THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF THE TRILOGY INFORMATION TECHNOLOGY MODERNIZATION PROJECT

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

Audit Report 05-07
February 2005

THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF THE TRILOGY INFORMATION TECHNOLOGY MODERNIZATION PROJECT

EXECUTIVE SUMMARY

This audit assesses the progress of the Federal Bureau of Investigation's (FBI) Trilogy project. Initiated in mid-2001, the objective of Trilogy is to modernize the FBI's information technology (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 in the FBI.

Trilogy consists of three parts: 1) upgrading the FBI's hardware and software, 2) upgrading of the FBI's communications network, and 3) upgrading the FBI's five most important investigative applications, including its antiquated case management system.

Because of the FBI's immediate and critical need for modern IT systems and the past problems in the Trilogy project, we conducted this audit to assess the FBI's progress in meeting cost, schedule, technical, and performance targets for the three components of Trilogy. We also examined the extent to which Trilogy will meet the FBI's current and longer-term IT needs.

In April 2004, the FBI completed the first two components of Trilogy. Among other improvements, the FBI has improved its IT infrastructure with new desktop computers for its employees and has deployed a Wide Area Network to enhance electronic communication among FBI offices and with other law enforcement organizations. However, despite additional funding the FBI had received to accelerate Trilogy, the first two phases of Trilogy were not completed any faster than originally planned.

While the infrastructure components are now in place to support improved user applications, the FBI is still far from implementing the third component of Trilogy. In this third phase, the FBI has been seeking to implement a case management system called the Virtual Case File (VCF), which was intended to replace the FBI's antiquated case management application, the Automated Case Support system (ACS). The VCF was designed to improve the FBI's ability to manage investigative case files, facilitate data and document searches, and

share information within and among FBI offices. The need for a new automated investigative case management system to replace the existing obsolete and limited ACS system is vital to the FBI's ability to perform its mission effectively.

Yet, the VCF has proven to be the FBI's most troublesome IT challenge in the Trilogy project. Our audit found that as of December 2004 the VCF still remains under development. Moreover, after more than three years and $170 million expected to be spent developing the VCF, the FBI has not provided a clear timetable or prospect for completing the VCF.

Between January and March 2005, the FBI plans to test a "proof-of-concept," or prototype, VCF. This test is designed to demonstrate that documents can be approved electronically and uploaded into the ACS. However, this very limited version of the VCF does not provide the FBI with the intended case management and information- sharing capabilities.

Instead, FBI officials informed the OIG that a parallel effort is underway in the FBI to reevaluate and update its requirements for a case management system and to identify solutions for a multi-agency case management framework called the Federal Investigative Case Management System (FICMS). The FBI believes this will provide a blueprint to guide the FBI in eventually acquiring the capabilities that the current VCF effort has been unable to accomplish and facilitate interagency information sharing. Working with officials at the Departments of Justice and Homeland Security, the FBI expects to enter into a contract by April 30, 2005, with a vendor to develop the framework for an interagency case management system for law enforcement components of the two participating departments, including the FBI. The FBI expects the resulting case management system to use off-the-shelf technology. The FBI is serving as the executive agent to lead the process of obtaining vendor information on potential solutions and to award a contract for FICMS.

However, the FBI informed us that until it enters into the FICMS contract, which is intended to eventually result in a case management system to replace the largely unsuccessful current VCF effort, it will not know with certainty the proposed schedule and cost for completing the third component of the Trilogy project — replacing its antiquated case management system. Further, any system resulting from the FICMS effort is unlikely to benefit substantially from the 3-years and

$170 million already devoted to the VCF effort because of technological advances since the FBI began the Trilogy project in 2001 and because of the FBI's current planned approach to adapt off-the-shelf systems to meet its case management requirements.

We concluded that the delays and cost growth 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) other lessons learned over the course of the project.

History of the Trilogy Project

As noted above, the Trilogy project was intended to upgrade the FBI's 1) hardware and software — referred to as the Information Presentation Component (IPC), 2) communications network — referred to as the Transportation Network Component (TNC), and 3) the five most important investigative applications — referred to as the User Applications Component (UAC). The IPC and TNC upgrades provide the physical infrastructure needed to run the applications for the UAC portion.

Early in the project, the FBI decided it needed to modify Trilogy's design requirements due to changes in FBI priorities after the Hanssen espionage case, the belated production of documents in the Oklahoma City bombing case, and the September 11, 2001, terrorist attacks. Most significantly, the UAC concept for the project changed from consolidating a variety of existing individual user applications to developing a new overall workflow process for FBI agents, analysts, and support personnel, which became known as the VCF.[1] The VCF was intended to develop a new case management system that would vastly improve the FBI's ability to manage investigative leads, evidence, and cases; analyze and share information; and approve and manage the flow of paperwork.

[1] Although FBI documents and reports to Congress have continuously referred to the UAC as the third component of Trilogy, FBI officials in commenting on a draft of this report told us that after September 11, 2001, the VCF replaced the UAC. We use both terms in this report since FBI documents refer to the UAC as well as to the VCF user application.

Initially, the Department of Justice required the FBI to use two contractors for the Trilogy project because the project was considered too large for a single contractor to manage. The FBI combined the IPC and TNC portions of Trilogy in one contract because both components involved physical IT infrastructure enhancements. That contract was signed in May 2001 with DynCorp (which later merged into Computer Sciences Corporation (CSC)).

In June 2001, the FBI awarded a contract to develop the UAC portion of Trilogy to another contractor, Science Applications International Corporation (SAIC). The purpose of the UAC was to:

- provide the ability to find information in FBI databases without having prior knowledge of its location, and to search all FBI databases with a single query through the use of search engines;

- improve capabilities to share information inside and outside the FBI;

- provide access to authorized information from internal and external databases; and

- allow the evaluation of cases and crime patterns through the use of commercial and FBI-enhanced analytical and case management tools.

After the September 11 terrorist attacks, the FBI reviewed the two Trilogy contracts and determined that the project did not fully meet the FBI's changed IT needs because of a significant design limitation. Providing web-enablement of the existing but antiquated and limited ACS system, as was originally planned, would not provide the investigative case management capabilities required to meet the FBI's post-September 11 priorities and mission. Instead, the FBI decided to develop a new case management system, the VCF, that would make both criminal and terrorist investigation information readily accessible throughout the FBI. Further, the FBI developed plans to accelerate Trilogy's planned completion because the original 3-year modernization timeframe was considered too slow in light of the FBI's urgent need to modernize its IT.

Trilogy Schedule

Our review found that the Trilogy project has been plagued by delays, and it is still not clear when the final component of the Trilogy project (originally called the UAC and now called the VCF) will be completed. Without completion of the VCF user application, the FBI continues to lack a fully functional case management system. This raises national security implications because the FBI is continuing to rely on the ACS and paper files, which hampers FBI agents and analysts from adequately searching and sharing information from investigative files.

The original target dates for completing the IPC/TNC infrastructure and the UAC were May and June 2004, respectively. However, even before September 11, 2001, the FBI was looking for ways to accelerate this schedule.

As described in this report, although the FBI received $78 million to accelerate Trilogy, the IPC/TNC portion was not completed more quickly than the original schedule. Instead the IPC/TNC portion was completed by April 2004, only slightly before the original pre-accelerated target date of May 2004.

UAC/VCF Completion Dates

The user applications portion of the Trilogy upgrade is still not completed, and our audit found that the FBI does not know when this component will be implemented. The FBI told us that the completion date of this portion of Trilogy depends on the outcome of the FICMS contracting process that the FBI believes will eventually lead to a fully functional investigative case management system.

From its inception, this portion of Trilogy has undergone repeated revision and schedule delays. In June 2002, the FBI decided to deploy the UAC in two phases under an accelerated plan: delivery one in December 2003 and delivery two in June 2004 (a third delivery eventually was added, also for June 2004). Delivery one of the UAC was supposed to consist of the VCF, which was intended to be a completely new case management system with data migrated from the ACS. The VCF also was intended to serve as the backbone of the FBI's information management systems, replacing paper files with electronic case files. The contractor, SAIC, provided the first delivery, or version, of the VCF in December 2003 in accordance with the

accelerated schedule. However, the FBI did not accept that version because it was not a functional system and did not meet the FBI's requirements. Deliveries two and three under the current contract consisting of enhancements and additional operational capabilities to the VCF, did not occur because of the difficulties experienced in completing the initial version of the VCF. The FBI informed us that these deliveries are not being pursued given the problems in the first delivery and the FBI's plans to seek a common interagency platform for a case management system.

With continued slippage in the VCF schedule, the FBI announced in June 2004 — the original target completion date prior to the FBI's attempts to accelerate the development schedule — a new two-track plan for continuing work on the VCF involving an "Initial Operational Capability" and "Full Operational Capability." The first track is an 6-week test of an electronic workflow process scheduled to be completed in March 2005. During this test, one FBI field office and a smaller resident FBI agency office will enter investigative lead and case data into the "proof-of-concept," or prototype, VCF file system and this information will be uploaded into the ACS. Paper case files will be created through the existing ACS system upon electronic approval of the information entered into the VCF. The FBI intends to obtain user comments on, and assess the performance of, this new workflow system.

Yet, the version of the VCF being tested in Track One will not provide the FBI with the case management application as envisioned throughout the Trilogy project because it represents just one developmental step in creating a fully functional investigative case management system. The tested version does not offer case management capabilities, but rather is designed to demonstrate that documents can be approved electronically and uploaded into the existing, obsolete ACS.

The second track, called Full Operational Capability, is intended to reevaluate and update requirements for the next phase of developing a functional case management system to replace the ACS. To aid in determining the necessary requirements for a new case management system, the FBI will identify user activities and processes for creating and approving documents and managing investigative leads, evidence, and cases. The FBI states that information gleaned during Track Two will help the FBI update and confirm the case

management requirements to be met through a new interagency system that will replace the current VCF effort.

On September 14, 2004, the Department of Justice and the Department of Homeland Security (DHS) — with the FBI acting as executive agent — issued a Request for Information (RFI) to discuss with potential vendors the creation of the interagency FICMS framework because the participating investigative agencies share in common an estimated 80 percent of the case management requirements. The FICMS effort is expected to ultimately result in what the FBI expected the VCF to provide: the ability to manage investigative leads, evidence, and cases; analyze and share information; and approve and manage the flow of paperwork.

On September 28, 2004, the FBI and the Department, along with the DHS and the Office of Management and Budget (OMB), presented an overview of the FICMS concept to the potential vendors in order to obtain information on available or potential solutions to meet the Department's and DHS's case management requirements. Given the technological advances over the last three years, the FBI anticipates that an off-the-shelf federal case management system might be adapted to meet the FBI's user applications requirements.

The FBI's Chief Information Officer (CIO) told us that until a contract is signed for the FICMS project, which he expects to occur by April 30, 2005, he cannot estimate the schedule for completing an investigative case management system for the FBI.

Trilogy Costs

The current total funding for the FBI's Trilogy IT modernization project is $581.1 million. As described in the chart below, Trilogy began as a 3-year, $379.8 million project. The FBI informed Congress in its February 2002 *Quarterly Congressional Status Report* that with an additional $70 million in FY 2002 funding, it could accelerate the deployment of Trilogy. Congress then supplemented Trilogy's budget with $78 million from the Emergency Supplemental Appropriations Act of January 2002 to expedite the deployment of all three components. Therefore, total funding for Trilogy increased from $379.8 million to $457.8 million by the end of FY 2002.

In December 2002, the FBI estimated $137.9 million was needed to complete Trilogy, in addition to the $78 million it received to

accelerate completion of the project. Congress approved a $110.9 million reprogramming of funds that took into account DynCorp's estimates to complete the IPC/TNC portions, as well as an estimate of SAIC's costs to complete the UAC portion. The $110.9 million reprogramming increased the FBI's total available funding for the project to $568.7 million. In addition, $4.3 million for operations and maintenance and $8 million for computer specialist contractor support were added in FY 2003, for a total of $581.1 million.

Component Area	Original Plan ($millions)	Current Plan ($millions)
TNC/IPC	$238.6	$337.0
UAC	$119.2	$170.0
Contractor Computer Specialists	n/a	$8.0
Integrator	n/a	$5.5
Project Management	$22.0	$32.5
Management Reserve	n/a	$28.1
Total	$379.8	$581.1

Currently, the FBI has not provided an estimated completion date for the third phase of Trilogy or an estimated cost. Pending the upcoming contract for FICMS, the FBI also does not have a firm cost estimate for bringing an investigative case management system to completion.

Reasons for Trilogy's Delays and Cost Increases

Various reasons account for the delays and associated cost increases in the Trilogy project, including:

- poorly defined and slowly evolving design requirements,
- contracting weaknesses,
- IT investment management weaknesses,

- lack of an Enterprise Architecture,[2]
- lack of management continuity and oversight,
- unrealistic scheduling of tasks,
- lack of adequate project integration, and
- inadequate resolution of issues raised in reports on Trilogy.

A more detailed discussion of the reasons for Trilogy's schedule, cost, technical, and performance problems is included in the full audit report.

The combination of these factors resulted in a project that has yet to be fully implemented. The current version of the VCF will not provide the needed case management capability to replace the obsolete but still functioning ACS. Whether and how soon the FICMS effort will result in the capabilities originally envisioned for the VCF remains to be seen.

Conclusions

The FBI recognized the need to modernize its IT systems before the September 11 terrorist attacks, but that event underscored the FBI's significant problems in effectively retrieving, analyzing, and sharing investigative information needed to carry out its mission. Although attempts to accelerate completion of the Trilogy project with additional funding were unsuccessful, the FBI completed the sorely needed infrastructure upgrade portion of the project in late April 2004.

However, we remain concerned about the FBI's ability to complete and deploy the VCF so that FBI agents and analysts can effectively enter, retrieve, analyze, and share investigative case information and other data. Costing an estimated $170 million to date and in development for more than 40 months so far, the VCF is scheduled to undergo testing of workflow features of a prototype from January to March 2005. But the full VCF will not be functional or

[2] According to the Government Accountability Office (GAO), an Enterprise Architecture is a set of descriptive models such as diagrams and tables that define, in business and technology terms, how an organization operates today, how it intends to operate in the future, and how it intends to invest in technology to transition from today's operational environment to tomorrow's.

deployed at that time, and the FBI is moving away from the existing VCF as the solution for its case management requirements. Instead, the FBI is relying on the future (and uncertain) development of an interagency FICMS framework intended to result in a system that meets its case management needs. However, as of December 2004, the FBI informed the OIG it was not in a position to state the schedule or cost for completing and deploying such an investigative case management system until a FICMS contract is awarded in the third quarter of FY 2005.

In the interim, the critical need to replace the ACS, the FBI's obsolete case management system, remains. During this period, the FBI's operations remain significantly hampered due to the poor functionality and lack of information-sharing capabilities of its current IT systems.

OIG Recommendations

In this report, we make nine recommendations for improving the FBI's management of the remaining aspects of the Trilogy project and its IT management in general. These recommendations are:

- 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.

TABLE OF CONTENTS

INTRODUCTION

Background

In May 2002, the FBI Director announced a major reorganization to accomplish the FBI's top priority of preventing terrorism. To support this transition to a redesigned and refocused agency, FBI officials have repeatedly highlighted the need for new and improved information technology (IT) systems. Consequently, upgrading IT to successfully perform the FBI's mission is among the FBI's highest priorities.

Even before the September 11, 2001, terrorist attacks, the FBI realized that its IT infrastructure and case tracking system were antiquated and in desperate need of modernization. However, the September 11 attacks and subsequent focus on terrorism prevention underscored the need for IT modernization so that investigative information would be readily available throughout the FBI for analysis and "connecting the dots."

The obsolete and severely limited capability of the FBI's IT has been well-documented in prior Office of the Inspector General (OIG) reports and congressional testimony.[3] In July 2002, a former FBI project management executive testified before the Senate Judiciary Committee that agents must go through 12 computer screens just to upload one document in the Automated Case Support (ACS) system, the FBI's primary investigative computer application that uploads and stores case files electronically. The former FBI executive stated, "there's no mouse, there's no icon, there's no year 2000 look to it, it's all very keyboard intensive." The limited capabilities of the ACS and its lack of user-friendliness meant that agents and analysts could not easily acquire and link information across the FBI, and some personnel avoided the system altogether.

In March 2004, the Director referred to the FBI's IT structure, including the ACS system, as archaic. He added that at the time of the September 11 terrorist attacks, the FBI's technology systems were several generations behind industry standards, and existing legacy systems were approaching the 30-year mark. Other FBI managers

[3] The OIG reports are summarized in Appendix 2 of this report. These reports include *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case, The FBI's Management of Information Technology Investments, and The FBI's Implementation of Information Technology Recommendations.*

have stated that the implementation of Trilogy is vital to modernizing the FBI's IT infrastructure, and consequently to the FBI's ability to effectively perform its mission, including managing investigative cases and sharing information FBI-wide to help prevent terrorist attacks. While FBI officials stated that Trilogy is not intended to provide the FBI with a state-of-the-art IT system, it is intended to lay the technological foundation so that an effective IT system can be built. A former Special Agent–in-Charge in the FBI's New York City Field Office stated that "Trilogy must improve the FBI's IT systems. There is just no other way that agents can continue operating with such limited abilities."

Beginning of the FBI's IT Modernization Efforts

As discussed in the OIG report entitled *Federal Bureau of Investigation's Management of Information Technology Investments*, issued in December 2002, the FBI recognized in the 1990s that its IT infrastructure was aging and in need of modernization. Beginning in 1997, the FBI proposed improvements to its IT infrastructure and office automation. However, its major IT modernization projects went unfunded, including the Information Sharing Initiative (ISI) in 1998 and eFBI in 2000.

As a result, the FBI's IT had not been substantially improved since the early 1990s, and there was an increasingly urgent need to modernize the FBI's obsolete IT capabilities. According to FBI documents, by September 2000:

- more than 13,000 of the FBI's desktop computers were 4 to 8 years old and could not run modern software;
- the communications capability (networks) between and within FBI offices was up to 12 years old;
- most of the FBI's network components were no longer manufactured or supported;
- most resident agency offices were connected to the network at speeds equivalent to a 56k modem;
- agents were unable to reliably e-mail each other case-related information and often resorted to facsimiles; and

- agents were unable to e-mail U.S. Attorney Offices, other federal agencies, or local law enforcement agencies.

To address the need to modernize the FBI's IT systems, the FBI proposed a major technology upgrade plan to Congress in September 2000 called the FBI Information Technology Upgrade Project (FITUP). Congress appropriated $379.8 million in November 2000 to fund FITUP over a 3-year period, and the project was renamed Trilogy. The three general objectives of this IT modernization project were to:

- provide the hardware and software tools for the FBI's law enforcement mission;

- enable the FBI's investigative personnel to easily and rapidly find, present, and manipulate required information; and

- transport and share information quickly and efficiently across the FBI.

Trilogy Components and Design

In furtherance of these three general objectives, Trilogy was intended to upgrade the FBI's: 1) hardware and software, known as the Information Presentation Component (IPC); 2) communication networks, known as the Transportation Network Component (TNC); and 3) the five most important investigative applications, known as the User Applications Component (UAC).[4]

The IPC and TNC upgrades were designed to provide the physical infrastructure needed to run user applications. The IPC refers to how users view and interact with information. It provides modern desktop computers, servers, and commercial off-the-shelf office automation software, including a web-browser and e-mail to enhance usability by FBI employees. The TNC is the complete communications infrastructure and support needed to create, run, and maintain the FBI's networks. It is intended to be the means by which the FBI electronically communicates, captures, exchanges, and accesses investigative information. The TNC includes high capacity wide-area

[4] These five most important investigative applications were: 1) ACS, 2) IntelPlus, 3) Criminal Law Enforcement Application, 4) Integrated Intelligence Information Application, and 5) Telephone Application.

and local-area networks, authorization security, and encryption of data transmissions and storage.

The UAC portion was intended to upgrade and consolidate what were seen as the 5 most important of the FBI's 42 investigative applications. The heart of the UAC portion of Trilogy became the development of the Virtual Case File (VCF) to replace the obsolete ACS. Because the FBI has 37 other investigative applications and approximately 160 non-investigative applications that Trilogy was not going to include or replace, Trilogy was intended to be a starting point toward eventually upgrading the FBI's entire IT environment.

According to FBI and Department officials, the Department required the FBI to use two contractors for Trilogy because the Department considered the project too large for a single contractor to manage. In December 2000, Congress approved the obligation of $100.7 million for the first year of Trilogy, with an estimated 3-year cost of $379.8 million.

The FBI combined the IPC and TNC portions of Trilogy for one of the contracts, because both components involved physical IT infrastructure enhancements. The contract for the IPC/TNC portions was awarded in May of 2001 to DynCorp, with a first year cost of $37 million. In March 2003, DynCorp merged into Computer Sciences Corporation (CSC).

The FBI awarded Science Applications International Corporation (SAIC) the UAC portion of Trilogy in June 2001, with a first year cost of $14.7 million. The UAC defined the software-based capabilities and functions that employees can use to access and analyze investigative information. The UAC was intended to provide the FBI with:

- improved communications inside and outside the FBI;
- access to properly authorized information from internal and external databases, using primarily commercial products;
- the capability to evaluate cases and crime patterns through the use of commercial and FBI-enhanced analytical and case management tools; and
- the ability to find information in FBI databases without having prior knowledge of its location, and to search all FBI

databases with a single query through the use of search engines.

In the aftermath of the September 11, 2001, terrorist attacks, the FBI reviewed the two Trilogy contracts — infrastructure and applications — to determine if the project would still meet the FBI's needs in light of the agency's changed priorities. The FBI also developed plans to accelerate the completion of Trilogy because at the time the project's 3-year modernization timeframe was considered too long.

In addition to timeframe concerns, the review of the Trilogy contracts identified a significant design limitation. Simply providing web-enablement, or Graphical User Interface, to the ACS as originally envisioned would not yield the investigative case management capabilities required in the post-September 11 era.[5] A Trilogy project manager told us that the ACS only serves as a backup to the FBI's paper file system, that information within the system cannot be changed or updated, and the technology is still severely outdated.[6] Because the ACS is archaic, retaining the system as first envisioned under Trilogy would preclude the FBI from developing a modern system to make both criminal and terrorist investigation information readily accessible FBI-wide.[7]

But while implementation of Trilogy would mark a significant modernization of the FBI's past IT environment, the project only represented the first major steps in upgrading the FBI's IT capabilities to fully support its mission. Or as one former FBI Chief Information Officer (CIO) stated to the OIG in February 2002, the Trilogy modernization project will get the FBI's IT "out of the ditch and moving

---

[5] Web-enablement would allow the current ACS system to be upgraded from outdated "green screen" technology of the 1980s to a point-and-click technology using a mouse.

[6] In commenting on a draft of this report, the FBI stated that certain subsystems within ACS provide the ability to maintain records within the system.

[7] As discussed in the OIG report, *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case* (March 2002), the inefficiencies and complexities of 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 response to the OIG report, the FBI stated that the VCF would solve many of the problems that this report noted.

in the right direction." Additionally, because the FBI's IT systems were in such need of improvement, FBI management pressed to implement the Trilogy project as quickly as possible.

Trilogy Schedule and Budget

Recognizing the poor state of its IT even before the September 11 terrorist attacks, the FBI was examining options to accelerate the planned 3-year Trilogy project. In its July 6, 2001, *Quarterly Congressional Status Report* the FBI stated that the IPC/TNC infrastructure could be completed in June 2003, nearly one year ahead of schedule, with a two-phase implementation plan. The FBI also wanted to accelerate deployment of the urgently needed user applications component, which was scheduled to take three years.

The September 11 attacks provided even greater impetus to completing Trilogy, and the FBI continued to explore options to accelerate deployment of all three Trilogy components. The FBI informed Congress in its February 2002 *Quarterly Congressional Status Report* that it had developed a new plan with DynCorp to complete the IPC/TNC phases by December 31, 2002, or nearly 18 months earlier than originally planned. Additionally, the status report stated that SAIC had developed a plan to make the ACS web-enabled by July 2002 – 24 months earlier than scheduled – without increasing project costs.

The FBI also informed Congress in its February 2002 report that with an additional $70 million in FY 2002 funding, the FBI could further accelerate the deployment of Trilogy. This acceleration would include completing the IPC/TNC phases by July 2002 instead of December 2002, and delivering by March 2004 (four months early) the most important analytical tools as part of the UAC phase. Congress supplemented Trilogy's FY 2002 budget with $78 million from the Emergency Supplemental Appropriations Act of January 2002 to expedite the deployment of all three components. This appropriation increased the total funding of Trilogy from $379.8 million to $457.8 million.[8]

[8] Of the $457.8 million, about $107.6 million was identified by FBI management as funding offsets, or cost savings, from other FBI operations that Trilogy would replace.

In December 2002, the FBI identified a need for an additional $137.9 million to complete the Trilogy program. Congress subsequently approved a $110.9 million reprogramming request to help meet this need. This reprogramming was anticipated to fund Dyncorp's estimates to complete the IPC/TNC portions of Trilogy, as negotiated, as well as an estimate of SAIC's costs to complete the UAC portion of the project. The reprogramming increased the FBI's total available funding for Trilogy to $568.7 million. Another $4.3 million for operations and maintenance and $8 million for computer specialist contractor support were added in FY 2003 for a total of $581.1 million. According to FBI documents, by the end of January 2004 the FBI had obligated about $559.6 million for Trilogy. The following table shows Trilogy's budget, by component area, as of January 2004.[9]

[9] In commenting on a draft of this report, the FBI stated that the infrastructure contractor, CSC, did not spend approximately $5.7 million and that these funds would be returned to the FBI. The FBI also said it recently revised the Trilogy budget and decreased total infrastructure costs by $2.8 million.

Trilogy Budget by Component Area

Component Area	FY	Original Plan ($millions)	January 2004 Revision Based on TNC/IPC Contractor Proposals* ($millions)
	2001	$68.0	$65.7
	2002	$87.8	$171.6
	2003	$82.8	$98.6
	2004	n/a	$1.1
TNC/IPC	Subtotal	$238.6	$337.0
	2001	$24.7	$25.2
	2002	$46.6	$26.8
	2003	$47.9	$115.8
	2004	n/a	$2.2
UAC	Subtotal	$119.2	$170.0
Contractor Computer Specialists	Subtotal	n/a	$8.0
Integrator	Subtotal	n/a	$5.5
	2001	$8.0	$7.1
	2002	$8.0	$8.2
	2003	$6.0	$13.9
	2004	n/a	$3.3
Project Management	Subtotal	$22.0	$32.5
Management Reserve	Subtotal	n/a	$28.1
Total		**$379.8**	**$581.1**

* Note: totals within this category include adjustments from the beginning of the project through January 2004.

Source: FBI *Quarterly Congressional Status Reports*

In addition, the following table shows how the FBI's estimates for completing the three Trilogy components, as periodically reported to Congress, fluctuated dramatically up until June 2004.

Trilogy's Development Schedule
(According to FBI Quarterly Congressional Status Reports)[a]

Component Area	Original Completion Target	Nov 2001[b]	Feb 2002[b,c]	Feb 2002[b,c]	June 2002[b]	Sept 2002[b]	Apr 2003[b]	Feb 2004[b]	June 2004[b]
IPC/TNC Completion[d]	May 2004	Jun 2003	Dec 2002	Jul 2002	Mar 2003	Mar 2003	Dec 2003	Oct 2003	Complete Apr 2004
Fast Track					Apr 2002	May 2002	Complete Dec 2002	Complete Dec 2002	Complete Dec 2002
Extended Fast Track					Oct 2002	July 2002	Complete Mar 2003	Complete Mar 2003	Complete Mar 2003
Full Site Capability					Mar 2003	Mar 2003	Dec 2003	Oct 2003	Complete Apr 2004
UAC Completion[d]	Jun 2004	Jun 2004	Jul 2002	Mar 2004	Jun 2004	Jun 2004	Jun 2004	Unknown	Unknown
ACS Web Enablement			Jul 2002	Cancelled					
Delivery 1					Dec 2003	Dec 2003	Dec 2003	Unknown	Unknown
Delivery 2					Jun 2004	Jun 2004	Jun 2004	Unknown	Unknown
Delivery 3							June 2004	Unknown	Unknown

Source: FBI *Quarterly Congressional Status Reports*

Notes: (a) This schedule does not include all of the quarterly reports submitted by the FBI, but does include those where significant scheduling changes took place.
(b) Dates represent the submission date for the FBI's Trilogy Program *Quarterly Congressional Status Report*. These reports were required by P.L. 106-553, *Department of Commerce, Justice and State, the Judiciary, and Related Agencies Appropriations Act, 2001*. The reports generally covered the quarter prior to the issuance date.
(c) Two reports were issued in February 2002.
(d) The schedule includes the portions of the components (e.g., Delivery 3) as they were initiated by the FBI during the course of the Trilogy project.

Project Management and Contractor Assistance

In addition to the Trilogy project's infrastructure and application components, the original Trilogy plan included a management process function, referred to as Program Management. Trilogy was to be managed under a Deputy Assistant Director, dedicated solely to the program, within the FBI's Information Resources Division. The Division employees who were responsible for the Trilogy program were to have no responsibilities outside of the Trilogy project. Shortly after the initiation of the Trilogy project, however, the FBI made management changes, including establishing a CIO position. The CIO brought in a Project Management Executive to manage the Trilogy project in place of the Deputy Assistant Director in the Information Resources Division.

Over the course of the Trilogy project, the FBI acquired contractor assistance to work on the project. For example, contractor computer specialists were brought into the Trilogy project in January 2002 when the FBI tried to accelerate the Trilogy project. The specialists, budgeted at $8 million, worked on infrastructure aspects of the project. A project integration contract was approved through the FBI's $20 million reprogramming request in December 2002.[10] However, the integrator, SAIC, was not brought on until the end of 2003. In an effort to limit costs, the FBI has initiated a contract termination. As of April 2004, SAIC had received over $2.8 million for project integration services.

Other Trilogy Contract Issues

At the outset of FITUP/Trilogy, the Department required the FBI to use two contractors because the project was so large. To expedite the contracting process, the FBI decided to use the General Services Administration's (GSA) Millennia contracting process. The GSA's Federal Technologies Services' Federal Systems Integration and Management (FEDSIM) Center provides IT contracting services for its federal agency clients. FEDSIM's role is to oversee competing contracts, and to award and manage existing contracts. In other words, FEDSIM acts as the contracting office. FEDSIM developed

[10] A project integrator provides the overall planning and coordination during the implementation of a new system. The tasks an integrator performs include the defining of requirements for system implementation, scheduling, and ensuring that testing is performed.

Millennia for contracts involving software engineering, system integration, or communications. Pre-approved contractors who could bid on an IT system contract were identified, and as a result contracts could be awarded much more quickly than through the traditional process where hundreds of bids might have to be evaluated. With Millennia, 11 contractors under the auspices of FEDSIM competed for the 2 Trilogy contracts. The Trilogy contract was offered as a cost-plus-award fee on labor whereby the contractors' costs are reimbursed and fees can be awarded to the contractor. Some smaller aspects of the contract were fixed-price. According to FEDSIM officials, a cost-plus-award-fee contract is not unusual for developing a system where there are many unknowns and risks, and the contract allows for sharing the risk between the contractor and the contracting agency.

The Department also initially required that the FBI perform the project integration function rather than hiring a contractor. A project integrator manages how each piece of the project will fit together smoothly. Because the Trilogy project included hardware, networking, and user application components, the integrator would determine when the equipment associated with the hardware and networking portions would be ready for the user applications to be installed and utilized. However, the FBI did not have sufficient project integration expertise, especially for such a large and complicated IT project.

Although an outside project integrator was not hired at this time, the FBI used a contractor, Mitretek Systems, to assist the FBI with a wide array of tasks, including program and contract management, system engineering and architecture, fiscal and budgetary oversight, communications, testing, configuration management, cost estimating, acquisition and source selection, requirements definition, training, database management, security certification and accreditation, and web development.

FINDINGS AND RECOMMENDATIONS

Finding: The Schedule, Cost, Technical, and Performance Baselines of the Trilogy Project

While Trilogy has greatly improved the FBI's information technology infrastructure, the critical VCF application remains incomplete and will not result in the required modernization of the FBI's case management system in the foreseeable future. The FBI plans to pilot test a prototype VCF by early 2005, but this test and subsequent evaluation will only involve workflow processes in conjunction with the existing ACS system, rather than a fully functional case management system. On a separate track, the FBI is leading an interagency effort to develop a Federal Investigative Case Management System (FICMS) framework, which is intended to lead to the development of fully functional investigative case management systems for the Departments of Justice and Homeland Security. However, the FBI will not have schedule and cost estimates for FICMS and the resulting case management system until April 2005 at the earliest, when it awards the FICMS contract. While the completed infrastructure components of Trilogy have provided the FBI with a sorely needed IT upgrade, the continuing lack of an effective case management system hinders the FBI's capability to perform its critical national security mission.

Additionally, the Trilogy project has been plagued throughout its development with missed deadlines and rising costs. While events affecting both the mission and operations of the FBI resulted in project modifications, had the Trilogy contracts included fully established requirements and firm completion milestones, the adverse effects of such changes could have been mitigated. Recently, the FBI has restructured and tightened its IT management and now intends to more rigorously manage its pursuit of a new solution to its case management requirements.

Need for Trilogy

Both the FBI's IT infrastructure and its case management system were in dire need of modernization at the time of Trilogy's initiation. Both aspects of the project are extremely important and interrelated — without the upgraded infrastructure a modern, fully functional case management system with information-sharing capabilities could not be implemented. At the same time, without an effective case management system the FBI cannot identify and capitalize on all of the information in its possession. With the completion of Trilogy's infrastructure components, the FBI has the ability to support an enhanced case management system. However, without a modern, fully functional case management system in place, agents and analysts largely rely on paper case files and an existing but obsolete case support system. Consequently, agents and analysts are at a severe disadvantage in performing their duties.

Infrastructure Components

In April 2004, the FBI completed the infrastructure components of Trilogy. However, although Congress funded an accelerated schedule for completing these components, the FBI only met the original target date. As described in the Introduction section of this report, for much of the Trilogy project's history the FBI had never established a stable schedule for development and deployment of the infrastructure components. Beginning in 2002, the FBI's estimated dates for completing the infrastructure began to fluctuate and were revised repeatedly. At one point, the FBI moved up the target completion date for deploying the Trilogy infrastructure from May 2004 to June 2003 in light of the September 11 attacks and the need to enhance the FBI's IT infrastructure as rapidly as possible. Subsequently, the FBI said the infrastructure deployment would be completed by December 2002. After receiving additional funding from Congress in FY 2002 to accelerate the project, the FBI again revised the completion date for the infrastructure to July 2002.

The plan to accelerate Trilogy involved deploying the IPC/TNC infrastructure enhancements in three phases. The first phase, called Fast Track, included the installation of Trilogy hardware in FBI field offices and the larger resident agencies. The Fast Track deployment consisted of new network printers, color scanners, local area network upgrades, desktop workstations, and office automation software. FBI officials reported that by the end of December 2002, all field offices

had Fast Track completed. This included 22,251 workstations, 3,408 printers, 1,463 scanners, and 475 servers.

Following the completion of Fast Track, the FBI initiated the next phase of the hardware deployment, Extended Fast Track. Completed in March 2003, Extended Fast Track: 1) installed servers and other network components at field office and resident agency sites, and 2) deployed the hardware included under Fast Track to additional resident agency sites that were not included in the first phase. The FBI also intended Extended Fast Track to correct any shortfalls in the distribution of hardware to the field offices that occurred in the original Fast Track deployment. During this phase, the FBI also deployed a wide area network (WAN) for 593 FBI sites. The WAN was certified and accredited to meet the security requirements for operating within the FBI.

The final phase of the infrastructure deployment, called Full Site Capability, represented the complete infrastructure upgrade. This phase provided WAN connectivity together with new encryption devices, new operating systems and servers, and new and improved e-mail capability. However, completion of this phase involved extensive contract renegotiations with Computer Sciences Corporation (CSC), into which DynCorp had merged, and increased efforts on the FBI's part to manage the project and encourage CSC to complete the Full Site Capability. The final year of the infrastructure component's evolution is discussed below.

The milestone for completing the infrastructure components slipped from the initial date of July 2002 to March 2003. On March 28, 2003, CSC completed the Local Area Network (LAN) for Trilogy. In March 2003, the FBI Director reported to Congress that the Trilogy LAN — with increased bandwidth and three layers of security — had been deployed to 622 sites.

In April 2003, the FBI and CSC agreed to a statement of work for the remaining infrastructure components of Trilogy, including servers, upgraded software, e-mail capability, and other computer hardware, with final engineering change proposals and a completion date of October 31, 2003. In August 2003, CSC informed the FBI that the October 2003 completion date would slip another two months to December 2003. In October 2003, CSC and the FBI agreed that the December 2003 date again would slip. In November 2003, the GSA's FEDSIM announced that CSC failed to meet the deadline for

completing work on the infrastructure portions of Trilogy that are required to support the user applications, including the VCF.

On December 4, 2003, CSC signed a commitment letter agreeing to complete the infrastructure portions of Trilogy by April 30, 2004, for an additional $22.9 million, including an award fee of over $4 million.[11] The FBI covered these additional costs by reprogramming funds from other FBI appropriations. In January 2004, the FBI converted the agreement with CSC to a revised statement of work providing for loss of the award fee if CSC did not meet the April 30, 2004, deadline. In addition, the revised statement of work provided for a cost-sharing rate of 50 percent if any work remained after April 30.

In April 2004, CSC installed the final infrastructure pieces in FBI field offices needed to use the previously deployed WAN, thereby completing the infrastructure portion of the project and meeting its contractual requirements. In the end, CSC completed the infrastructure component by May 2004 – the FBI's original target date – but missed the completion date under the accelerated schedule funded by Congress by some 22 months. The total expected costs for the infrastructure components of Trilogy increased from $238.6 million to $339.8 million over the course of the project.

User Applications and the Virtual Case File

The design of and schedule for the UAC portion of Trilogy were substantially modified after the September 11 attacks. The most significant design change was eliminating the web-enablement of ACS and instead developing an enterprise-wide solution to replace ACS, an obsolete and inconsistently utilized case information system. The replacement for the web-enablement of ACS was to be deployed in two phases under an accelerated plan: delivery one and delivery two. A third delivery was added in March 2003.

Delivery one of the UAC was intended to consist of a new application known as the Virtual Case File (VCF). The VCF was intended to be a completely new investigative case management system with data migrated from the ACS. The VCF was to serve as the backbone of the FBI's information systems, replacing the FBI's paper case files with electronic files. The first delivery of VCF was targeted

[11] An award fee is a financial incentive provided to a contractor, based on the contractor's performance, as a form of motivation to meet directed baselines.

for completion in December 2003. The second and third deliveries, which were intended to upgrade and add additional investigative applications to the VCF, were targeted for completion in June 2004.

At the outset of the Trilogy project, the UAC was intended to replace each of the following five primary user applications:

- ACS, the FBI's primary investigative application;
- IntelPlus, which allows scanning, importing of electronic documents, and full-text retrieval capabilities;
- the Criminal Law Enforcement Application (CLEA), a repository of criminal investigation data;
- the Integrated Intelligence Information Application (IIIA), which supports counterintelligence and counterterrorism investigations by enabling the collection, collation, analysis, and dissemination of intelligence; and
- the Telephone Application (TA), which provides a central repository for telephone data obtained from investigations.

According to one VCF project manager, the plan to replace each of the FBI's five primary investigative applications was not based on an objective evaluation of the operational needs of the organization, but rather on an assumption made by the FBI's IT managers at the time that replacing these applications would have the greatest benefit for agents and analysts.[12] The FBI refined the VCF concept through Joint Application Development (JAD) sessions held between January and June 2002. The JAD sessions brought together FBI representatives to determine what applications were needed to support the case management and information requirements of FBI agents, analysts, and support personnel; UAC contractor representatives to determine what applications could be created; and infrastructure contractor representatives to ensure that the applications could be supported by the groundwork that was being developed.

[12] In commenting on a draft of this report, the FBI stated that the five primary applications were selected because they were the applications used most frequently by agents in support of investigative activities and that this was a reasonable set of applications to pursue given the original approach of "webifying" the ACS.

The VCF plan that resulted from these JAD sessions in 2002 rejected the previous plan to replace the five separate investigative applications in favor of developing an entirely new electronic workflow with systems that are integrated into one process. The VCF concept not only would change where the data for case files is stored, but also would create an entirely new environment in which agents, analysts, and support personnel operate. This workflow would be based on the information required to create case files and would combine aspects of ACS, CLEA, and TA applications into one application. After these sessions, the FBI removed IntelPlus from the planned VCF to avoid redundancy with the current version of the Information Data Warehouse (IDW) project and the revamped VCF.[13]

Implementation of the VCF would require a complete change in how agents establish case files. Rather than creating paper records as they currently do, agents would be required to input case information into the VCF electronically to complete a series of data fields. The data fields would be tagged so that the information entered into the VCF is consistent throughout the system. These electronic "case files" would be the sole case files utilized by the FBI, so that only one set of data would exist for a case and only one search within the VCF would be required to locate and view case-related information.

VCF case files would enable a wide variety of functionalities. For example, when a "parent" case file is established by one FBI field office and an action relating to that case is taken by another field office (such as a fraud case in New York requiring a summons being delivered in Philadelphia), a "child" to the original case file can document all of the activities related to the parent case. This capability would allow the entire case history to be traceable from initiation through closure.

In addition, the VCF was intended to include a multimedia capability that would rectify a longstanding information-sharing limitation within the FBI. Agents would be able to scan documents, photographs, and other electronic media into the case file. This capability would allow evidence and other case-related information to

[13] However, while the IIIA application's functionality was to be captured within the VCF, the migration of the IIIA data may not be a part of the VCF because, according to one VCF project manager, agents utilized the system inconsistently and the data within the application may not be complete. The FBI told us it is reviewing the IIIA data to determine if it will be captured in the ACS data migration to the VCF.

be shared among agents working on a case FBI-wide without the need to exchange physical copies of the information. Also, under the case structure established in the first delivery of the VCF, the Reports on Investigative Activity (RIA) component of a case eventually would allow data comparisons and correlations to be made between cases in order to "connect the dots."[14]

According to a former VCF project manager at the FBI, the VCF would also incorporate additional applications to aid agents' work. For example, because ACS does not offer statistical reporting capabilities, agents have had to perform such tasks using a separate application outside of ACS. The VCF would incorporate the features of the Integrated Statistical Reporting and Analysis Application, which maintains case-related statistics such as the number of investigative leads that result in arrests and convictions. The VCF also would allow agents to request funding for cases rather than to have to enter requests through a separate financial management system.

Current Schedule for User Applications Component

The VCF contractor, SAIC, delivered the first of three planned system deliveries for the VCF in December 2003. However, the application was not fully functional and the FBI did not accept the product. FBI officials stated that 17 issues of concern pertaining to the functionality and basic design requirements of the VCF needed to be resolved before the application could be deployed. According to FBI personnel working on the resolution of these problems, the 17 issues were corrected as of March 7, 2004.

However, significant work still remained on the VCF, including security aspects and records management issues. As a result, the FBI revised the VCF deployment schedule again. Rather than having the VCF implemented and enhanced in three deliveries, the FBI Director announced in June 2004 that development of the project would be split into two parallel tracks, "Initial Operational Capability" (IOC) and "Full Operational Capability" (FOC). Neither Track One, the IOC, nor Track Two, the FOC, will result in the deployment of a fully functional VCF with case management capabilities. As discussed in more detail below, the two tracks will test a limited VCF paperwork flow feature

[14] The RIA component consists of current data collected within a file whenever an agent performs investigative work on a lead or case. The data within the RIA would be entered into the VCF within established data fields. An enhancement to the VCF would allow for the data to be compared to other leads or case files.

and continue to identify and refine user requirements that the FBI believes will eventually lead to the development of a new case management system through the Federal Investigative Case Management System (FICMS) effort to replace the stalled VCF project.

On July 30, 2004, the FBI signed a contract modification with SAIC to work on Track One. By December 31, 2004, SAIC provided the FBI a "proof-of-concept" or prototype VCF. This prototype is being used by agents and analysts in a test field office to demonstrate an electronic workflow process in ongoing investigations. Over a 6-week pilot test period scheduled between January and March 2005, the FBI's New Orleans Field Office and the Baton Rouge Resident Agency are entering actual investigative lead and case data into the VCF. This information will be uploaded into the ACS to create paper case files upon electronic approval of the electronic information in the VCF.

Yet, the version of the VCF tested in Track One will not provide the FBI its goal of a paperless records management application or a system that will handle the vital investigative leads, evidence, and case management application. Rather, the goal of the Track One test phase is to determine the efficiency and effectiveness of the electronic workflow and document approval process — even while still using the antiquated ACS system. Due to its limited progress in developing the VCF, the FBI has determined that SAIC will not provide the previously planned second and third deliveries. These enhancements were intended to upgrade the VCF's capabilities and provide a deployable VCF that would enable the FBI to efficiently manage its investigative cases and documents and allow agents and analysts to access and share investigative information much more effectively.

Track Two, the FOC, also will not result in the delivery of a fully functional VCF. Instead, Track Two represents an effort to reevaluate and identify new requirements for developing a functional case management system to replace the ACS. Under Track Two, the FBI is identifying requirements for a new system, including user activities and processes for creating and approving documents and managing investigative leads, evidence, and cases. As a part of Track Two, a separate contractor, The Aerospace Corporation, evaluated the initial VCF delivery to determine the extent to which the design can be of further use to the FBI.

In essence, under Track Two, the FBI will update system requirements for the future development of a case management system.[15]

The VCF effort that began in June 2001 has been unable to meet the FBI's case management needs. Instead, the FBI has taken a new approach for pursuing the development of a case management system. On September 14, 2004, the Departments of Justice and Homeland Security, in conjunction with the Office of Management and Budget, released a Request For Information for the FICMS (see Appendix 3). The FICMS is intended to result in a common platform in support of a multi-phased program to modernize investigative and intelligence processes within the federal government as a whole. On September 28, 2004, the Departments of Justice and Homeland Security — with the FBI acting as the executive agent — presented an overview of the FICMS to vendors in order to obtain information on existing or potential solutions for this multi-agency case management system.[16] Nearly 100 vendors, including SAIC, attended the FBI's presentation, which included a discussion of the challenges facing the FBI in implementing the VCF, as well as the requirements that have been identified in working on the VCF. The requirements include creating and managing electronic case files; assigning cases; integrating workflow and document management including the creation, review, collaboration, approval, storage and disposition of documents; evidence management; and records search and reporting. The FICMS overview also outlined security measures and labeling requirements for national security information.

The FBI told the OIG that it anticipates issuing a Request for Proposals by about January 2005 and awarding a contract by April 30, 2005, to develop the FICMS framework through a step-by-step modular approach. The FBI hopes that through this approach the

---

[15] In commenting on a draft of this report, the FBI stated that Track Two is in essence the FICMS effort that is expected to eventually result in a fully functional investigative case management system.

[16] The FBI's CIO stated that the FBI's involvement in FICMS stems from both the Office of Management and Budget and Executive Order 13356 entitled *Strengthening the Sharing of Terrorism Information to Protect Americans*, signed on August 27, 2004 (see Appendix 4). The Executive Order provides guidance to organizations that possess or acquire terrorism information on issues relating to the sharing of such information among agencies. Part of the guidance is to establish an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies.

project will be broken down into manageable components such as workflow, security, records management, evidence management, investigative leads management, and administration. Further, the system architecture will be developed to comply with the information-sharing requirements of Executive Order 13356.

However, until the FICMS framework is developed and an investigative case management system is developed and deployed, the FBI will continue to use the poorly functioning ACS to manage its cases. The FBI is unable to provide even a rough estimate of the schedule or costs for developing the FICMS framework and resulting system until it receives and evaluates the contractors' proposals. In the meantime, FBI personnel will continue to use paper files and the limited capabilities of the antiquated ACS. Although the FBI emphasized that it has scanned a multitude of documents into its data warehouse, this document repository does not equate to the case management and information-sharing and searching capabilities envisioned for the VCF.

The Current VCF Application Will Not Meet the FBI's Needs

After committing over three years and $170 million — nearly $51 million more than initially estimated — the FBI thus far has not completed the original UAC portion of Trilogy, the critical VCF.

The urgent need within the FBI to create, organize, share, and analyze investigative leads and case files on an ongoing basis remains unmet. As of December 31, 2004, the VCF will only result in a test version of a new workflow system involving the capability to upload of documents into the ACS system. From that point, the FBI is further refining the user needs and more fully developing requirements for a future investigative case management system. The FBI is now counting on the interagency FICMS effort to eventually result in a modern case management system primarily using off-the-shelf technology that was unavailable in 2001 when Trilogy's development began.

According to the FBI's CIO, about 80 percent of the FBI's case management system requirements are consistent with other federal investigative agencies, so that a "flagship" platform such as that envisioned through FICMS is feasible. Further, the FBI CIO said that using existing IT solutions in developing a case management system under FICMS (commercial off-the-shelf systems or government off-

the-shelf systems) should reduce its costs that will be shared by the participating agencies. The FBI expects to pay its share of FICMS developmental costs by reprogramming some of its IT appropriations. The extent to which the VCF development effort to date can be leveraged in developing an interagency case management platform is unknown at this point, because the FICMS is in its early conceptual stage. In our opinion, although the VCF effort helped the FBI define its user requirements, a successor case management system is unlikely to benefit substantially from the VCF from a technical or engineering standpoint due to: 1) advances in technology during the lengthy VCF developmental process, and 2) the FBI's intended approach of adapting existing systems to provide the various components of the case management system.

Although the development of an interagency investigative case management system is desirable to enable information to be shared across agencies, Trilogy was supposed to provide case management and information-sharing capabilities for the FBI. While the FBI is looking toward developing a system through the FICMS effort to ultimately replace the largely unsuccessful VCF, the ability of the FBI to adequately compile, analyze, and share case information within its own organization will be delayed as the FICMS framework and resulting system are developed.

Problems in Trilogy's Development

We found that the delays and associated cost increases in the Trilogy project have resulted from several factors, including:

- poorly defined and evolving design requirements,
- contracting weaknesses,
- IT investment management weaknesses,
- lack of an Enterprise Architecture,
- lack of management continuity and oversight,
- unrealistic scheduling of tasks,

- lack of adequate project integration, and

- inadequate resolution of issues raised in reports on Trilogy.

The combination of these factors has resulted in a Trilogy project that received significant additional funding to accelerate completion, but that after three years has not been fully implemented. It now appears that the multi-agency FICMS effort, which currently is purely conceptual, will result in a replacement of the existing inadequate VCF as the FBI's solution to meet its need for an investigative case management system. A discussion of the reasons for Trilogy's schedule, cost, technical, and performance problems follows.

Poorly Defined and Slowly Evolving Design Requirements

One of the most significant problems with managing the schedule, cost, and technical aspects of the Trilogy project was the lack of a firm understanding of the design requirements by both the FBI and the contractors. Trilogy's design requirements were ill-defined and evolving as the project progressed. In addition, certain events required the need to modify initial design concepts. For example, after the September 11 attacks the FBI recognized that the initial concept of simply modifying the old ACS would not serve the FBI well over the long run. The FBI then created plans for the VCF. Additionally, a need for broadened security requirements due to vulnerabilities identified in the Hanssen espionage case affected Trilogy's development. According to one project manager, this recognition of the need to upgrade security caused more problems and delays for the full implementation of the infrastructure component.[17]

During the initial years of the project, the FBI had no firm design baseline or roadmap for Trilogy. According to one FBI Trilogy project manager, Trilogy's scope grew by about 80 percent since initiation of the project. Such large changes in the requirements meant that the specific detailed guidance for the project was not established, and as a result a final cost and schedule was not established. The project manager stated that for future projects, requirements must be defined

[17] In commenting on a draft of this report, however, the FBI disputed the project manager's explanation, saying that security requirements were initially identified within the base contract. Instead, the FBI cited the addition of a new e-mail function as the primary reason for the schedule delays along with the implementation of a product assurance program.

in specific detail, and all parties involved in such a project must be onboard with the requirements.

Another problem in managing Trilogy was the limited engineering capabilities of the FBI and the contractor in creating the VCF. In January 2004, the acting Chief Technology Officer brought in a group of engineering contractors to review technical and performance aspects of the VCF. This review examined the technical design decisions, reliability, performance, and resiliency of the system being developed by the contractor. The main objective of the group was to identify fundamental design flaws. The group's decision paper cited 37 basic design flaws, including network, server, and storage infrastructure issues, operating system and software issues, application issues, and problems with the test plan. The lack of redundancy and resiliency in the system was seen as a major flaw because the design failed the basic "can of soda" test. This test simply shows that if a can of soda were to be spilled on one of the servers, causing it to fail, that server's backup would also fail because it was located directly below and would also be damaged by the liquid.

The contractors performing the review stated that the VCF design was adversely affected by a lack of engineering expertise on the project. The group said that the FBI should have approached developing the Trilogy system from an engineering perspective rather than just by relying on what the system should achieve for the user. According to the contractors, this approach should have been implemented from the outset of the project so that the FBI could have acted as an educated consumer, directing more of what the contractor should have been implementing in the technical development of the VCF rather than just from a user perspective.

The current status of the VCF demonstrates that the lack of fully developed requirements for the project negatively affected schedule, cost, technical, and performance baselines. At this point in the project's development, a limited-use application that will continue to create paper files is the most optimistic outcome of the current Trilogy user application contract. However, the technical and performance requirements for the future inter-agency case management system are yet to be fully defined.

Contracting Weaknesses

The FBI's current and former CIOs told us that a primary reason for the schedule and cost problems associated with Trilogy was weak statements of work in the contracts. According to FBI IT and contract managers, the cost-plus-award-fee type of contract used for Trilogy:

- did not require specific completion milestones,
- did not include critical decision review points, and
- did not provide for penalties if the milestones were not met.

Under cost-plus-award-fee contracts, contractors are only required to make their best effort to complete the project. Furthermore, if the FBI does not provide reimbursement for the contractors' costs, under these agreements the contractors can cease work. Consequently, in the view of the FBI managers with whom we spoke, the FBI was largely at the mercy of the contractors. A Trilogy project manager compiling lessons learned from the project told us that the FBI should require all future IT projects to operate solely with fixed-price contracts that contain award fees.[18] He stated that this type of contract would greatly enable the FBI to achieve the results being sought without relying too heavily on contractors. However, in order to use such contracts, the manager noted, the FBI must have much more fully defined requirements for a project.

Because the FBI wanted to award the Trilogy contracts quickly and did not have clearly defined requirements, it used the cost-plus-award-fee contract vehicle. While the contracting process was expedited, the lack of well-defined requirements severely affected the timeliness and cost of the implementation of the Trilogy project.

IT Investment Management Weaknesses

At Trilogy's inception and over much of its life, the FBI's IT Investment Management (ITIM) process was not well-developed, as described in the OIG's December 2002 audit report, *The Federal Bureau of Investigation's Management of Information Technology*

[18] An award fee is a financial incentive provided to a contractor, based on the contractor's performance, as a form of motivation to meet directed baselines.

Investments. That audit found that while the FBI had started centralizing its project management structure, it still needed to integrate its ITIM process with a standardized project management methodology. Specifically, the report stated that project management was not consistently followed by IT project managers and policies and procedures were not developed for management oversight of IT projects. This lack of oversight included a lack of project management plans that would include cost and schedule controls.

The report included a brief case study of Trilogy, and the lack of a mature ITIM process was found to contribute to the missed milestones and uncertainties associated with Trilogy. The report stated that most of Trilogy's development had been managed in a "stovepipe," and as a result FBI personnel not involved in the management of Trilogy had little knowledge of the project's status and progress. Additionally, there was little coordination among Trilogy management and contract specialists from the Finance Division or the Information Resources Division unit responsible for procurement of non-Trilogy IT needs. Finally, the philosophy employed in implementing Trilogy, according to the original FITUP plan, was "to get 80% of what is needed into the field now rather than 97% later. Then we can proceed in an orderly fashion to move toward 100% in the future." In essence, the FBI took risks to expedite Trilogy's implementation to the field, and that approach failed because the management processes requiring the creation of baselines for Trilogy were simply not in place.

Had the FBI developed a mature ITIM process — and the schedule, cost, technical, and performance baselines for the project been fully developed through the ITIM process — the Trilogy project likely could have been completed more efficiently and timely. The development of a mature ITIM process is ongoing within the FBI, and most of the recommendations of the OIG's report on this subject have been implemented. However, absent a mature ITIM process, all FBI IT investment efforts are at a risk for the significant developmental problems experienced by Trilogy.

Lack of an Enterprise Architecture

An Enterprise Architecture provides an organization with a blueprint to more effectively manage its current and future IT infrastructure and applications. As stated in the Government

Accountability Office's (GAO) report *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, issued in September 2003, the development, maintenance, and implementation of Enterprise Architectures are recognized hallmarks of successful public and private organizations. The GAO reported that the FBI does not have an Enterprise Architecture, although it began developing one in early 2000. The GAO also found that the FBI lacks the management structures and processes to effectively develop, maintain, and implement an Enterprise Architecture.

Additionally, the OIG's December 2002 audit report entitled *FBI's Management of Information Technology Investments* recommended that the FBI continue its efforts to establish a comprehensive Enterprise Architecture. The report also recommended that the FBI develop and implement a specific plan to integrate the ITIM and Enterprise Architecture processes. While the FBI agreed to develop a comprehensive Enterprise Architecture, this recommendation has not been fully implemented. The FBI has contracted for an Enterprise Architecture to be completed by September 2005. Without a complete Enterprise Architecture, the FBI's systems are not defined. As a result, in the Trilogy project the FBI needed to conduct reverse engineering to identify existing IT capabilities before developing the infrastructure and user applications requirements.

Lack of Management Continuity and Oversight

Turnover in key positions has inhibited the FBI's ability to manage and oversee the Trilogy project. Since November 2001, 15 different key IT managers have been involved with the Trilogy project, including 5 CIOs or Acting CIOs and 10 individuals serving as project managers for various aspects of Trilogy. This lack of continuity among IT managers contributed to the lack of effective and timely implementation of the Trilogy project.

According to contractor personnel who are advising the FBI on Trilogy, the FBI has suffered from a lack of engineering expertise, process weaknesses, and decision making by committees instead of knowledgeable individuals. In the opinion of the contractors with whom we spoke, weak government contract management was more of the problem with Trilogy than the terms of the contracts.

In addition to the lack of consistent management, the processes used to manage Trilogy were also inadequate. For example, the FBI's ability to adequately track Trilogy costs was questioned by a March 3, 2004, FBI inspection report. The inspection review was conducted to ensure that transactions for the Trilogy project were documented and recorded accurately, and to determine whether the financial management of the Trilogy project was in compliance with federal regulations and FBI policies and procedures.

The inspectors found that the FBI's Financial Management System did not capture detailed Trilogy-related expenditures, while numerous entities tracked and monitored specific segments of the operation. Overall, Trilogy-related financial records were fragmented and decentralized with no single point of accountability. The FBI's Project Management Office did not implement a centralized budget, accounting, and procurement structure to ensure global financial management oversight.

The report also found that an individual functioning in an advisory role to the FBI for increasing funding of the various contracts associated with Trilogy worked for a contractor that provided IT services on Trilogy. As a result, the inspectors found a conflict of interest in decision-making regarding the Trilogy project. Additionally, although the contractor maintained detailed records for vendor invoicing as part of her bookkeeping duties, she did not have access to overall FBI financial data and therefore was unable to provide the FBI with a complete picture of Trilogy costs.

Finally, the FBI internal report stated that the Budget Unit of the FBI's Information Resources Division was not reconciling or updating portions of the Trilogy tracking report, which resulted in discrepancies in the dollar amounts reported to management. During the review, the inspectors gave the information to the Budget Unit in order to coordinate a reconciliation of the Trilogy project's funding.

The FBI said it has resolved these issues, but the cost-reporting problems that occurred demonstrate another area in which a thorough, regimented program management framework would have allowed the FBI to better capture and monitor expenditures and funding for the Trilogy project.

We interviewed officials in the FBI, the Department, and FEDSIM, many of whom said that the FBI recently has improved its

management and oversight of Trilogy and of IT in general. The FBI appears to have hired capable IT managers from other federal agencies and private industry, including the current CIO and several key project management personnel. Officials within both the Department and the FBI are optimistic that the FBI's current IT management team has the talent to solve the FBI's seemingly intractable IT problems. That said, we believe it is essential for the FBI to maintain continuity in its management of Trilogy.

Unrealistic Scheduling of Tasks

Along with the lack of firm milestones in the Trilogy contracts, the scheduled completion dates for individual project components were unrealistic. According to an FBI official monitoring the development of the Trilogy infrastructure, CSC had problems producing an appropriate resource-driven work schedule. Until the FBI became more active in examining the scheduling of the project, the FBI accepted the project's schedules as presented by the contractor. This acceptance began to shift when the FBI's scheduler worked with the contractor to establish a realistic resource-driven work schedule for completing the infrastructure components. At that point, the contractor disagreed with the resulting schedules, because the schedules showed that the full implementation of the project exceeded the proposed completion date of the project. According to the FBI official, the schedule showed a completion date in 2004, not the more optimistic October 2003 date that the contractor desired. When it became apparent that the infrastructure would not be implemented in October 2003, contract renegotiations established a more realistic completion date of April 30, 2004. The infrastructure components were completed in April 2004 in accordance with the revised schedule.

According to the FBI's Project Management Office scheduler, the contractor for the User Applications Component (UAC), SAIC, used a scheduling tool for the development of the VCF with which the FBI was unfamiliar. As a result, the FBI was unable to determine if the assumptions within the schedule were reasonable and whether the implications on the schedule were adequately reflected. Thus, the FBI was unable to validate the contractor's schedule for completing the project.[19]

[19] In commenting on a draft of this report, the FBI agreed that it was unfamiliar with SAIC's scheduling tool but said it was still able to validate and analyze the schedule and use that information in managing the project.

In our view, unrealistic scheduling of project tasks led to a series of raised expectations, followed by frustration when the completion estimates were missed. Additionally, the FBI's lack of familiarity with the contractor's scheduling system for the UAC may have limited the FBI's ability to quickly recognize the extent of schedule slippages and take steps to mitigate them. Standardizing the scheduling process among contractors would facilitate the FBI's ability to recognize potential problems with project milestone dates.

Lack of Adequate Project Integration

Despite the use of two contractors to provide three major project components, the FBI did not hire a professional project integrator to manage contractor interfaces and take responsibility for the overall integrity of the final product until the end of 2003. According to FBI IT managers, FBI officials performed the project integrator function even though they had no experience performing such a role. Although FBI and Department officials stated that the Department required the FBI to perform project integration duties without contractor support, the expertise to adequately perform this function did not exist within the FBI. The problems involved with the scheduling of the project would have been more apparent to the FBI had proper project integration efforts taken place. A professional project integrator could have coordinated the scheduling of the infrastructure with the VCF implementation. Any delays in completing the infrastructure component would have pushed back the full implementation of the VCF, and project costs could rise. Yet the FBI was not fully aware that the infrastructure would not meet its target date until August 2003. Additionally, until December 2003, the FBI was unaware that significant changes to the VCF were needed to achieve the desired performance.

If monitoring the scheduling of the project had been a priority, the FBI could have taken more timely action to effectively address Trilogy's problems. At the end of 2003 — well over two years into the project — the FBI hired a contractor to perform these project integration duties when it became apparent that a professional project integrator was needed to effectively complete the project. According to the *Quarterly Congressional Report* on Trilogy for the period ending April 30, 2004, the FBI has initiated a termination of the integrator's contract due to cost considerations. As of the reporting period, the integrator had received over $2.8 million.

Inadequate Resolution of Issues Raised in Reports

The FBI's management of its IT, including the Trilogy project, was the focus of several reports issued both by components within the FBI and external reviewing entities, including the OIG. These reports are summarized in Appendix 2 of this report. The following discussion of the internal reports covering Trilogy demonstrates that the FBI took inadequate actions to resolve the findings of the reports. Because of the lack of resolution, many of these issues have remained throughout the course of the project.

Within a matter of months after the initiation of the Trilogy project, the FBI recognized significant issues that needed resolution. The internal reports issued by the FBI's Inspection Division, CJIS Division, and consultants identified a lack of a single project manager, undocumented requirements, and a baseline that was not frozen. The CJIS Division's assessment concluded that:

> The predominant area of concern for the Trilogy program appears to be an overall lack of consistency. From baselines to technical direction, from clear lines of authority to a single accountable program manager, the message is clear – without consistency, it is increasingly difficult to apply standard contract analysis tools and methodologies to gain helpful insight into contract status and progresses.

Additionally, the report stated that "until requirements are documented and a baseline is established, it is difficult at best to effectively gauge the many aspects of project management that should be in place on a program of this maturity."

Based on its own reports, the FBI was aware of the risks that faced the Trilogy project. While FBI management eventually hired a project manager to oversee the project — a recommendation made in all of the reports — the process of defining requirements and baselines for the VCF continues, more than two years after these internal reports were issued. Although the Hanssen espionage case and the difficulties experienced in retrieving documents for the Oklahoma City bombing case (events that occurred after these reports were released) resulted in additional security and information-sharing requirements, the difficulties of incorporating the changes would have been greatly

minimized had the FBI established project requirements and baselines in advance.

The FBI's Current and Future IT Needs

As discussed in the Background section of this report, the FBI's IT was severely outdated by the time the Trilogy project was initiated in 2001.

In the current CIO's vision, the counterterrorism mission of the FBI is supported by three functions that must revolve around IT: 1) data collection, 2) data analysis and investigation, and 3) dissemination of information. IT, as the current CIO sees it, is the enabler that will allow agents and analysts to perform these three functions, and Trilogy specifically was intended to provide a solid framework in performing those functions. However, because the VCF is incomplete, that framework has only been enhanced in two ways.

First, the IPC portion of Trilogy has placed more modern equipment on the desk of every agent and analyst, when previously agents and analysts had to share computers that in some cases were 8 to 12 years old. The IPC modernization process allows agents to access FBI systems immediately. Additionally, the new computers include a standardized set of applications for e-mail, word processing, databases, and spreadsheets. As a result, the ability for information sharing among agents, analysts, and other support personnel is enhanced because all employees are working within the same formats and structures.

Second, the connectivity of the Trilogy network provides electronic communications capability and access to investigative and administrative information. While the FBI's previous system did not allow for data to be transferred among agents and analysts, the new system allows for sharing large files, such as photographs. Additionally, the modernized system allows for better encryption of the data transmitted among FBI staff, as well as better storage of the information.

The FBI believes that the system resulting from the FICMS effort will replace the limited and antiquated ACS system. The ACS data management system has not been fully utilized by agents in performing their casework. Consequently, the data contained in the system does not necessarily represent all of the information for a

specific investigative case file. This requires agents to search more than one database in an effort to obtain all the documents relating to a case. Additionally, the functionality and operation of the ACS is not user-friendly and requires the input of several pieces of information to perform basic tasks. The version of the VCF due by December 31, 2004, (the Initial Operational Capability or IOC) is intended to demonstrate that case documents can be approved electronically and uploaded into the ACS. However, this version of the VCF does not provide the case management and information-sharing system envisioned for Trilogy.

In addition to the IOC, the FBI has developed an interim step to make the ACS more user-friendly by making the system accessible through the FBI's intranet. The web-based ACS reduces the number of steps needed to operate the ACS from 12 to 3 and offers other features to make the ACS easier to use. However, the FBI's need for a fully functional case management system to replace the technologically obsolete ACS remains urgent.

Improvements in IT Management

Despite the problems in completing Trilogy, it is important to note that the FBI is making progress to improve its IT management. After appointing a new CIO in May 2004, the FBI reorganized its IT resources in July 2004. The FBI established the Office of the CIO to centrally manage all IT responsibilities, activities, policies, and employees across the FBI. As mentioned earlier, one of the problems cited in the OIG's audit of the FBI's management of IT investments was that all of the FBI divisions that had IT investments were not under a single authority and, as a result, had disparate management processes and procedures. With the FBI's new IT organization, all IT projects now fall under the Office of the CIO. (Appendix 5 shows the organizational chart for the new Office of the CIO.) The CIO has the responsibility for the FBI's overall IT efforts, including developing the FBI's IT strategic plan and operating budget, developing and maintaining the FBI's technology assets, and providing technical direction for the re-engineering of FBI business processes.

The Office of the CIO has also developed an FBI-wide Life Cycle Management Directive to guide FBI personnel on the technical management and engineering practices used to plan, acquire, operate, maintain, and replace IT systems and services. The directive provides detailed guidance to each FBI Program/Project Manager charged with

managing programs or projects throughout the life cycle from inception to deactivation. The processes and procedures, if fully implemented, should help prevent the delays and problems that occurred during the Trilogy project.

The FBI's 2004–2009 Strategic Plan includes the objective to "ensure that all current and future information technology plans work towards a harmonized system." This objective would be met through the creation of an Enterprise Architecture. The FBI is in the process of creating an Enterprise Architecture by September 2005 through its IT Portfolio Management Program.

The FBI's IT Portfolio Management Program is a phased process where the documentation of the FBI's enterprise-wide IT portfolio is established or, in lay terms, a listing that contains all of the FBI's current IT systems will be created, including the technical documentation of those systems. The first phase in creating the listing, completed in February 2004, focused on a pilot performance assessment of Information Resources Division applications. The second phase of the program, the infrastructure portfolio assessment, was initiated in March 2004. Once the data collection for this phase is completed, the next steps include workshops to begin assessing the division's current infrastructure. Completion of the portfolio assessment was targeted for late 2004, and the FBI anticipates that the recommendations from the completed portfolio will be included in the development of the FY 2007 budget.[20]

Federal Intelligence Information Reports Dissemination System

In addition to the VCF IOC, the FBI's CIO pointed to the recent development of the Federal Intelligence Information Reports Dissemination System (FIDS) as an example of how the FBI's reorganized IT management structure can successfully implement a significant project, although FIDS does not represent an application as

[20] In commenting on a draft of this report, the FBI cited the VCF IOC as demonstrating the advances made in its program management processes to achieve cost and schedule baselines. For example, the FBI listed the following improvements: assigning dedicated individuals in key project roles; clearly defining objectives, requirements, and constraints; planning; using control gates at major milestones to release funding and keep the project focused; configuration management; co-locating government and contractor staff; collaborating with other FBI divisions; and providing project oversight at all levels within and also outside the FBI. Because the VCF IOC was incomplete at the time of our audit, the OIG could not evaluate the claims about recent process improvements cited by the FBI.

complex as the VCF or involve case management functions. FIDS is a web-based system for creating the FBI's Intelligence Information Reports (IIR), a primary intelligence product intended for dissemination throughout the U.S. intelligence community. Through FIDS, the drafting of IIRs is automated and standardized, and they can be approved electronically after supervisory review. Because of the computer language used, FIDs is interoperable with other intelligence agencies' systems. Further, a variety of attachments are possible including photographs, video, and audio. The CIO said that the system complies with the information-sharing requirements of Executive Order 13356.

According to the CIO, the FBI developed FIDS in six months for $350,000 by adapting an existing secure system used for Foreign Investigative Surveillance Act requests. The FBI identified, prioritized, and froze the requirements prior to developing the system. The CIO said that FIDs results in a standardized FBI-wide format for IIRs and allows the IIRs to be prepared, approved, and disseminated much more rapidly. This reporting function, however, does not represent the significant systems that will be required for a case management system, and FIDS was only used to demonstrate a recently developed project that includes some of the functionality a case management system would include, such as supervisory reviews and information dissemination.

Conclusion

The FBI has made progress in modernizing its IT infrastructure by installing modern computers and providing a secure network. However, the FBI has not been able to achieve one of the most critical requirements of the Trilogy project, development and deployment of the investigative case management capabilities of the VCF. The FBI does not know how long it will take to achieve this fundamental goal or what this process will ultimately cost. After more than three years of attempted development of the VCF at an estimated cost of $170 million, FBI employees are still using the outdated and inadequate ACS system. While during this process the FBI likely has advanced its understanding of the requirements needed for a future case management system, the $170 million obligated to date on development of the VCF has not fulfilled the FBI's goal of producing a usable case management system.

We found a number of reasons for the FBI's difficulties in completing the Trilogy project successfully and on time. One major reason for the delays and cost growth in the overall project was a lack of specific design requirements for each of the project components. Only with specific requirements in place can the methods, costs, and timeframes for implementation be determined. Because the FBI did not establish at the outset what was needed for the project and establish how those needs should be implemented, the cost of the project ballooned and the implementation schedule slipped. The effect of the lack of specific design requirements was worsened later by necessary modifications.

The Trilogy project, having been initiated prior to September 11, focused on modernizing the FBI's infrastructure to make ACS a user-friendly system. But once the FBI acknowledged that ACS was too archaic a system, the need for the VCF became evident. Such changes could have been more easily managed without severe schedule and cost implications had the technical and performance requirements been established and the project managed more effectively.

The FBI's decision to use a cost-plus-award-fee contract to develop Trilogy placed it at a significant disadvantage because the contract did not establish firm milestones or prescribe penalties for a contractor that missed deadlines or delivered an unacceptable product. According to the FBI, it used this type of contract because it wanted to move forward on the Trilogy project expeditiously. Instead, however, this process resulted in delays and, with respect to the VCF, ultimately did not result in a fully functioning product. In addition to an unsuitable contracting mechanism and the lack of firm design requirements, the FBI also lacked sound IT management processes, continuity of project management and oversight, and project integration and engineering skills. Further, FBI management did not act in a timely manner on a number of critical internal and external reports that demonstrated significant project risks. Had well-established investment management practices been in place earlier, the FBI's IT needs may have been defined better, possibly avoiding the misstep of initially pursuing merely a modification of the ACS system. In addition, a professional project integrator might have recognized more quickly the scheduling setbacks for both the infrastructure and user application components.

FBI management did not exercise adequate control over the Trilogy project and its evolution in the early years of the project. It now appears that with the new organizational structure and authority given to the CIO in July 2004, project management is receiving the attention that was needed throughout the Trilogy project.

Still, the original UAC portion of the Trilogy project remains incomplete despite the FBI's allocation of $170 million for the VCF. Moreover, the cost and schedule for full implementation of the successor to the VCF through the interagency FICMS effort, is unknown because: 1) the FBI has not fully established the requirements for the case management system, and 2) no contract will be in place to develop the framework for this new case management system before the third quarter of FY 2005.

In sum, we believe the FBI's ability to perform its important functions effectively, including counterterrorism, counterintelligence, and criminal law enforcement, will be significantly affected by its ability to implement a modern case management system.

Recommendations

We recommend that the FBI:

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

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

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

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

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

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

7. 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.

8. Apply ITIM processes to all Trilogy-related, or successor, projects.

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

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

This audit assessed the FBI's management of its Trilogy project. In connection with the audit, as required by the 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 Trilogy 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:

- Justice Acquisition Regulations,
- Federal Acquisition Regulations, and
- Government Performance and Results Act of 1993.

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

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the FBI's management of its Trilogy 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 Trilogy project. During our audit, we found the following internal control deficiency.

- The Trilogy project's User Application Component, including the Virtual Case File, remains without final requirements or a contract to complete and fully implement the project.

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 managing its IT investments. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The primary objectives of the audit were to determine: 1) the progress made toward achieving the Trilogy project's schedule, cost, technical, and performance baselines; and 2) the extent to which Trilogy will meet the FBI's overall current and longer-term IT requirements.

Scope and Methodology

The audit was performed in accordance with *Government Auditing Standards*, and included tests and procedures necessary to accomplish the audit objectives. We conducted work at FBI Headquarters and the Department of Justice in Washington, D.C., and at FEDSIM and a contractor's facility in suburban Virginia.

We interviewed officials from the FBI, the Department, and the GAO. The FBI officials interviewed were from the Director's office, Office of the CIO, Information Resources Division, Criminal Justice Information Services Division, Inspection Division, and Finance Division. Additionally, we reviewed documents related to the Trilogy project, budget documentation, organizational structures, congressional testimony, and prior GAO and OIG reports.

To determine whether the FBI is making progress toward achieving the Trilogy project's schedule, cost, performance, and technical baselines, we examined the methodologies the FBI used to complete established baselines. We did this by reviewing completed phases of the project and the processes used. For baselines not fully achieved, we examined the steps being taken by the FBI to achieve the baselines. We did not audit the FBI's statements of project costs.

To determine the extent to which Trilogy will meet the FBI's overall current and longer-term IT requirements, we examined the current status of the Trilogy project, particularly the completion of the infrastructure components and the continuing lack of an effective case management system, as well as the future vision of the FBI's IT end-state as described by the FBI's CIO.

PRIOR REPORTS ON THE FBI'S INFORMTAION TECHNOLOGY

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

OIG Reports on the FBI's IT

OIG reports issued over the past 14 years have highlighted issues concerning the FBI's utilization of IT, including its investigative systems. In 1990, the OIG issued a report entitled, *The FBI's Automatic Data Processing General Controls*. This report described 11 internal control weaknesses and found that:

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

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

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

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

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

A March 2002 OIG report entitled, *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case*,

analyzed the causes for the FBI's belated delivery of many documents in the Oklahoma City bombing case. This report concluded that the ACS system was extraordinarily difficult to use, had significant deficiencies, and was not the vehicle for moving the FBI into the 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. 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 has been slow to correct identified weaknesses and implement corrective action and, as a result, many of these deficiencies repeat 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.

In September 2003, the OIG issued a report entitled *The Federal Bureau of Investigation's Implementation of Information Technology Recommendations* that outlined the FBI's continued need to address the recommendations made by oversight organizations concerning its IT strategies. The report stated that although OIG audits found repeated deficiencies in the FBI's IT control environment and lack of compliance with information security requirements, the current FBI leadership has committed to enhancing controls to ensure that recommendations are implemented in a consistent and timely manner. Additionally, the report noted that the FBI established a system to facilitate the tracking and implementation of OIG recommendations.

External Reports on the FBI's IT and Trilogy

In March 2002, the Commission for the Review of FBI Security Programs issued a report entitled *A Review of FBI Security Programs*. This commission, chaired by former FBI Director William H. Webster, was established to investigate the espionage of former FBI Supervisory Special Agent, Robert Hanssen. The report identified a wide range of IT security issues, including Hanssen's utilization of the ACS system to obtain information for the Soviet Union and to track an FBI counterintelligence investigation. According to Hanssen, "any clerk in the Bureau could come up with the stuff on that system," and he described the lack of security on the ACS system as criminal negligence. The report asserted that many of its findings resulted from the FBI's lack of attention to IT security in developing and managing computer systems.

The National Research Council of the National Academies issued a report in May 2004 entitled *A Review of the FBI's Trilogy Information Technology Modernization Program*. The report was updated in June 2004 to reflect the FBI's response to the report, because significant changes had occurred in many of the areas critically reviewed by the Council. The original report identified significant issues in four major

areas: Enterprise Architecture, system design, project and contract management, and human resources. For each of these areas, recommendations were made to address the likelihood of success in and drive an accelerated pace for the FBI's IT modernization efforts. 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 so inadequate in the past, there was still an enormous gap between the FBI's IT capabilities and the capabilities that are urgently needed.

The update to the report also stated that the Council saw 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. Sustained success in IT, the update noted, "require strong and forceful leadership over an extended period of time." 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. The update also concluded that no one should expect a decrease in expenses for IT when the Trilogy program is completed.

The GAO has issued several reports and related testimony that highlight deficiencies with the FBI's IT. In a review of the Department's Campaign Finance Task Force, the GAO reported in May 2002 that the FBI lacked an adequate information system that could manage and interrelate the evidence that had been gathered in relation to the Task Force's investigations. Also, as part of a government-wide assessment of federal agencies, the GAO reported in February 2002 that the FBI needed to fully establish the management foundation that is necessary to successfully develop, implement, and maintain an Enterprise Architecture.

In September 2003, the GAO issued a report entitled, *Information Technology: FBI Needs an Enterprise Architecture to*

Guide Its Modernization Activities. This report reiterated the GAO's assertion, made in the May 2002 report on the Department's Campaign Finance Task Force, that the FBI did not have an Enterprise Architecture, although it had begun efforts to develop one. Additionally, the GAO found that the FBI still did not have the processes in place to effectively develop, maintain, and implement an Enterprise Architecture.

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 are under way and more are 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 do 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 develops 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.

FBI Internal Assessments on Trilogy

In 2001 and 2002 the FBI performed internal assessments concerning the management of the Trilogy project. The FBI's Inspection Division, Criminal Justice Information Services Division (CJIS), and a contractor performing independent verification and validation (IV&V) work for the FBI completed these assessments. The assessments found that a lack of baselines and oversight posed potential risks for the Trilogy project to meet its budget, schedule, technical, and performance goals. The assessments recommended that the FBI designate a program manager specifically for Trilogy, and that the program manager immediately take steps to establish baselines and requirements for the project.

The assessments addressed areas of potential risk within Trilogy, such as security and configuration management.[21] Based on the recommendations of these reports, the OIG recommended in its December 2002 report on the FBI's IT investment management (ITIM) that Trilogy project managers prepare an action plan to address the risks identified by the three internal reports on Trilogy. Overviews of the three independent assessments (FBI Inspection Division Trilogy Risk Assessment, November 2001; Trilogy Independent Validation and Verification, December 2001; and CJIS Division Trilogy Assessment, January 2002) follow.

Inspection Division Trilogy Risk Assessment

Because of the size and importance of Trilogy to the FBI, the FBI Inspection Division's Major Project Management Oversight Unit (MPMOU) issued a risk assessment report to the Director in November 2001. This assessment identified areas of high risk within the acquisition, financial, requirements, and overall project management of Trilogy. The areas found to be high risk included a lack of project requirements and baselines, the lack of a defined program organizational structure and program manager, and improper scheduling and cost estimates.

The report recommended that the FBI institute a short-term strategy to provide interim capabilities and a long-term strategy to restructure Trilogy. The report also recommended that the short-term strategy should include a detailed plan identifying what can realistically be accomplished within a pre-determined period. It further stated that the short-term plan should have a clearly defined scope so that progress can be measured and quantified.

The MPMOU issued follow-up letters to the Director in December 2001 and February 2002 assessing the FBI's progress in taking action on the recommendations and mitigating Trilogy's risks. In December 2001, the Inspection Division stated that while Trilogy project managers acknowledged certain project risks, the managers were willing to accept aspects of those risks and move forward. However, to address those risks, FBI senior management hired a program manager for Trilogy in March 2002.

[21] Configuration management is the discipline of identifying the configuration of hardware or software systems at each life cycle phase for the purpose of controlling changes to the configuration and maintaining the integrity and traceability of the configuration through the entire life cycle.

In February 2002, the Inspection Division's letter to the Director stated that Trilogy project managers disagreed on the level of project risk for Trilogy. The Inspection Division pointed to the CJIS review and an outside independent validation and verification report on Trilogy, both discussed below, establishing that significant risks to the project exist in the areas originally identified by the Inspection Division. The Inspection Division reiterated its previous recommendation that called for the development of a short-term strategy and a long-term strategy for Trilogy. Inspection Division personnel told us that Trilogy management did not sufficiently develop these recommended strategies.

Trilogy Independent Validation and Verification

The FBI hired an outside contractor to determine the labor requirements, level of effort, and verification and validation tasks necessary to ensure that the Trilogy acquisition would meet the requirements of FBI users into the future within the established schedule and budget. The IV&V report, issued in December 2001, disclosed risks in the program management of Trilogy, the IPC/TNC portion, and the UAC portion, including: 1) a lack of program management structure and focus; 2) a lack of formal requirements, schedules, and baselines; 3) modifications to the UAC/IPC/TNC portions without formal changes to the contracts.

CJIS Division Trilogy Assessment

Upon reviewing the Inspection Division's risk assessment, the Director requested the CJIS Division perform an independent review of Trilogy to get another perspective on the project. The CJIS Division performed its assessment from January 3-16, 2002. This assessment covered management, quality assurance, configuration management, IT security, administrative and technical requirements, and technical management. The assessment found weaknesses similar to those identified by the Inspection Division, including: 1) a lack of clear lines of authority; 2) no clearly designated Program Manager; 3) a lack of authority and support in the areas of quality assurance, security, configuration management, and technical requirements; and 4) insufficient technical reviews of Trilogy documentation.

DOJ REQUEST FOR INFORMATION FOR THE FEDERAL INVESTIGATIVE CASE MANAGEMENT SYSTEM

Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, SEPTEMBER 9, 2004
WWW.USDOJ.GOV

OCIO
(202) 514-2007
TDD (202) 514-1888

DOJ, DHS ANNOUNCE RFI AND INDUSTRY DAY SCHEDULED FOR FEDERAL INVESTIGATIVE CASE MANAGEMENT

WASHINGTON, D.C. - The Department of Justice and the Department of Homeland Security, in conjunction with the Office of Management and Budget, will release a Request for Information (RFI) on September 14, 2004, seeking information for a Federal Investigative Case Management System (FICMS). The FICMS will provide a common solution platform in support of a multi-phased program designed to modernize investigative and intelligence processes within the federal government.

The FICMS will deploy key capabilities including management of paperless case files; case tasking; integrated workflow and management of documents to include their creation, review, collaboration, approval, storage and disposition; evidence management; and records search and reporting. FICMS will implement security measures that include role-based access controls and labeling compliant with Executive Order 13292 on Classified National Security.

To facilitate the information sharing that is vital to our national security imperatives, FICMS will rely on open architecture standards to ensure interoperability with existing and next generation case management systems, especially those that support the litigation (e.g., federal prosecutions) and administrative (e.g., responding to Freedom of Information Act requests) needs of the federal government.

The RFI addresses the objective of this initiative, which is to establish common solutions for case management that promote information sharing throughout the federal government while increasing efficiency and reducing cost. Respondents will be asked to submit literature and/or white papers defining existing commercial and government off-the-shelf solutions that address FICMS capabilities, in part or in whole.

As part of the RFI process, the Departments of Justice and Homeland Security will host an "Industry Day" beginning at 8:30 am on September 28, 2004. A panel representing participating agencies will present an overview of FICMS and respond to questions as appropriate. The event is not open to the public or press. Participants should refer to the FICMS website, http://www.aero.org/related/ficms/index.html, for more information on Industry Day.

###

EXECUTIVE ORDER 13356

The White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
August 27, 2004

Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans

By the authority vested in me as President by the Constitution and laws of the United States of America, and in order to further strengthen the effective conduct of United States intelligence activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

Section 1. Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:

(a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and

(b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).

Sec. 2. Duty of Heads of Agencies Possessing or Acquiring Terrorism Information. To implement the policy set forth in section 1 of this order, the head of each agency that possesses or acquires terrorism information:

(a) shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency in accordance with the standards and information sharing guidance issued pursuant to this order, unless otherwise directed by the President, and consistent with (i) the statutory responsibilities of the agencies providing and receiving the information, (ii) any guidance issued by the Attorney General to fulfill the policy set forth in subsection 1(b) of this order, and (iii) other applicable law, including section 103(c)(7) of the National Security Act of 1947, section 892 of the Homeland Security Act of 2002, Executive Order 12958 of April 17, 1995, as amended, and Executive Order 13311 of July 29, 2003;

(b) shall cooperate in and facilitate production of reports based on terrorism information with contents and formats that permit dissemination that maximizes the utility of the information in protecting the territory, people, and interests of the United States; and

(c) shall facilitate implementation of the plan developed by the Information Systems Council established by section 5 of this order.

Sec. 3. Preparing Terrorism Information for Maximum Distribution within Intelligence Community. To assist in expeditious and effective implementation by agencies within the Intelligence Community of the policy set forth in section 1 of this order, the Director of Central Intelligence shall, in consultation with the Attorney General and the other heads of agencies within the Intelligence Community, set forth not later than 90 days after the date of this order, and thereafter as appropriate, common standards for the sharing of terrorism information by agencies within the Intelligence Community with (i) other agencies within the Intelligence Community, (ii) other agencies having counterterrorism functions, and (iii) through or in coordination with the Department of Homeland Security, appropriate authorities of State and local governments. These common standards shall improve information sharing by such methods as:

(a) requiring, at the outset of the intelligence collection and analysis process, the creation of records and reporting, for both raw and processed information including, for example, metadata and content, in such a manner that sources and methods are protected so that the information can be distributed at lower classification levels, and by creating unclassified versions for distribution whenever possible;

(b) requiring records and reports related to terrorism information to be produced with multiple versions at an unclassified level and at varying levels of classification, for example on an electronic tearline basis, allowing varying degrees of access by other agencies and personnel commensurate with their particular security clearance levels and special access approvals;

(c) requiring terrorism information to be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any other agency to which it has been made available, to the maximum extent permitted by applicable law, Executive Orders, or Presidential guidance;

(d) minimizing the applicability of information compartmentalization systems to terrorism information, to the maximum extent permitted by applicable law, Executive Orders, and Presidential guidance; and

(e) ensuring the establishment of appropriate arrangements providing incentives for, and holding personnel accountable for, increased sharing of terrorism information, consistent with requirements of the Nation's security and with applicable law, Executive Orders, and Presidential guidance.

Sec. 4. Requirements for Collection of Terrorism Information Inside the United States. (a) The Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence shall, not later than 90 days after the date of this order, jointly submit to the President, through the Assistants to the President for National Security Affairs and Homeland Security, their recommendation on the establishment of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information to be collected within the United States, including, but not limited to, from publicly available sources, including nongovernmental databases.

(b) The recommendation submitted under subsection (a) of this section shall also:

(i) address requirements and guidelines for the collection and sharing of other information necessary to protect the territory, people, and interests of the United States; and

(ii) propose arrangements for ensuring that officers of the United States with responsibilities for protecting the territory, people, and interests of the United States are provided with clear, understandable, consistent, effective, and lawful procedures and guidelines for the collection, handling, distribution, and retention of information.

Sec. 5. Establishment of Information Systems Council. (a) There is established an Information Systems Council (Council), chaired by a designee of the Director of the Office of Management and Budget, and composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of Central Intelligence; the Director of the Federal Bureau of Investigation; the Director of the National Counterterrorism Center, once that position is created and filled (and until that time the Director of the Terrorism Threat Integration Center); and such other heads of departments or agencies as the Director of the Office of Management and Budget may designate.

(b) The mission of the Council is to plan for and oversee the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in section 1 of this order.

(c) Not later than 120 days after the date of this order, the Council shall report to the President through the Assistants to the President for National Security Affairs and Homeland Security, on a plan, with proposed milestones, timetables for achieving those milestones, and identification of resources, for the establishment of the proposed interoperable terrorism information sharing environment. The plan shall, at a minimum:

(i) describe and define the parameters of the proposed interoperable terrorism information sharing environment, including functions, capabilities, and resources;

(ii) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by agencies to share terrorism information, and recommend as appropriate the redirection of existing resources to support the interoperable terrorism information sharing environment;

(iii) identify gaps, if any, between existing technologies, programs, and systems used by agencies to share terrorism information and the parameters of the proposed interoperable terrorism information sharing environment;

(iv) recommend near-term solutions to address any such gaps until the interoperable terrorism information sharing environment can be established;

(v) recommend a plan for implementation of the interoperable terrorism information sharing environment, including roles and responsibilities, measures of success, and deadlines for the development and implementation of functions and capabilities from the initial stage to full operational capability;

(vi) recommend how the proposed interoperable terrorism information sharing environment can be extended to allow interchange of terrorism information between agencies and appropriate authorities of States and local governments; and

(vii) recommend whether and how the interoperable terrorism information sharing environment should be expanded, or designed so as to allow future expansion, for purposes of encompassing other categories of intelligence and information.

Sec. 6. Definitions. As used in this order:

(a) the term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office;

(b) the terms "Intelligence Community" and "agency within the Intelligence Community" have the meanings set forth for those terms in section 3.4(f) of Executive Order 12333 of December 4, 1981, as amended;

(c) the terms "local government," "State," and, when used in a geographical sense, "United States," have the meanings set forth for those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101); and

(d) the term "terrorism information" means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other United States Government activities, relating to (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) information relating to groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Sec. 7. General Provisions. (a) This order:

(i) shall be implemented in a manner consistent with applicable law, including Federal law protecting the information privacy and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the authority of the principal officers of agencies as heads of their respective agencies, including under section 199 of the Revised

Statutes (22 U.S.C. 2651), section 201 of the Department of Energy Reorganization Act (42 U.S.C. 7131), section 102(a) of the National Security Act of 1947 (50 U.S.C. 403(a)), section 102(a) of the Homeland

Security Act of 2002 (6 U.S.C. 112(a)), and sections 301 of title 5, 113(b) and 162(b) of title 10, 1501 of title 15, 503 of title 28, and 301(b) of title 31, United States Code; and (iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals.

(b) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

GEORGE W. BUSH

THE WHITE HOUSE,

August 27, 2004.

Chief Information Office
Organizational Structure
As of June 1, 2004

GLOSSARY OF ACRONYMS

ACS	Automated Case Support
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
CLEA	Criminal Law Enforcement Application
CSC	Computer Sciences Corporation
FBI	Federal Bureau of Investigation
FEDSIM	Federal Systems Integration and Management Center
FICMS	Federal Investigative Case Management System
FIDS	Federal Intelligence Information Reports Dissemination System
FITUP	Federal Bureau of Investigation's Information Technology Upgrade Plan
FOC	Full Operational Capability
GAO	Government Accountability Office
GSA	General Services Administration
IDW	Information Data Warehouse
IIIA	Integrated Intelligence Information Application
IIR	Intelligence Information Report
IPC	Information Presentation Component
IOC	Initial Operational Capability
ISI	Information Sharing Initiative
IT	Information Technology
ITIM	Information Technology Investment Management
IV&V	Independent Verification and Validation
JAD	Joint Application Development
MPMOU	Major Project Management Oversight Unit
OIG	Office of the Inspector General
RIA	Reports on Investigative Activity
RFI	Request for Information
RFP	Request for Proposals
SAIC	Science Applications International Corporation
TA	Telephone Application
TNC	Transportation Network Component
UAC	User Application Component
VCF	Virtual Case File
WAN	Wide Area Network

THE FBI'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

January 26, 2005

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

Re: DRAFT AUDIT REPORT - THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF THE TRILOGY INFORMATION TECHNOLOGY MODERNIZATION PROJECT

Dear Mr. Fine:

The Federal Bureau of Investigation (FBI) appreciates your efforts, and those of your staff, in assessing the progress of our Trilogy technology modernization project. As always, the FBI welcomes your observations and final recommendations. We will give them thorough review and consideration.

We have completed our review of your draft report entitled, "The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project" and appreciate this opportunity to respond to your preliminary findings and recommendations. Based upon our review, your findings and recommendations are consistent with the FBI's internal reviews and with those of other oversight entities. I am pleased to inform you that the FBI has made significant progress in addressing not only all the recommendations, but all the key issues raised in your draft report.

Before responding to the individual recommendations, however, there are several issues that call for clarification. These relate to the national security impact of the delay of the Virtual Case File (VCF), the future of the VCF, and changes in the FBI's management of information technology (IT). A more detailed "fact check" that pointed out specific inaccuracies was submitted under separate cover on January 19, 2005.

The Honorable Glenn A. Fine

Issue 1: National security remains uncompromised by the delay of VCF

We agree that we have not met our goals for an automated case management system. However, we disagree with your finding that "the continuing lack of an effective case management system hinders the FBI's capability to perform its critical national security mission." The draft report states that delays in the VCF program raise national security implications because the FBI is continuing to rely on the Automated Case Support (ACS) system and paper files, which hamper FBI Agents and Analysts from adequately searching and sharing information from investigative files. These statements overlook the substantial IT improvements that directly support our counterterrorism mission.

While VCF would improve efficiency, workflow, and records management, it is important to stress that VCF is a software application, not a counterterrorism database or hardware set. All FBI Special Agents and Intelligence Analysts have access to the necessary FBI databases. The legacy case management system, ACS, has limitations, but it is a widely used tool that heavily supports case, lead, and collected-item management, reporting, and indexing services. ACS is searchable and data entered into it can be updated. More importantly, ACS is far from the only means by which the FBI searches, analyzes, and shares data.

Substantial IT improvements have been made, such as upgrading our secure network to a high-speed reliable network. Hardware and robust search tools have greatly enhanced our ability to access, analyze, and share information. As pointed out in the draft report, the new Trilogy network and hardware provides a uniform suite of software that has given FBI personnel the ability to share information, including images, audio, video, and multimedia files, quickly, reliably, and securely. The Trilogy upgrades have also provided a foundation for a number of new capabilities that support the FBI's counterterrorism mission.

The FBI's Investigative Data Warehouse (IDW) now provides Special Agents, Intelligence Analysts, and members of Joint Terrorism Task Forces (JTTFs), with a single access point to more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds, that were previously available only through separate, stove-piped systems.

New analytical tools are used across multiple data sources providing a more complete view of the information possessed by the Bureau. Users can search up to 100 million

pages of international terrorism-related documents and billions of structured records such as addresses and phone numbers in seconds. They can also search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. Coupled with sophisticated state-of-the-art search tools, the IDW enhances the FBI's ability to identify relationships across cases quickly and easily.

Other critical IT improvements have given the FBI unprecedented connectivity with our partners in the Intelligence and Law Enforcement Communities. The Top Secret/Sensitive Compartmented Information Operational Network (SCION) gives FBI personnel the ability to electronically receive, disseminate, and share compartmented sources of intelligence information among the FBI's counterterrorism and counterintelligence operations and with the Intelligence Community. SCION also provides for video teleconferencing at the TOP SECRET level.

The FBI has further enhanced its SECRET level connectivity to the Intelligence and Homeland Security Communities via the Department of Defense's (DOD) SECRET Internet Protocol Router Network (SIPRNET). At the start of 2004, the FBI had a SIPRNET presence of 50 stand-alone workstations. In December 2004, the FBI implemented a new strategy which currently provides FBI users with access to SIPRNET from their Trilogy desktop.

The FBI uses SIPRNET to disseminate both raw and finished intelligence and to support more than 100 JTTFs, the Foreign Terrorist Tracking Task Force (FTTTF), the National Virtual Translation Center (NVTC), the Terrorism Screening Center (TSC), and the Terrorist Explosive Devices Analytical Center (TEDAC).

The Secure Video Teleconferencing Network (SVTCN) provides SECRET level, state-of-the-art video teleconferencing capability between FBI Headquarters, remote field offices, JTTFs, and other secure locations. The SVTCN operates over the FBI's new Trilogy network and can relay live video and information from a crisis center to senior FBI management located at any FBI site. The SVTCN also supports distance learning activities.

We have also enhanced connectivity through the FBI's Automated Messaging System (FAMS). FAMS began 24/7 operations on December 15, 2004, and now provides users with the capability to send and receive critical organizational message traffic to any

of the 40,000+ addresses on the Defense Messaging System (DMS). FAMS will replace the legacy SAMNET system and support all FBI users by April 30, 2005. The Top Secret version of FAMS is currently under test and will provide the same capability to everyone on SCION by May 30, 2005. The FBI is the first civilian agency to operate on the classified DMS.

Another innovation is the FBI Intelligence Information Reports Dissemination System (FIDS), deployed throughout the FBI on November 15, 2004. FIDS is a web-based software application that allows all FBI personnel with access to the FBI's Intranet to create and disseminate standardized Intelligence Information Reports (IIRs) quickly and efficiently. FIDS is significant because it is the first Extensible Markup Language (XML)- based IIR system in the federal government with a message format output standardized to Intelligence Community standards. It facilitates interoperability with other Intelligence Community databases and dissemination systems using XML. It also automates the IIR re-engineered process with a re-engineered electronic workflow allowing for improved information management.

The FBI is also beginning to implement programs for data marts as part of the Intelligence Community System for Information Sharing (ICSIS). The first FBI Secret/Top Secret Intelligence Community data mart is currently being developed and will be online by January 30, 2005.

To facilitate information sharing with state, municipal, and tribal law enforcement and first responders, the FBI continues to expand its use of Law Enforcement Online (LEO). LEO is used to support the sharing of vital information between the National JTTF, the Department of Justice (DOJ), the TSC, and local JTTFs across the country. The National JTTF and each of the JTTFs have established Special Interest Groups on LEO, accessible to all law enforcement personnel, to facilitate the exchange of terrorism information nationally and locally.

We have interfaced LEO with two other law enforcement networks: (1) the National Law Enforcement Telecommunications System (NLETS), an information sharing network that connects state, municipal, and federal law enforcement and justice agencies; and (2) the Regional Information Sharing Systems Network (RISS), that provides law enforcement users in six regional centers with database pointer systems, investigative leads bulletin boards, and encrypted e-mail. These networks are specifically designed to facilitate sharing of intelligence to coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Interconnectivity among

the combined users of LEO, NLETS, and RISS gives us the means to share information about groups posing the greatest threats to the United States with more law enforcement partners, quickly, and with greater ease.

LEO also supports the National Alert System (NAS), which uses push-technology to notify up to 21,000 users/agencies of critical alert information within minutes. Messages pop up on computers - like instant messaging, but in a secure environment - and alert notifications are sent to police chiefs' cell phones and pagers. The system can deliver the message selectively to specific groups (as dictated by geography or function, such as border states or airport security) or broadcast to all possible recipients. Messages can include text, photos, and maps.

The Criminal Justice Information Services (CJIS) Information Sharing project will use LEO's sensitive but unclassified (SBU) infrastructure to share information between CJIS Division systems, including the National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS), and federal, state, municipal and tribal law enforcement.

In addition, we are well on our way toward implementing the Law Enforcement National Data Exchange (N-DEx). The N-DEx will provide federal, state, municipal and tribal law enforcement with a system to collect, process, and disseminate criminal and investigative data. This national information sharing program will provide the Law Enforcement Community with:

- Information about methods of criminal operation identified by national contributors;
- arrestee/indictor information;
- victim information;
- suspect information; and
- other ongoing criminal and investigative information.

N-DEx will provide a national law enforcement "pointer" to more detailed indices, case, and intelligence information. It will provide for automated direct electronic input from local, tribal, state, and federal agencies, as well as interactive responses.

On June 15, 2004, the FBI's Security Division granted interim approval to operate the N-DEx system. A number of law enforcement agencies have signed MOUs with the FBI regarding

prototyping, including: (1) Marietta, Georgia, Police Department; (2) Alexandria, Virginia, Police Department; (3) the Uniform Crime Reporting (UCR) State Repository, West Virginia State Police, Huntington, West Virginia; and (4) Cabell County, West Virginia, Sheriff's Office. Upon final FBI Office of the General Counsel approval of the Privacy Impact Statement and the signing of the new piloting memorandum of understanding, the prototyping phase will transition to the piloting phase.

N-DEx is fully integrated with the Global Justice XML initiative for improving interoperability of all criminal justice information systems under one standard. N-DEx is also fully integrated with the DOJ Law Enforcement Information Sharing Program (LEISP) plan.

In short, the FBI's capacity to access, analyze, and share data internally and externally has improved considerably since the OIG began this audit, strengthening our ability to predict and prevent acts of terrorism and otherwise supporting our national security mission. Additional improvements currently underway will further strengthen these capabilities over the next few months.

Issue 2: The FBI has a plan to leverage what has been developed on the VCF project and move forward with a long-term solution

The draft report states that "the FBI is moving away from VCF as the solution of its case management requirements. Instead, the FBI is relying on the future (and uncertain) development of an interagency FICMS for its case management needs." This statement requires clarification.

First, it implies that the VCF project is being abandoned and replaced by the Federal Investigative Case Management System (FICMS). In fact, VCF and FICMS are two separate, but related projects that will move forward simultaneously. The VCF project remains the highest IT priority for the FBI, and we are developing an implementation plan that will result in deployment of a fully functional investigative case and records management system.

We have tasked Aerospace Corporation, a non-for-profit federally funded contractor, to evaluate the SAIC-delivered VCF application. Under a separate option, we tasked Aerospace with evaluating commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products that may meet the defined FBI's requirements. Aerospace has delivered two reports to the FBI, a *Commercial Off the Shelf /Government Off the Shelf (COTS/GOTS) Technology Trade Study* and an *Independent Verification and Validation of the Trilogy*

Virtual Case File Report. These reports will serve as vital sources of information for the FBI's future VCF.

Second, the finding represents a fundamental misunderstanding of the FICMS project. To clarify, FICMS does not replace VCF. FICMS serves as the framework that will govern development of DOJ and Department of Homeland Security (DHS) investigative case management systems to ensure the high level of inter-agency compatibility needed to facilitate information sharing. Each agency has unique needs and will implement its own services to manage investigative workflow, manage records, and analyze data. However, these individual systems will follow the broad FICMS blueprint so that data can flow easily and securely between agencies.

The two projects are on parallel tracks that will eventually converge. The FBI is moving forward in the development and deployment of a case management system. The success from the FBI project will be used to develop the FICMS, a broad blueprint for federal investigative case management systems.

The FBI has learned critical lessons in various areas, including: contract management, project management, adequate policies and procedures, modular development and deployment, discretionary access controls for security of data, record management requirements, and the value of prototyping. These lessons learned will be applied to future case management systems and to all future IT projects.

Issue 3: The FBI's Management of IT

The draft report states that contracting weaknesses were a primary cause of schedule and cost problems associated with Trilogy. We agree with the finding that the FBI's oversight of the Trilogy contracts should have been stronger. However, it is important to note that at the start of the Trilogy project, the FBI recognized its limitations and appropriately outsourced elements of the project in accordance with the general framework for handling these contracts that was dictated by DOJ. As the draft report states, DOJ initially required that the FBI perform the project integration function and that Trilogy be divided among two contractors.

The General Services Administration's Federal Technologies Services' Federal Systems Integration and Management (FEDSIM) Center acted as the contracting office on behalf of the FBI for the key Trilogy contracts. Accordingly, FEDSIM was responsible for overseeing competing contracts, awarding and

maintaining contracts, tracking contract health, and day-to-day management. Mitretek Systems was the Program Management and Systems Engineering and Technical Advisory Services (SETA) contractor that supported the Trilogy Program. Computer Sciences Corporation (formerly DynCorp) was the contractor responsible for the network and hardware components of the Trilogy Program. SAIC was responsible for delivering the user applications component, including the VCF. SAIC also later assumed the role of Integrator for the Trilogy Program.

With regard to the overall management of IT, we are pleased to report that we have made fundamental changes in the method by which IT is managed in the FBI - changes that will ensure that we move forward in a manner that supports our mission, priorities, and Strategic Plan, and that is consistent with industry best practices and established principles of IT management.

As part of a top-to-bottom reorganization of the FBI's IT resources, the FBI established the Office of the Chief Information Officer (OCIO) to centrally manage all IT responsibilities, activities, policies, and employees across the Bureau. With the FBI's new IT organization, all IT projects now fall under the OCIO. The OCIO is responsible for the FBI's overall IT efforts, including developing the FBI's IT strategic plan and operating budget, developing and maintaining the FBI's technology assets, and providing technical direction for the re-engineering of FBI business processes.

The OCIO is divided into four components: policy and planning, project management, technology development, and operation and maintenance. This structure provides for end-to-end management of IT projects within the FBI and incorporates best practices for governing a large IT organization.

Under the centralized leadership of the OCIO, the FBI is taking a coordinated, strategic approach to IT. OCIO has established an IT governance framework for managing IT projects at each stage of their "lifecycle" from planning and investment, through development and deployment, operation and maintenance, and disposal. The OCIO has also implemented a comprehensive set of safeguards to ensure that future IT programs do not run into problems like those encountered on the VCF project.

In December 2004, the OCIO completed our first release of the Strategic IT Plan (SITP), which maps out how IT will support the FBI's Strategic Plan and mission goals over the next five years. All IT projects are now required to be consistent with the FBI's Strategic Plan.

We established our baseline Enterprise Architecture (EA) in 2004 and are in the process of developing our target EA in September 2005. We have already identified all of the IT systems, applications, networks and databases in the Bureau in an IT Master Systems List. All IT projects in the future will be required to be consistent with the FBI's EA.

We have implemented a Life Cycle Management Directive (LCMD) that fundamentally changes how IT projects are managed in the Bureau. Our LCMD governs how IT projects are managed from "cradle to grave" and is consistent with industry and other government agency best practices. The LCMD guides FBI personnel on the technical management and engineering practices used to plan, acquire, operate, maintain, and replace IT systems and services. All IT projects and programs will be required to undergo rigorous project and executive level "control gate" reviews for each stage, from inception through disposal. There are seven gates, nine phases, and 14 key supporting processes in the LCMD. These reviews are the mechanism for management control and direction, decision-making, coordination, and confirmation of successful performance. The LCMD will help prevent the delays and problems that occurred during the Trilogy project.

We have established five Enterprise IT Governance Review Boards: (1) the Investment Management/Project Review Board; (2) the Technical Review Board; (3) the Change Management Board; (4) the IT Policy Review Board; and (5) the Enterprise Architecture Board. These Boards decide whether to proceed with, revise, or terminate a program or project. An Executive Assistant Director-Level IT Advisory Board now meets quarterly to discuss IT matters with key stakeholders. We have established charters and procedures, and all Boards are operational.

The Investment Management/Project Review Board now reviews and approves new IT investments at specified stages of each IT project's life cycle. We are also in the process of evaluating the FBI's 130+ existing IT projects for overall health and placement within the system development life cycle. This will enable FBI executives to uncover and address cost, schedule, and performance risks.

The FBI has implemented a comprehensive and effective IT Portfolio Management Program. The program focuses on performance assessments of IT investments in the operations and maintenance (O&M) phase of their life cycle. Since the majority of our IT investments currently reside in the O&M phase, these assessments help senior management make more informed decisions about IT investments (personnel and dollars). Portfolio

Management recommendations are focused on those investments that should be leveraged, replaced, outsourced, or retired. A pilot portfolio assessment of one Division has been completed to date, and the enterprise portfolio assessment will be completed in the fall of this year, in time to support the FY 2008 budget/investment cycle.

The FBI has established an IT Portfolio Management Automation project that will develop the FBI's Enterprise IT Tool. This is a software package that will identify and track sanctioned IT projects with baselined plans, schedules, scope, and costs. It will also track all FBI IT hardware and software infrastructure procurements at an integrated, enterprise level. The Enterprise IT Tool will electronically track all IT projects throughout the lifecycle and help us to ensure that new IT investments are aligned with mission goals.

We are also taking steps to ensure a high level of performance for our IT projects. The OCIO is in the process of establishing an IT Metrics program that identifies and measures IT performance according to industry standards, government regulations, and earned value management system (EVMS) principles. Currently, we publish a CIO Monthly IT metrics report using the Balanced Scorecard Methodology. Our plan is to establish EVMS for "major" IT projects, which are being reviewed by the Investment Management/Project Review Board at the rate of approximately five projects per month, beginning in January 2005. When a program or project metric varies by more than 10 percent of the acceptable thresholds for cost, schedule and performance, it will trigger closer scrutiny and remedial action by the Investment Management/Project Review Board.

We have launched a joint initiative between the CIO and the Chief Financial Officer of the FBI that will standardize and automate all procurement actions involving all IT acquisitions, as well as focus on increased competition and small business involvement.

To build a stronger IT workforce, including managers, the OCIO has begun to train our Program and Project Managers, as well as executive management personnel, to be certified as Program Management Professionals (PMP). The OCIO currently has two certified government and five contractor PMPs. Approximately 25 managers have taken the PMP review course and plan to take the test. Another 20 are currently enrolled in the training program. This and other leadership training provides best practices and techniques to provide better management of the IT projects and the enterprise IT portfolio.

To coordinate IT policies, the OCIO is in the process of establishing a Master IT Policy List. Once established, any new IT policies or modifications will have to be reviewed and approved by the IT Policy Review Board. The Master IT Policy List will enable the OCIO to monitor all IT projects during the LCMD control gate review processes and enforce all applicable IT policies.

We are also taking steps to standardize technology assessments. The FBI CTO is working closely with the EA team to standardize enterprise technology standards, technical reference models, technical architectures, and technical design reviews under the LCMD and system testing/integration. A unified test and integration facility will allow for centralized technology assessment that provides responsive IT solutions to meet mission needs. These measures mitigate project risks through common, interoperable, supportable, and affordable solutions.

In the area of security, the FBI has implemented an Information Assurance Program, which also contributes to the LCMD. It is implementing key IT capabilities, such as Public Key Infrastructure (PKI) and the Enterprise Security Operations Center (ESOC), which will strengthen IT services in the Bureau and mitigate internal and external threats. Additionally, Security and Information Assurance is being fully integrated into the new LCMD and the EA, throughout the process, instead of being "bolted-on" afterwards. Certification and Accreditation is being required for all IT Projects and Systems.

The VCF Initial Operating Capability (IOC) was fully executed using the FBI's new approach to IT management. Project objectives, requirements, and constraints were clearly identified before proceeding forward to each control gate. A cost-sharing arrangement was established as part of the renegotiated UAC contract. A well developed plan was established and agreed to as part of the contract negotiations. Control gates (i.e., go/no go criteria) were used at major milestones to control the release of funding and to keep the project focused. Adherence to defined management processes was mandated. As a result, the VCF IOC was developed on schedule and within budget and its deployment is currently on schedule.

Development of the FIDS is another example of how the FBI's new approach to IT management is supporting our national security mission. The FIDS was designed to meet exigent intelligence mission needs and was successfully developed using a proven business process and information management framework. It was created by a five-member development team and conformed to

the FBI CIO's new Life Cycle Management Process. Its successful six-month development cycle is an example of focused systems development in record time at reasonable cost.

As demonstrated by VCF IOC, PKI, and FIDS, proper planning and contractor oversight will ensure success on future IT projects.

Response to Recommendations

Recommendation 1: Replace the obsolete ACS system as quickly and as cost-effectively as feasible.

The FBI agrees with the recommendation to replace the ACS system as quickly and as cost-effectively as feasible, and doing so remains our top IT priority.

We are continuing to move forward with the VCF project in accordance with a two-track plan initiated in June 2004. Track One, also known as IOC, will pilot the operational use of VCF's automated workflow process. Several hundred employees in the New Orleans Field Office, Baton Rouge RA, and the Drug Unit within the America's Criminal Enterprise Section at FBIHQ will use the system as their document routing system from mid-January through the end of March 2005. Objectives of the pilot are to: (1) test drive the workflow concept; (2) validate the human machine interface; (3) create an electronic interface to ACS; (4) assess network performance; and (5) develop and deliver an enterprise-geared training curriculum. The IOC is on track to accomplish all these objectives.

As part of Track Two, the FBI contracted with multiple independent vendors to perform the following tasks:

1. Examine the latest working version of the VCF application to determine if the software, as designed, will meet the FBI's operational, security, and performance requirements. The contractor is also tasked to determine if the VCF application is scalable and can be maintained and enhanced easily.

2. Examine the current technologies and vendors, as well as available off-the-shelf software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. In many ways, the pace of technological innovation has overtaken our original vision for VCF, and there are now products to suit our purposes that did not exist when Trilogy began.

3. We have also asked a different contractor to review and revalidate our users' requirements because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing among different entities.

As mentioned above, we are currently reviewing the Aerospace report, and the other reports are expected by the end of January 2005. These independent reviews will provide the FBI with valuable information to help managers make future decisions related to FBI applications.

Recommendation 2: Reprogram FBI resources to meet the critical need for a functional case management system.

The FBI agrees with this recommendation. As mentioned above, deployment of a new case management system is the FBI's top IT priority. Accordingly, we will devote all necessary resources to support the project, even if this requires reprogramming. In 2004, resources were reprogrammed to support reorganization of the OCIO and related human capital development initiatives. As discussed above, these efforts will help ensure that all IT projects, including the VCF, are well managed in accordance with established best practices for IT management.

Recommendation 3: 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.

The FBI agrees with this recommendation and has already taken steps to address it. This recommendation is consistent with the FBI's new approach to IT management and, accordingly, all future IT contracts will follow this approach. At the heart of our new IT management initiatives, including the IT Strategic Plan and the LCMD, is the understanding that we must have a clear picture of what we intend to achieve before making substantial investments. This principle is being applied to VCF Track Two to include the revalidation of our users' requirements.

The implementation of the LCMD and Review Boards will mitigate the project scope and requirements creep. The LCMD requires the requirements to be clearly defined before system development starts. The Review Boards will ensure that the LCMD is enforced.

Similarly, FICMS will move forward with clear System Requirement Specifications and will use a proven contract vehicle to help ensure that they are met.

Recommendation 4: Incorporate development efforts for the VCF into the development of the requirements for any successor case management system.

The FBI agrees with this recommendation and has already taken steps to address it. Lessons learned over the course of the VCF project can and will be incorporated into development of any future case management system.

For example, the VCF project suffered in part from runaway scope. After evaluating the lessons learned from the VCF development, we have adopted a process that will avoid a recurrence. The FBI has created a complete set of requirements for developing future case management applications. To ensure that future IT systems do not expand beyond their functional level, the IT system will be designed, developed, and deployed incrementally against specified and planned parameters.

Recommendation 5: Validate and improve, as necessary, financial systems for tracking project costs to ensure complete and accurate data.

The FBI agrees with this recommendation and has already taken remedial steps. Following the FBI's submission of the LCMD, this recommendation was closed by the OIG on December 17, 2004 in the report entitled "FBI's Management of IT Investments, Audit Report Number 03-09."

Recommendation 6: 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.

The FBI agrees with this recommendation and has taken appropriate action. Following the FBI's submission of the LCMD, this recommendation was closed by the OIG on December 17, 2004 in the report entitled "FBI's Management of IT Investments, Audit Report Number 03-09."

Recommendation 7: 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.

The FBI agrees with this recommendation and has taken appropriate action. As previously outlined, the FBI has implemented a comprehensive approach to management of IT under which all IT projects are evaluated for overall health, cost, contribution to the FBI mission, and performance at each stage of their lifecycle.

Recommendation 8: Apply ITIM processes to all Trilogy and any successor projects.

The FBI agrees and will apply ITIM processes to future IT projects, including any additional Trilogy-related projects. This recommendation was resolved by the OIG in the report entitled, "FBI's Management of IT Investments, Audit Report Number 03-09." In that report, the OIG concurred with the FBI's Plan of Action and Milestones, and the FBI continues to provide status updates on a quarterly basis in accordance with that report.

In the March 24, 2004, OIG report entitled "FBI's Implementation of IT Recommendations, Audit Report Number 03-36," the OIG agreed that efficiencies can be achieved by both the OIG and the FBI by tracking a duplicate recommendation only under a single audit -- the audit in which the recommendation originated. Accordingly, we recommend that the FBI continue to report on progress in this area under Audit Report Number 03-09.

Recommendation 9: Monitor the Enterprise Architecture being developed to ensure timely completion as scheduled.

The FBI agrees with this recommendation and has already taken steps to address it. As discussed above, the FBI has made considerable progress toward development of an EA.

This recommendation was closed by the OIG on September 12, 2003, in the report entitled, "FBI's Management of IT Investments, Audit Report Number 03-09." It was also resolved in the Government Accountability Office (GAO) report entitled, "Information Technology - FBI Needs an Enterprise Architecture to Guide Its Modernization Activities, GAO-03-959." Also, in September 2004, the GAO initiated a follow-up review of the FBI's Enterprise Architecture Efforts (Job Code 310291) and a report is pending. Accordingly, we recommend that this recommendation be closed to avoid unnecessary duplication of GAO's efforts.

Conclusion

Although deployment of a new case management system for the FBI has been delayed, the overall pace of IT modernization in the FBI continues to accelerate. We have made substantial IT improvements to enhance our ability to access, analyze, and share information. We did so in a manner that has not hampered critical ongoing operations and that ensures the security of our information and the privacy rights of individuals. Today, armed with a solid IT foundation, a new organization and framework for

IT management, and with the lessons learned over the course of the Trilogy project, the FBI is moving forward with further IT enhancements to help us perform our mission.

We appreciate the OIG's guidance throughout this process. We look forward to working with your office in implementing recommendations that remain unaddressed.

Sincerely,

Zalmai Azmi
Chief Information Officer
Federal Bureau of Investigation

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

Pursuant to the OIG's standard audit process, the OIG provided a draft of this audit report to the FBI on December 20, 2004, for its review and comment. The FBI's January 26, 2005, response is included as Appendix 7 of this final report. The FBI concurred with the nine recommendations in the audit report and also provided comments regarding three general issues in the report. Our analysis of the FBI's response to these three issues and to the nine recommendations is provided below.

FBI's General Comments

1. In its response, the FBI disagreed with the OIG's assertion that "the continuing lack of an effective case management system hinders the FBI's capability to perform its critical national security mission." According to the FBI, such statements "overlook the substantial IT improvements that directly support our counterterrorism mission."

In our report, we note that there are national security implications when the FBI must continue to rely on an archaic case management system, ACS, which hampers analysts and agents from adequately searching and sharing investigative information. We believe the ability to timely receive, link, analyze, and share investigative leads and case information is essential to help prevent future terrorist attacks. As documented in prior OIG reports, the ACS is an inefficient and burdensome tool that does not contain all of the investigative lead and case information available within the FBI. We found that many FBI employees do not fully use ACS because of its deficiencies. Further, as stated in the final report of the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission): "Finally, the FBI's information systems were woefully inadequate. The FBI lacked the ability to know what it knew: there was no effective mechanism for capturing or sharing its institutional knowledge."

In responding to the audit, the FBI points to improved capabilities resulting from the Trilogy infrastructure as well as the availability of various other FBI systems, databases, and analytical tools to facilitate intelligence analysis and sharing. We do not dispute the FBI's progress in these areas, although we did not examine these other systems because they were not the subject of our audit. We did

analyze the FBI's progress in implementing the VCF case management application, which was intended to replace ACS and serve as the FBI's sole case management system. The VCF was intended to contain all investigative lead and case file information in a paperless system. Due to the FBI's failure to develop a workable and complete VCF after spending more than 3 years and $170 million, the FBI continues to lack a modern case management system containing complete and accessible investigative lead and case information.

In responding to several prior OIG reports that identified substantial deficiencies in the ACS system, the FBI stated that the deficiencies found within the ACS system would be corrected through implementation of the VCF.[22] However, the VCF still remains under development without a clear timetable of when it will be implemented and at what cost. The FBI's response recognizes the urgent need to replace ACS, stating that doing so remains the FBI's top IT priority.

As pointed out in the prior OIG reports and as noted in this report, ACS is based on obsolete technology and has been extraordinarily difficult to use. Furthermore, because agents did not always use the ACS, the system does not contain complete investigative case data and records. Also, due to its obsolete technology, the ACS is not readily or timely used to acquire and link information across the FBI. Although the FBI recently has reduced the number of steps needed to use the ACS from 12 to 3, the system remains archaic. According to a 9/11 Commission Staff Statement on information sharing within the FBI:

> Although there are many explanations for the failure to share information internally, one of the most common in the FBI's outdated information technology, the Automated Case Support system in particular. It employs 1980s-era technology that is by all accounts user-unfriendly. More troubling, the system cannot be used to store or transmit top secret or sensitive compartmented information. For a variety of reasons, significant information that gets collected by the FBI never gets uploaded into the

[22] Problems with the ACS were discussed in the following OIG reports: *The Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation* (July, 1999); *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case* (March 2002); and *The FBI's Management of Information Technology Investments* (December 2002).

Automated Case Support system, or it gets uploaded long after it is learned.

In its response, however, the FBI cites other IT initiatives to support its assertion that national security remains uncompromised by the delay in deploying the VCF. For example, the FBI's response states that the newly created Investigative Data Warehouse allows FBI employees greater access to a variety of counterterrorism information. Although we did not include the Investigative Data Warehouse in our audit and have not evaluated its capabilities, we believe that the VCF case management system would have many features that a data warehouse does not. The VCF was intended to be the backbone of the FBI's information systems, replacing the FBI's paper case files with electronic files. Case data in the VCF could be approved electronically, and the electronic files would be available throughout the FBI immediately as entered, and various lead and case information could be associated for analysis. The VCF not only would allow dissemination of this information immediately across the FBI, but would "push" information to agents and analysts who have a need to receive it timely. The Investigative Data Warehouse requires that information be affirmatively uploaded into the warehouse so that employees can then conduct searches. Updates must be made to the information in the warehouse, and the information in the warehouse is not available immediately or universally, unlike information in the VCF.

In sum, the Investigative Data Warehouse, while perhaps a useful tool, does not manage case workflow and does not substitute for an effective case management system. Consequently, the FBI continues to lack critical tools necessary to maximize the performance of both its criminal investigative and national security missions.

2. In its response, the FBI clarified the relationship between the VCF and the proposed Federal Investigative Case Management System (FICMS). During our audit, the FBI offered evolving explanations of the status of the VCF effort and its relationship with FICMS. In June 2004, the FBI had announced a two track corrective plan for the VCF, which included the development of what the FBI called the Initial Operational Capability (IOC) and the Full Operational Capability (FOC) for the VCF. The IOC represented a pilot test consisting of an electronic approval process. Employees were to create electronic documents on standard FBI forms, and these forms were to be sent for approval electronically from within the VCF IOC system. The goal of the pilot test was to determine the efficiency and effectiveness of the electronic approval process. Once the initial testing and evaluation

were completed, a determination was to be made as to how the FBI would proceed with future system deployments.

The FOC was intended to resolve outstanding issues, provide advice, and reevaluate requirements for the VCF. Additionally within the FOC, the processes for document creation, approvals, leads management, and evidence management were to be developed to determine the best phased approach to obtain the necessary components for the FOC.

However, FBI managers told the OIG audit team in November 2004 that the FICMS would replace the VCF and that requirements for the FICMS were to include user activities and processes for creating and approving documents and managing investigative leads, evidence, and cases. These requirements were expected to come from the VCF efforts already undertaken, and the VCF was described as the leading driver for the FICMS. Additionally, the creation of a Request for Proposal (RFP) from vendors for the FICMS was to include a full case management capability for the FBI. At the time, the OIG was left with the impression that, as the name implies, the FICMS was to be an actual system that could adopt aspects of the stalled VCF effort.

In commenting on a draft of this report, the FBI suggested that the FICMS represented a "framework" that would lead to a case management system. Whether the FBI intended the resulting case management system to be part of the FICMS effort or a separate follow-on effort remained unclear from the FBI's earlier comments.

However, in its formal response to this report, which is contained in Appendix 7, the FBI describes the VCF and the FICMS as two different projects proceeding in parallel. The FBI states that it is continuing to pursue the VCF through development of an implementation plan that will result in the deployment of a fully functional case and records management system. According to the FBI, it hired Aerospace Corporation to evaluate currently available software products to determine if they meet the FBI's requirements. The FBI also asked Aerospace to evaluate the adequacy of the VCF as delivered by SAIC to determine what might be salvaged from that effort.

In its response, the FBI also states that the FICMS project will develop a "framework that will govern development of DOJ and Department of Homeland Security (DHS) investigative case management systems to ensure the high level of inter-agency

compatibility needed to facilitate information sharing." The response states that the FICMS represents a broad blueprint for such systems and does not replace the VCF. As FICMS is being developed, the FBI plans to continue working on a case management system, whether it continues to be called the VCF or is given a new name.

As a result of this information, we have clarified the report to reflect the FBI's current description of the relationship of FICMS and the VCF.

3. In its response, the FBI agrees that its oversight of the Trilogy contracts should have been stronger, but it notes that the FBI had recognized its limitations and outsourced elements of the project to other entities, in accordance with guidance from the Department. The response discusses the role of FEDSIM in acting as the contracting office for key Trilogy contracts and of others in assisting the FBI with managing the project. The FBI's response also describes steps the FBI has taken to improve its IT management processes as part of what it called a "top-to-bottom reorganization" of FBI IT resources.

We agree that the responsibility for the contracting and management of the Trilogy project was shared among several parties, including the FBI and FEDSIM. However, the FBI selected FEDSIM and its Millenia contracting mechanism because the process could be expedited without the need to first fully develop the design requirements for the Trilogy project. Consequently, the FBI assumed certain risks in taking this path in attempting to expedite Trilogy's implementation. That approach created problems because the management processes requiring the development of schedule, cost, technical, and performance targets for Trilogy were not in place. Moreover, the FBI, as the consumer, had the primary responsibility for managing the project and overseeing those retained to assist in that management. However, we agree that having the FBI act as the project integrator was unrealistic, given the FBI's lack of expertise and experience to perform such a key function of ensuring that all three components of the project would mesh.

Additionally, while the FBI stated in its response that while it recognized its management limitations at the start of the project, it did not take the necessary steps to correct identified problems. Even internal FBI reports on Trilogy issued by the FBI's Inspection and Criminal Justice Information Service Divisions repeatedly pointed to the lack of both requirements and project oversight, including improper scheduling and cost estimates.

The OIG agrees that the FBI has taken a number of positive steps to improve its IT management recently. We have noted key improvements, including those cited by the FBI in its comments, beginning on page 33 of this report. However, these steps do not mitigate the significant deficiencies in the FBI's management of the Trilogy project, and the problems created by the delay in deploying the VCF and the associated cost increases. Moreover, while the FBI states that the VCF's Initial Operating Capability (IOC) was executed using the FBI's new approach to IT management "on schedule and within budget," the IOC is only one step towards a fully functioning case management system. The FBI still has significant work before it can develop and deploy a modern case management system.

Finally, in response to the FBI's "Conclusion" paragraph in its formal response, we agree that the FBI has taken steps to modernize its IT, particularly its infrastructure. But the FBI has not succeeded in its goal to replace the antiquated ACS system with a fully functional and effective case management system, despite more than 3 years in development and $170 million. This critical IT project affects the FBI's ability to perform its mission as effectively and efficiently as it should, and implementing an effective case management system should remain the FBI's top IT priority.

Response to Recommendations:

1. **Resolved.** In response to this recommendation, the FBI stated that it agrees that it must replace the ACS as quickly and as cost-effectively as feasible. The FBI reports that it has contracted to examine the VCF software, as well as available off-the-shelf software, to determine whether these products could be adapted to meet the FBI's needs. The FBI also points out in its response that technological innovation may have overtaken the FBI's original vision for the VCF, and that new products may exist to meet the FBI's need that did not exist when Trilogy began. We agree that the FBI must consider new and available technologies. In light of the FBI's agreement that it must replace the obsolete ACS system, this recommendation is resolved. The recommendation can be closed when the FBI demonstrates that a fully functional case management application replacing the ACS has been developed and deployed, and is being utilized throughout the FBI.

2. **Resolved**. This recommendation is resolved based on the FBI's agreement to devote all necessary resources to support a new case

management system. This recommendation can be closed when the FBI provides evidence that it has reprogrammed the resources necessary to meet its need for a functional case management system.

3. **Resolved.** This recommendation is resolved based on the FBI's agreement to take steps to establish critical design requirements for the case management system before initiating a new contract and ensuring that the contractor fully understands the requirements and has the capability to meet them. This recommendation can be closed when the FBI provides documentation demonstrating that the critical design requirements for the case management system have been established before initiating a new contract, and that the future contractor fully understands the requirements and has the capability to meet them.

4. **Resolved.** The FBI agrees with this recommendation, stating that the VCF project "suffered in part from runaway scope." The FBI response also states that it has learned from the VCF experience and that it has "adopted a process that will avoid a recurrence." This recommendation is resolved based on the FBI's agreement to incorporate the development efforts for the VCF into the requirements for any successor case management system. This recommendation can be closed when the FBI provides documentation demonstrating that the development of requirements for a future case management system incorporates the VCF development efforts for any successor case management system.

5. **Resolved.** The OIG acknowledges that the FBI has issued a Life Cycle Management Directive (LCMD), which resulted in the closing of a broader FBI-wide recommendation in December 2004 from a prior OIG report. However, the recommendation in this audit report addresses specifically the FBI Inspection Division's review of the Trilogy project's finances, rather than the broader new LCMD process. This recommendation can be closed when the FBI provides documentation that the financial systems used for tracking Trilogy project costs have been validated and improved to ensure complete and accurate data on project costs.

6. **Resolved.** This recommendation is resolved based on the FBI's agreement with the recommendation. The FBI's issuance of the LCMD resulted in closing a general FBI-wide recommendation in December 2004 from a prior OIG report. However, the current

recommendation can be closed when the FBI provides documentation demonstrating that upcoming Trilogy-related contracts have applied the LCMD and include defined requirements, progress milestones, and penalties for deviations from cost, schedule, performance, and technical baselines.

7. **Resolved.** This recommendation is resolved based on the FBI's agreement with the recommendation. Again, the OIG acknowledges that the FBI has issued a LCMD. However, this recommendation deals specifically with both existing and future Trilogy-related contracts. We also note that a recommendation from the OIG's report on the FBI's IT Investment Management regarding the need for establishing baselines has not been closed because the FBI has not provided evidence that it has established final cost and schedule baselines for the Trilogy project. Further, the Full Operational Capability phase of the VCF project is ongoing, and additional contracts will be required to complete Trilogy with a functional case management system. This recommendation can be closed when the FBI provides documentation demonstrating that it has established management controls and accountability to ensure that baselines are met for current and upcoming Trilogy-related contracts.

8. **Resolved.** This recommendation is resolved based on the FBI's agreement to apply ITIM processes to future IT projects, including additional Trilogy-related projects. Because key ITIM-related recommendations have not yet been closed from a prior report and the VCF portion of Trilogy remains in flux, we have included this recommendation to ensure the FBI provides appropriate follow-up as it develops a framework for a case management system and to completes and deploy such a system. This recommendation can be closed when the FBI provides documentation that it has applied ITIM processes to both existing and upcoming Trilogy-related projects.

9. **Resolved.** This recommendation is resolved based on the FBI's agreement with the recommendation and its stated progress toward completing an Enterprise Architecture. The OIG previously closed a recommendation from a prior OIG report that called for the FBI to continue its effort to establish an Enterprise Architecture. Due to the clear need for the FBI to have a blueprint to effectively manage its overall IT, including Trilogy, the current recommendation is for the FBI to monitor, or track, the development of its Enterprise Architecture to ensure that it meets its September 2005 deadline.

This recommendation can be closed when we receive documentation of an effective monitoring system for ensuring that the FBI's Enterprise Architecture is completed and implemented on schedule.