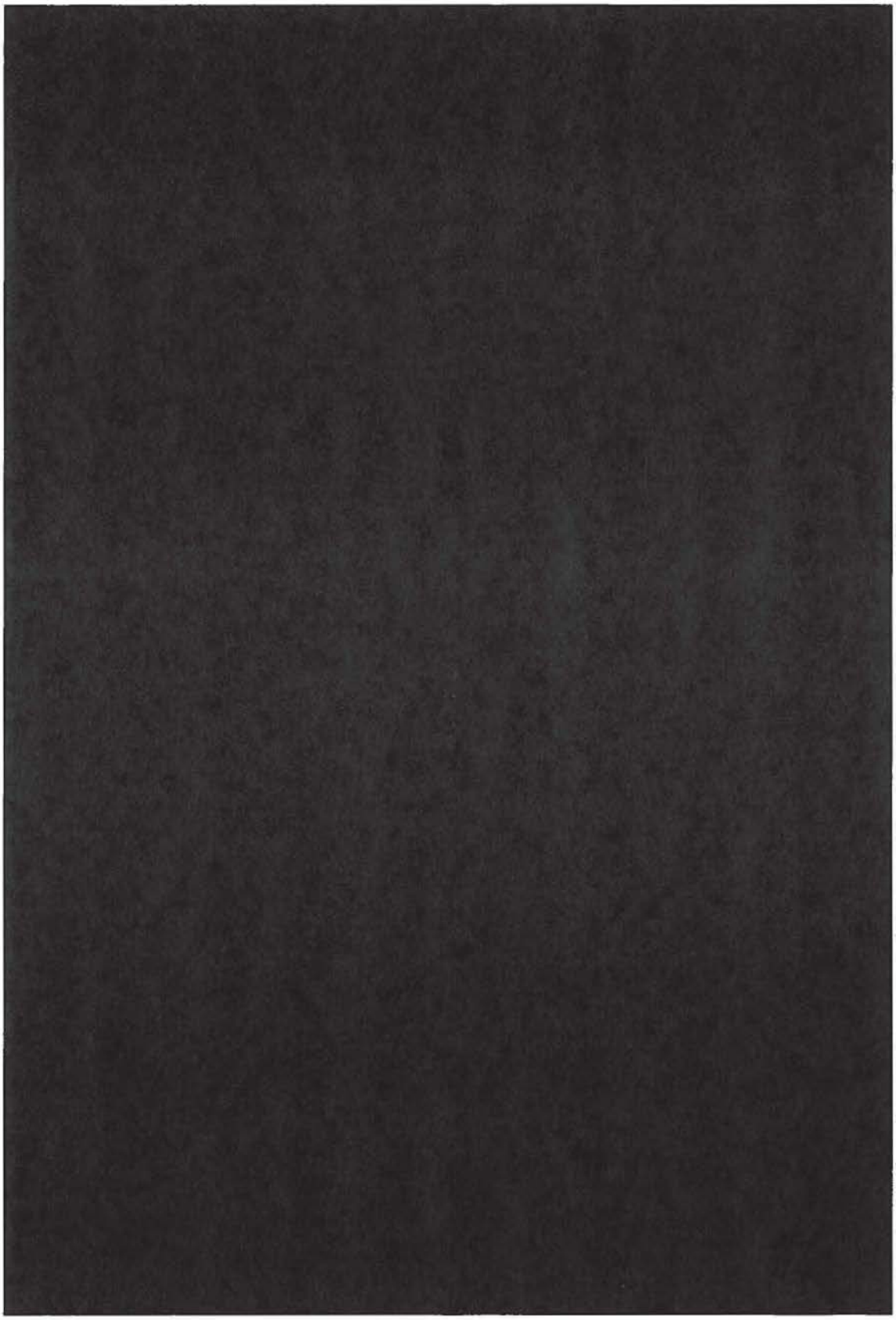


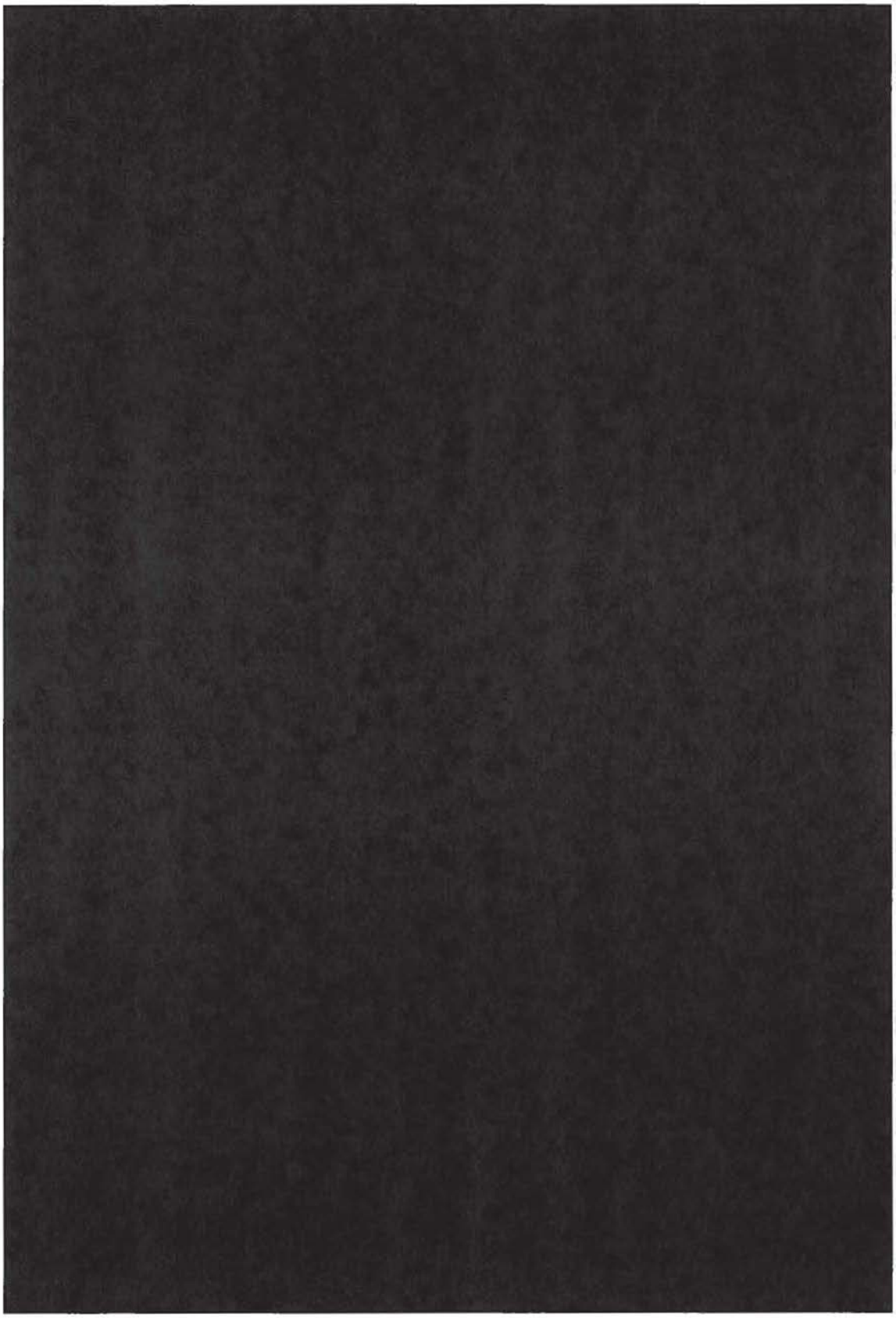
APPENDIX VIII

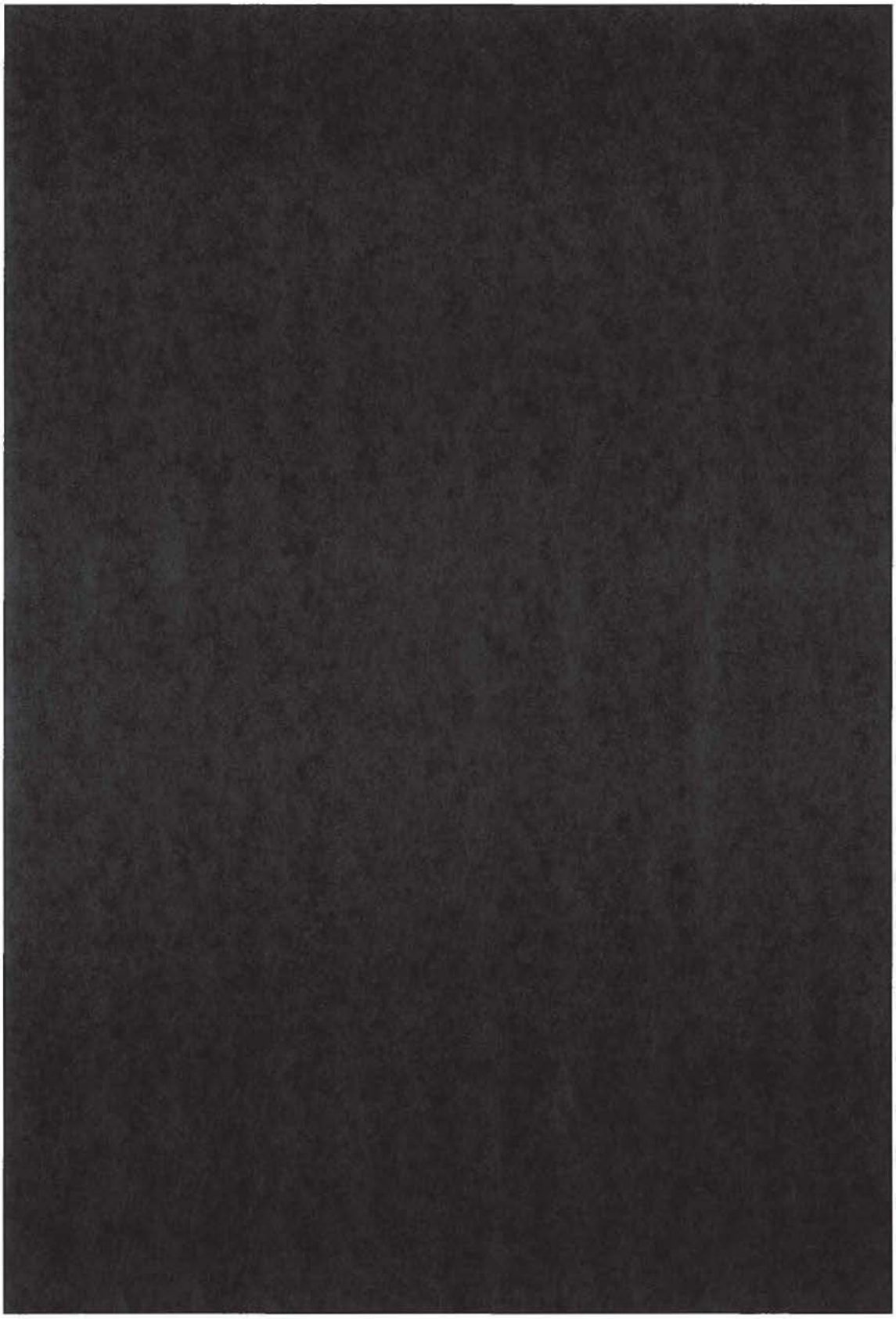
SENTINEL BUILDS

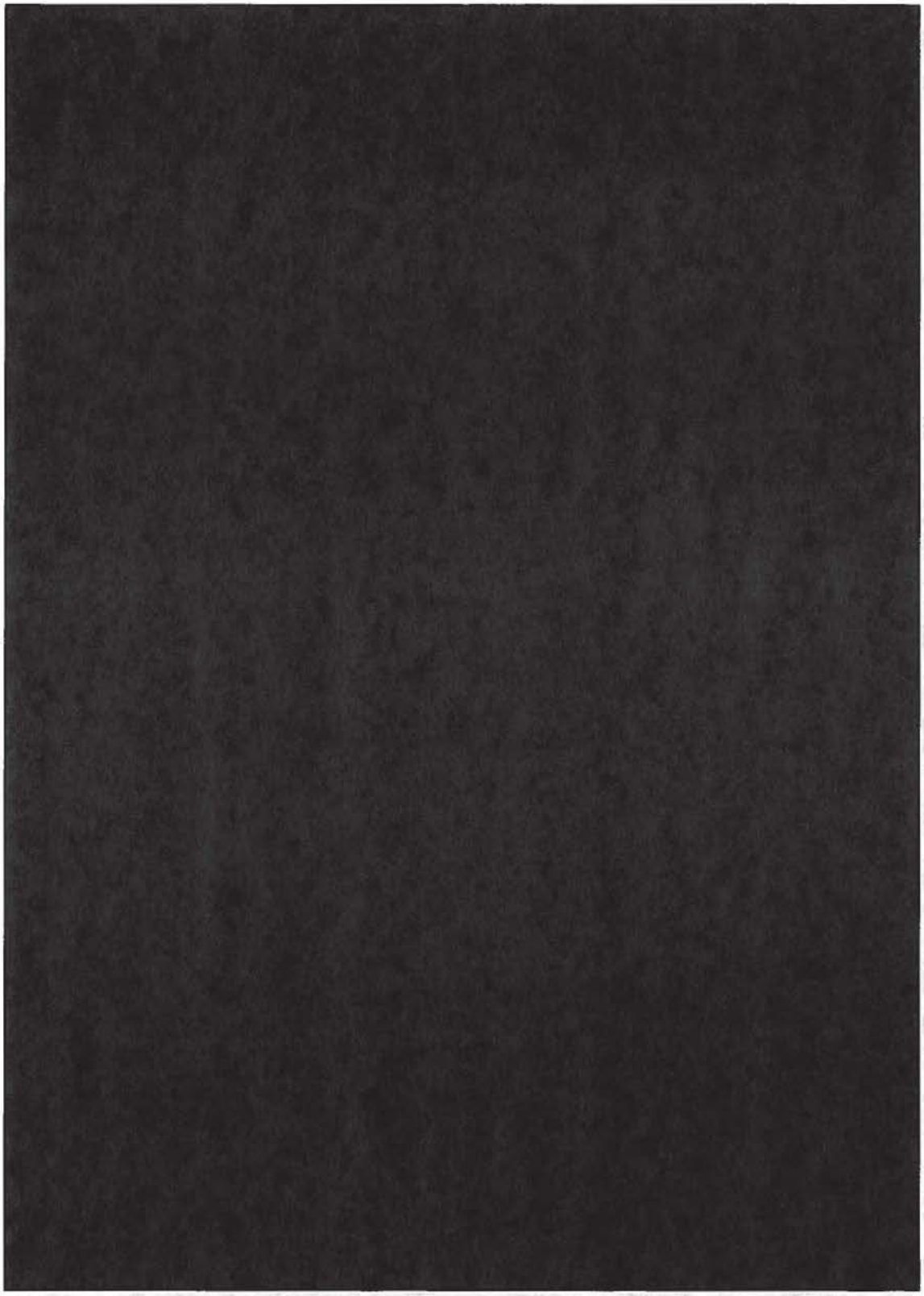


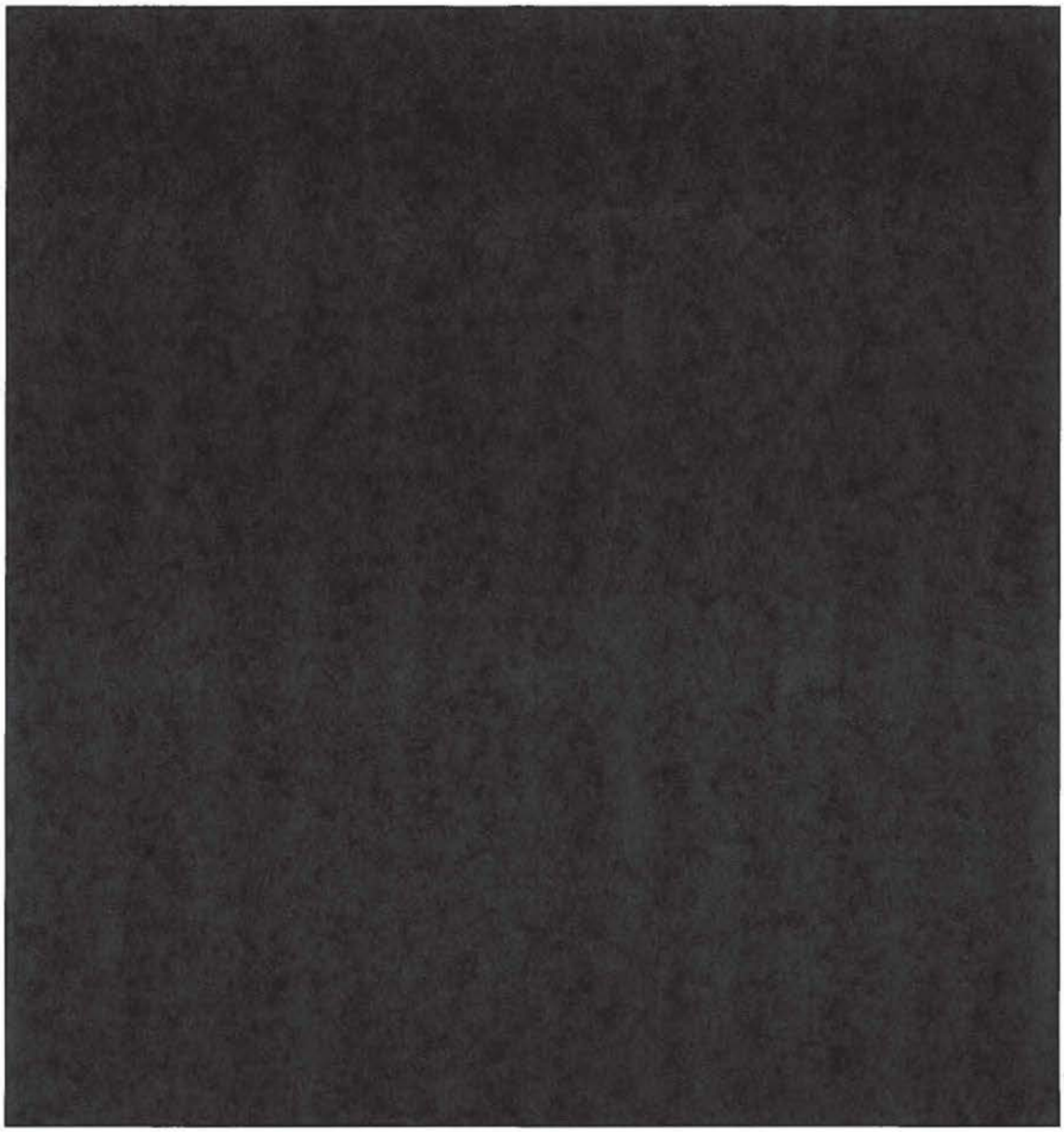












APPENDIX IX

DEFECT REPORT PRIORITY CODES

CODE	PRIORITY	DESCRIPTION
1	Resolve Immediately	Prevents the performance of an operational mission or the use of a mission essential function as defined by the applicable specifications (e.g. causes a program stop, produces an unstable product, or produces no product). A reasonable alternative workaround has not been identified. Provide a solution as soon as possible.
2	Give High Attention	Degrades the performance of an operational function as defined by the applicable specifications. A reasonable alternative workaround has not been identified. Provide a workaround immediately and a solution in the near future.
3	Normal Queue	Degrades the performance of an operation function as defined by the applicable specifications. A reasonable workarounds has been identified. The workaround must be thoroughly documented and tested. Provide a solution in the normal course of business.
4	Low Priority	Does not degrade the performance of an operational function as defined by the applicable specifications. A reasonable alternative workaround is not necessary. Provide a solution as resources permit.

Source: FBI

Defect Report (DR) Process

Both the Sentinel PMO and Lockheed Martin may initiate DRs. Lockheed Martin drafts DRs to: (1) document deficiencies found during operations or maintenance activities, (2) implement an approved request for change or ECP, (3) forward a problem ticket from the Enterprise Operations Center (EOC), or (4) document deficiencies found during testing prior to deployment of a new build.[67] The

[67] An approved request for change adds, deletes, or modifies Sentinel's requirements as documented in the system requirements specification. The EOC, located at FBI headquarters, is the primary resource for FBI personnel with computer problems. The center, which operates 24 hours a day and 365 days a year, logs and

Sentinel PMO may also submit DRs to document deficiencies found prior to deploying a new build. Not all DRs address a technical problem. Some DRs, called enhancement DRs, add capability deemed necessary by FBI users, but were not included as a deliverable in Phase 1. For example, the FBI added field offices' two digit codes to an alphabetical list of the FBI field offices included in the initial deployment of Sentinel. This change allows FBI personnel to easily cross reference a field office name and two digit code.

The Sentinel Joint Engineering Board (JEB), a governance board comprised of both FBI and Lockheed Martin personnel responsible for managing changes to Sentinel, decides which technical problems and functionality updates will be addressed in each of the builds. The JEB also monitors the resolution of defect reports to verify that the solution completely addressed the problem. All draft DRs are forwarded to the JEB, initiating the change management process. The originator presents the proposed DR to the JEB who then reviews the technical description, the affected software products, and the consequences of not resolving the DR. The JEB assigns one of four priority and one of five severity rankings to each DR it approves.[68] The priority ranking assesses the total operational impact of each DR. The severity ranking assesses the impact of each DR from the perspective of Sentinel users only. According to the JEB Charter, severity and priority rankings are often highly correlated, and the combination of the two provides clarity and flexibility in the DR resolution process. The JEB then assigns each DR to a future build. Development proceeds through a fix, build, and test cycle with iterations as necessary. Sentinel PMO personnel draft DRs for any problems they find in the testing of a new build and the JEB adjudicates the draft DRs. After Sentinel PMO personnel complete test and validation of all changes, the Sentinel PMO approves the build for deployment.

---

tracks all incidents and problems until they are closed. For Sentinel incidents, FBI personnel report incidents by calling the EOC service desk. The service desk technician creates a problem ticket and attempts to resolve the incident. Incidents that cannot be resolved by the service desk technician are referred to an on-call O&M engineer. Lockheed Martin drafts DRs for any incidents that the on-call O&M engineer cannot resolve and presents them to the JEB for adjudication.

[68] We focused our DR analysis on priority rankings instead of severity rankings because the criteria for priority rankings correlate to system health.

APPENDIX X

FUNCTIONAL CATEGORIES

Systems Engineering – Develops & integrates needs, required functionality, design synthesis; problem resolution modeling.

Organizational Change Management – Human capital services and knowledge management, training, communications, and organizational cybernetics.

Operations & Maintenance – Supports system to sustain operational readiness; configuration changes, patch management and other system administration tasks; includes system security activities.

Other Internal – Other program-related activities not included in the one of the pre-defined categories.

Systems Architecture – Composite design elements of the system's environment; comprises the system's component design plan for implementation.

Test – Testing or the test environment.

Security Engineering – Enforces security policy to meet security requirements of the system.

Software Development – Includes the knowledge, tools and practices involved with software analysis, development, requirements, engineering, and construction.

COTS Integration – Integration, optimization, and modification of COTS products into the system to achieve the desired result.

DB Engineering – Database design, integration, and implementation.

Development Environment / Data Center – Contractor's development environment, the data center itself.

Computing Storage and Network Infrastructure – Staging, configuring, and installing any Increment-related infrastructure sequentially in all environments (Development, Test, Pre-Production, and Production).

Data Management – Database Management.

Service Oriented Architecture Core Services - Development of a Service Oriented Architecture governance approach and associated procedures, policies, permissions, approval, certification, and security. Also, all services on the Enterprise Service Bus (ESB).

Security – Security engineering throughout product implementation, test, and deployment.

Test Engineering – Test engineering throughout product implementation, test, and deployment.

The following table summarizes the total number of DRs addressed in O&M Builds by functional area.

PHASE 1 DEFECT REPORTS BUILD SUMMARY

Functional Area	Number of DRs
Systems Engineering	11
Organizational Change Management	7
Operations and Maintenance	11
Other Internal	1
Systems Architecture	1
Test	24
Security Engineering	1
Software Development	302
COTS Integration	35
Database Engineering	6
Development Environment / Data Center	11
Unassigned[69]	15
Computing, Storage, & Network Infrastructure	1
Data Management	1
Security	1
Service Oriented Architecture Core Services[70]	27
Test Engineering	1
Total	456

Source: OIG analysis of FBI data

[69] Sentinel PMO personnel provided a listing of all DRs addressed in O&M Build 1.1 through Build 1.12. This list included the functional area affected by each DR. The Sentinel PMO did not identify a functional area for the 15 DRs identified in the table as "unassigned."

[70] A Service Oriented Architecture is a means for integrating across diverse systems. Each IT resource, whether an application or system, can be accessed as a service. These capabilities are available through interfaces.

APPENDIX XI

CPM INDICATOR DATA ELEMENTS DESCRIPTIONS

DATA ELEMENT	PURPOSE	COLLECTION METHOD	THRESHOLD
Average Hourly CPU per Application Platform	Determine the CPU for each application platform. The system shall not exceed 70% CPU utilization during the peak load period (hourly).	Unix Report	70%
Simultaneous User Sessions	Determine that the Simultaneous User Sessions can be sustained. The system shall be capable of processing 25,000 simultaneous user sessions.	Test Report	25,000
Active User Sessions	Determine that the Active User Sessions can be sustained. The system shall be capable of processing 5,000 active user sessions.	Test Report	5,000
System Response Time	Determine the System Response Time. Response time is the time that elapses from when a user issues a command to when the system provides enough results so the user can continue his or her work.	Unix Report	2.5 Seconds
System Availability	Determine System Availability. The system shall provide an operational availability of at least 99.98%. This percentage allows for no more than 1 hour 45 minutes of downtime in a year.	Manual Calculation	99.98%
Storage Capacity and Growth	Determine Storage Capacity and Growth. The system shall provide adequate data storage reserve at deployment.	Test Report	200TB
Web Page Size	Determine the maximum webpage size produced. Some parts of the FBI have limited bandwidth connection, and engineering trade-offs made during design need to take this limitation into account. Web pages should not exceed 50K.	Manual Test Report	50KB

Source: FBI

As shown in the following table, Sentinel has met the criteria for three of the seven CPMs. If Sentinel exceeded its threshold for any CPM data element during one or more of the reporting periods we reviewed, we determined that it was not within its threshold.

CRITICAL PERFORMANCE MEASURE SUMMARY

Data Element	Purpose	Threshold	Within Threshold
Average Hourly CPU Application per Application	Determine the CPU for each application platform.	70%	YES
Simultaneous User Sessions	Determine that the simultaneous user sessions can be sustained.	25,000	NO
Active User Sessions	Determine that the active user sessions can be sustained.	5,000	NO
System Response Time	Determine the system response time.	2.5 seconds	YES
System Availability	Determine the system availability.	99.98%	NO
Storage Capacity and Growth	Determine the storage capacity and growth.	200 Terabytes (TB)	YES
Web Page Size	Determine the maximum web page size produced.	50 Kilobytes (KB)	NO

Source: OIG analysis of FBI data

As shown in the following table, three CPM data element thresholds are inconsistent as identified in the Sentinel Measurement Plan and the Phase 1 System Specification: (1) simultaneous user sessions, (2) active user sessions, and (3) system availability.

COMPARISON OF CRITICAL PERFORMANCE MEASURE THRESHOLDS IN THE MEASUREMENT PLAN AND THE PHASE 1 SYSTEM SPECIFICATION

Data Element	Measurement Plan Threshold	Phase 1 System Specification Threshold	Consistent Threshold?	Within Phase 1 System Specification Threshold?
Average Hourly CPU Application per Application	70%	70%	YES	YES
Simultaneous User Sessions	25,000	5,000	NO	YES
Active User Sessions	5,000	2,000	NO	YES
System Response Time	2.5 seconds	2.5 seconds	YES	YES
System Availability	99.98%	97.50%	NO	YES
Storage Capacity and Growth	200 TB	200 TB[71]	YES	YES
Web Page Size	50 KB	50 KB	YES	NO

Source: OIG analysis of FBI data

[71] Neither the SRS nor the Phase 1 System Specification identified a specific threshold. Therefore we relied on the Sentinel Measurement Plan for the identification of the threshold (200 TB).

APPENDIX XII

O&M INDICATOR DATA ELEMENTS DESCRIPTIONS

DATA ELEMENT	PURPOSE	COLLECTION METHOD	THRESHOLD
System Availability	Determine meeting SLA	Manual	97.5%
Problem ticket response time	Determine meeting SLA	Manual	Critical (15min/2days) High (24hrs/4days) Medium (48hrs/5days) Low (72hrs/6days)
CPU Utilization	Determine meeting SLA	Manual	NTE 70%
Scheduled outage	Determine meeting SLA	Manual	NTE 2 hours unless approved for longer
Unscheduled outage	Determine meeting SLA	Manual	Respond within 1 hour NTE 4 hours

Source: OIG analysis of FBI data

The following table identifies and describes the O&M data elements captured in the Sentinel Measurement Plan, and whether Sentinel has exceeded the thresholds for each element during the periods that we analyzed. From November 2007 through February 2008, Sentinel met the criteria for three of the five O&M elements. If Sentinel exceeded its threshold for any O&M data element during one or more of the reporting periods we reviewed, we determined that it was not within its threshold.

OPERATIONS AND MAINTENANCE DATA
NOVEMBER 2007 THROUGH FEBRUARY 2008

Data Element	Threshold	Within Threshold
System Availability	97.5%	NO
Problem Ticket Response Time	Critical (15min/2days; High (24hrs/4days); Medium (48hrs/5days); Low (72hrs/6days)	NO
CPU Utilization	70%	YES
Scheduled Outage	NTE 2 hours unless approved for longer	YES
Unscheduled Outage	Respond within 1 hour NTE 4 hours	YES

Source: OIG analysis of FBI data

APPENDIX XIII

POA&M DATA ELEMENTS

Type of weakness. Describe weaknesses identified by the annual program review, Inspector General independent evaluation or any other work done by or on behalf of the agency. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity. Where more than one weakness has been identified, agencies should number each individual weakness.

Identity. The office or organization that the agency head will hold responsible for resolving the weakness.

Estimated funding resources required to resolve the weakness. Include the anticipated source of funding, i.e., within the system or as a part of a cross-cutting security infrastructure program. Include whether a reallocation of base resources or a request for new funding is anticipated. This column should also identify other, non-funding, obstacles and challenges to resolving the weakness, e.g., lack of personnel or expertise, development of new system to replace insecure legacy system, etc.

Scheduled completion date for resolving the weakness. The initial date entered should not be changed. If a weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in the "Status" column.

Key milestones with completion dates. A milestone will identify specific requirements to correct an identified weakness. The initial milestones and completion dates should not be altered. If there are changes to any of the milestones the agency should note them in the "Changes to Milestones" column.

Milestone changes. This would include new completion dates for the particular milestone.

Source (e.g., program review, IG audit, GAO audit) of the weakness. Weaknesses that have been identified as a material weakness, significant deficiency, or other reportable condition in the latest agency Inspector General audit under other applicable law, e.g., financial system audit under the Financial Management Integrity Act, etc. If yes is reported, also identify and cite the language from the pertinent audit report.

Status. The agency should use one of the following terms to report status of corrective actions: Ongoing or completed. "Completed" should be used only when a weakness has been fully resolved and the corrective action has been tested. Include the date of completion.

POA&M Environment Descriptions

Herndon Secret Sentinel System (HS3)

The HS3 is an FBI classified system operating at the secret, system high mode of operation. The HS3's mission is to provide logically separated environments for Sentinel development, pre-production staging, user acceptance testing, and system testing (integration and functional).

Sentinel Phase 1

SP1 provides end users with a web-based portal for accessing stored data on ACS. SP1 consists of a storage area network that services multiple application servers, and it is deployed at two locations.[72] The primary site is in Clarksburg, West Virginia, and a backup site is located at the J. Edgar Hoover Headquarters Building in Washington, D.C. Both Sentinel sites are identical in equipment and configuration, with the exception of a training environment that is present at the headquarters location.

[72] A storage area network (SAN) connects multiple servers and storage devices on a single network.

APPENDIX XIV

PMO STAFF POSITIONS AND RESPONSIBILITIES

Program Leadership

Program Manager

The one individual held accountable for program outcome is the Program Manager (PM). The PM is responsible for cost, schedule, and performance including system capabilities deployed to the users; Organizational Change Management (OCM) leading to users accepting and employing Sentinel capabilities and budget preparation, defense, and execution. The PM is also responsible for the PMO's organization, staffing, and operations; governance processes for program execution; communications between Sentinel and its stakeholders; Systems Requirements configuration management (CM); prime contractor direction to ensure delivered capabilities meet requirements; and Chairs Task Order(s) Award Fee Board.

Deputy Program Manager (DPM)

Two DPM's support the PM as Branch Chief's within the PMO. One DPM manages the system development and technology and the other DPM manages organizational change, program support to include budget and finances, training, communications, user representation and liaison.

Direct Reporting Staff

Reporting directly to the Program Manager are staff with diverse roles and responsibilities. We identify several of the members who compose the Direct Reporting Staff below.

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.

Quality Manager

Provides guidance, oversight and coordination related to quality control issues within the PMO and with the development contractor.

Program Advisor

Provides overall execution advice to the Program Manager and deputy program manager.

Operations and Maintenance Unit (OMU)

The OMU is responsible for Sentinel's O&M Concept of Operations as well as oversight of Sentinel's deployed capabilities operations and maintenance. The OMU retains these responsibilities until Sentinel achieves FOC and total O&M responsibilities are transferred to ITOD. The OMU will establish and maintain close collaboration with ITOD throughout Sentinel capability development. The OMU also plans for and coordinates deployment of Sentinel to all of the FBI receiving locations and units.

Organization Change Management

The 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 Branch is composed of the following units.

Training and Communications Unit (TCU)

The TCU Unit is the Program Manager's representative for communicating program information. The TCU is also responsible for

the design and development of the program's communication strategies; to make sure all stakeholders are aware of, and accurately informed about the program's plans and accomplishments; primary contact point for external entities seeking information about the Sentinel program; to act as a liaison to Inspection Division for Inspector General and Government Accountability Office reviews; coordinates and plans training; and training staff in which they ensure all required system, O&M, and business process training is developed, tested, and executed in support of Phase deployments

User Representation and Policy Unit (URPU)

The URPU is responsible for the strategy employed for changing the FBI organization, to include how it carries out its overall mission, while enabling users to learn new behaviors, skills, and business processes. The URP assists in providing robust training and outreach programs while the Sentinel Program evolves and deploys its functional capability. The URPU ensures the FBI's overall strategy and user acceptance through continual process diagramming, requirements clarification, testing, communications, program advocacy, marketing, as well as the development and deployment of training.

Program Support Unit (PSU)

The PSU is made up of the Program Integration Team (PIT) and the Business Management Team (BMT).

Program Integration Team

The PIT is responsible for developing and maintaining the Sentinel program baseline, tracking progress and risks against that baseline, and incorporating changes to the baseline as directed by the PM. The PIT operates collaboratively with the other Line Units in defining, collecting, monitoring, and maintaining the Sentinel program baseline including documentation that defines that baseline. PIT has a key role in preparing material for use in oversight reviews, external documentation, and joint program activities.

Business Management Team

The BMT develops and maintains the program's investment, budget and spend plans. The BMT monitors, analyzes and reports on

the program's Earned Value Management (EVM) status. It also provides the COTR who will assists the CO in technical oversight of all Sentinel contract execution, and manages the administrative support elements.

Systems Branch

The Systems Branch is comprised of the Systems Development Unit (SDU), On-Site (OS) staff, Systems Analysis Team (SAT), and Systems Engineering/Test Team.

Systems Development Unit

The SDU is responsible for the Sentinel system development in terms of both the overall system design and its implementation increments. It owns the technical performance outcome of the Sentinel Program and is accountable for the systems requirements and delivering a system solution whose technical performance meets the User Community expectations. The SD Unit Manager oversees the Sentinel capability development effort through several functional staffs.

- On-Site Staff — The On-Site Staff is responsible for direct and daily interactions with the Prime Contractor as a facilitator for effective, responsive development of Sentinel's capability by the Prime. OS staff represents the Program Manager's primary independent source of information on Lockheed's progress toward meeting the Sentinel development Task Orders, increments, and requirements.

- Systems Analysis Team — The Systems Analysis Team is responsible for Sentinel's requirements, design, and performance from a total system perspective and Sentinel's interoperability within the FBI Enterprise and with other Agencies' systems.

- Systems Engineering/Test Team — The Systems Engineering/Test Team is responsible for development of Sentinel's individual increments/phases. It also serves as the core of the On-Site Team.

APPENDIX XV

PHASE 2 SEGMENT 1 CAPABILITIES

Segment	Increment	Capability
1	1	Enhancement of Sentinel's provisioning capabilities by delivering: • patch management abilities for the underlying operating systems, and • improved software inventory reporting.
1	2	Enhancement of Sentinel's internal monitoring capabilities.
1	3	• Installation and configuration of the data migration system into the FBI's test and development environment. • Regression testing, modification, verification, and integration of data migration scripts prototyped in Phase 1, including benchmarking, will also be completed. • Generation of test and development test data.
1	4	Initial deployment of the Sentinel Enterprise Portal (SEP). The following capabilities will be part of the SEP: • Create a single entry point to existing FBI applications including Sentinel for appropriately authorized FBINET users; provide a single location of links to other FBI applications; and provide a single location for user generated shortcuts.
1	4	• Create a framework into which future portlets may be deployed and hosted and create portlets consisting of personal and squad summarized information from ACS.

Source: FBI

APPENDIX XVI

RISK EXPOSURE MATRIX

Probability of Occurrence (PO)

VERY HIGH Extremely likely that the risk event will occur (4)	0	1	0	0
HIGH Highly likely that the risk event will occur (3)	0	0	0	0
MEDIUM Likely that the risk event will occur (2)	1	3	1	0
LOW Unlikely that the risk event will occur (1)	2	0	0	0
I x P = Total Risk Exposure	**LOW** Minimal impact on schedule, cost, technical, or business performance (1)	**MEDIUM** Minor impact on schedule, cost, technical, or business performance (2)	**HIGH** Major impact on schedule, cost, technical, or business performance (3)	**VERY HIGH** Significant impact on schedule, cost, technical, or business performance (4)

Impact Severity (IS)

Source: FBI

APPENDIX XVII

FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

November 14, 2008

Mr. Raymond J. Beaudet
Assistant Inspector General
Office of the Inspector General
U.S. Department of Justice
1425 New York Avenue
Suite 5000
Washington, D.C. 2005

Re: SENTINEL Audit IV: STATUS OF THE FEDERAL BUREAU OF INVESTIGATION'S CASE MANAGEMENT SYSTEM

Dear Mr. Beaudet:

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 IV: 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 and sensitivity review which is enclosed with this letter.

Please feel free to contact me on (202) 324-6165, or Mr. Andrew F. Brackenridge of my staff. Mr. Brackenridge may be reached on (202) 324-5175.

Sincerely,

Dean E. Hall
Acting Executive Assistant
Director and Chief Information
Officer

Enclosure

FEDERAL BUREAU OF INVESTIGATION (FBI) RESPONSE TO THE DEPARTMENT OF JUSTICE (DOJ) OFFICE OF THE INSPECTOR GENERAL (OIG)
DRAFT AUDIT REPORT
SENTINEL AUDIT IV: STATUS OF THE FEDERAL BUREAU OF INVESTIGATION'S CASE MANAGEMENT SYSTEM

Responses to Recommendations:

Recommendation 1: Decide what data will be stored in SENTINEL, how that data will be collected, and what FD forms SENTINEL will replace and adjust the Systems Requirement Specification if necessary.

FBI Response: Agree. The FBI is in the process of resolving this issue. The FBI continues to reduce the number of forms in coordination with the Corporate Policy Office. To date, seven forms or work items have been developed within SENTINEL for deployment in early 2009. Additional forms are scheduled to be deployed later in the year. In addition, the FBI is also in the process of converting approximately 70 WordPerfect macros into Microsoft InfoPath forms in preparation for the enterprise-wide deployment of Windows Vista. The FBI is determining if and how the remaining forms and InfoPath forms will be ingested into SENTINEL.

Recommendation 2: Decide which statistics will be stored in SENTINEL and how those statistics will be entered into SENTINEL, and adjust the Systems Requirement Specification if necessary.

FBI Response: Agree. The FBI is in the process of resolving this issue. The SENTINEL PMO initiated a statistics project in mid-2007 in an effort to overhaul the type of statistics the FBI should be capturing and the manner in which those statistics should be collected. The current process requires users to prepare an Accomplishment Report (FD-515) or Investigative Accomplishment Report (FD-542) form. These two forms capture approximately 1,500 different types of statistics, many of which appear to be outdated and/or of no significant value.

In early 2008, the SENTINEL PMO joined efforts with the FBI's Resource Planning Office (RPO) at FBIHQ to address this issue. Officially named the Analysis and Statistical Reporting Project, a streamlined list has been generated which currently totals approximately 160 types of statistics. Each of these statistics is directly linked to the FBI's strategic objectives, investigative program objectives, and/or inspection process. The RPO is currently reviewing this revised list with each operational division at FBIHQ. Once this review is completed, a final list will be submitted to the FBI Director for approval. Once approved, the requirements will be provided to Lockheed Martin for design and implementation in SENTINEL.

Recommendation 3: Decide whether SENTINEL **will serve as the FBI's enterprise-wide records management system, and adjust the Systems Requirement Specification if necessary.**

FBI Response: Agree. The FBI will utilize the commercial off - the - shelf (COTS) Records Management Application (RMA) provided with SENTINEL as the base for an enterprise-wide FBI RMA. As applications emerge outside the scope of the SENTINEL program, the FBI organization that makes use of the capability will provide, when necessary, the resources to expand the RMA capability to store records generated by their non-SENTINEL application.

To accommodate this concept, the entire FBI records disposition schedule is being incorporated into the SENTINEL RMA as a deliverable under Phase 2, Segment 3. Discussions among EMC Corporation, the COTS RMA provider, FBI Finance Division, and the Office of IT Policy and Planning have clarified the terms of the enterprise-wide licensing for the RMA.

Recommendation 4: Complete the SENTINEL FOC architecture.

FBI Response: Completed. This task was completed and certified by the DOJ's Department Investment Review Board in June 2008. The FBI requests that this recommendation be closed.

Recommendation 5: Update the EVM System Description.

FBI Response: Agree. The FBI is in the process of revising the Earned Value Management (EVM) System Description.

Recommendation 6: Provide better descriptions and justifications for EVM baseline changes.

FBI Response: Completed. Each quarter, the FBI's SENTINEL PMO submits a Quarterly Baseline Change Report to DOJ's EVM oversight lead. Additionally, the PMO participated in the yearly EVM Oversight Surveillance Audit conducted on September 23, 2008. Favorable results were communicated to the SENTINEL PMO from the DOJ on October 2, 2008. The FBI requests that this recommendation be closed.

Recommendation 7: Revise Attachment 1 of the current SENTINEL Statement of Work to clarify the requirements with respect to Attachment 1 of the July 2005 version of the SENTINEL Statement of Work.

FBI Response: Completed. The Statement of Work (SOW) Attachment 1 Program Process Methodology (PPM) Directive was incorrectly provided as version 1.0. The PPM was updated in March 2008 as version 1.1 as part of the Joint Audit and should

have been provided as an update to the SOW. Version 1.1 has subsequently been provided to the OIG. The FBI requests that this recommendation be closed.

Recommendation 8: Amend the Measurement Plan to reflect the addition of Phase 1 System Specification CPM thresholds, and update the Measurement Plan as the CPM thresholds change in subsequent versions of the System Specification.

FBI Response: Agree. The FBI will incorporate this change in the next version of the Measurement Plan.

Recommendation 9: Update the POA&M template and all open POA&M findings on the HS3 and SP1 POA&Ms to include all of the reporting elements required by OMB.

FBI Response: Agree. The FBI believes that it has already remedied the concern. The template was updated and reviewed by the FBI's Security Division who postulates that it complies with all Office of Management and Budget Memoranda.

Recommendation 10: Revise the SENTINEL Risk Management Plan to use the risk criteria contained in Version 1 of the Risk Management Plan.

FBI Response: Completed. The SENTINEL PMO implemented a revision to the Risk Management Plan (Version 1.7, dated July 9, 2008) that changed the threshold of impact from **"overall program"** to **"period impacted."** This change allows the program to identify risks and mitigations at a lower level of impact to the program.

Version 1.6 stated: "Significant (greater than 15%) cost impact to the **overall** program. Mitigation requires additional funding exceeding available funding sources to complete program." Version 1.7 now reads: "Significant (greater than 15%) cost impact to **period** impacted. Mitigation requires additional funding exceeding available funding sources to complete program."

Depending on whether the impact was considered to be very high, high, medium, or low, the percentages changed from 15, 10-15, 5-9, or less than 5, respectively.

The FBI requests that this recommendation be closed.

APPENDIX XVIII

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

The OIG provided a draft of this audit report to the FBI for its review and comment. The FBI's response to our audit report is included as Appendix XVII of this report. The FBI concurred with all of the recommendations in this report. Our analysis of the FBI's response to the 10 recommendations is provided below. Based on the FBI's response, the OIG considers the report resolved. The following is a summary of the actions necessary to close the recommendations.

Summary of Actions Necessary to Close the Recommendations

1. **Resolved.** This recommendation is resolved based on the FBI's ongoing efforts to resolve this issue and to reduce the number of forms in coordination with its Corporate Policy Office. This recommendation can be closed after we review documentation demonstrating what data will be stored in Sentinel, how that data will be collected, and what FD forms Sentinel will replace.

2. **Resolved.** This recommendation is resolved based on the PMO joining efforts with the FBI's Resource Planning Office to address this issue as part of the FBI's Analysis and Statistical Reporting Project. The Reporting Project team generated a list of approximately 160 types of statistics, and each statistic has been linked to the FBI's strategic objectives, investigative program objectives, or the FBI's inspection process. The Resource Planning Office is reviewing the list with each operational division within the FBI. This recommendation can be closed after we review the revised Sentinel plans or System Requirement Specification that incorporates the statistics that will be stored in Sentinel and how those statistics will be entered into Sentinel.

3. **Resolved.** This recommendation is resolved based on the FBI's plan to utilize the commercial off-the-shelf (COTS) Records Management Application (RMA) provided with Sentinel as the base for an enterprise-wide FBI RMA. The FBI stated that as applications emerge outside the scope of the Sentinel program, the FBI organization that makes use of the capability will provide, when necessary, the resources to expand the RMA's capability to store records generated by their non-Sentinel application. The

entire FBI records disposition schedule is being incorporated into the Sentinel RMA as a deliverable under Phase 2, Segment 3. This recommendation can be closed after we review documentation demonstrating that the COTS RMA is the base application for the enterprise-wide FBI RMA and that the relevant changes have been captured in the Sentinel System Requirement Specification.

4. **Closed.** This recommendation is closed based on the FBI's completion of the Sentinel Full Operating Capability (FOC) Architecture. The Department Investment Review Board certified the architecture in June 2008 with 10 qualifications. In November 2008, the FBI provided documentation demonstrating that the FBI had completed the FOC Architecture.

5. **Resolved.** This recommendation is resolved based on the FBI's statement that it is in the process of revising the Earned Value Management (EVM) System Description. This recommendation can be closed after we have reviewed the revised Earned Value Management System Description.

6. **Resolved.** This recommendation is resolved based on the FBI's statement that the FBI's PMO: (1) produces Quarterly Baseline Change Reports that are sent to the Department's EVM oversight lead, (2) participated in the yearly EVM Oversight Surveillance Audit conducted in September 2008, and (3) received favorable results from the Department in October 2008. This recommendation can be closed after we review documentation demonstrating that the PMO has provided better justification and descriptions for EVM baseline changes.

7. **Closed.** This recommendation is closed based on documentation provided by the FBI in November 2008 showing the revision of the Sentinel Statement of Work (SOW) to remove conflicting requirements related to SOW Attachment 1.

8. **Resolved.** This recommendation is resolved based on the FBI's plan to incorporate the addition of System Specification CPM thresholds and update the Measurement Plan as the CPM thresholds change in subsequent versions of the System Specification. This recommendation can be closed after we review documentation demonstrating that the PMO has: (1) added the Phase 1 System Specification CPM thresholds, and (2) updated the

Measurement Plan as the CPM thresholds change in subsequent versions of the System Specification.

9. **Resolved.** This recommendation is resolved based on the POA&M template update reviewed by the FBI's Security Division and based on statements that it complies with all OMB memoranda on the subject. This recommendation can be closed after we review open POA&M findings for HS3 and SP1 to ensure that they meet all of the reporting elements required by OMB.

10. **Resolved**. This recommendation is resolved based on the FBI's PMO implementing a revision to the Risk Management Plan that changed the threshold of impact from "overall program" to "period impacted." This recommendation can be closed after we review documentation defining the term "period impacted" and demonstrating that all risks of medium or higher impact severity or probability of occurrence have a mitigation strategy and contingency plan, as identified previously in Risk Management Plan Version 1.2.