A REPORT TO THE

COMMITTEE ON APPROPRIATIONS

U.S. HOUSE OF REPRESENTATIVES

on the

FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF VIRTUAL CASE FILE

Surveys and Investigations Staff

April 2005

TABLE OF CONTENTS

SUMMARY

Investigative Results

By Committee direction, the Surveys and Investigations Staff undertook an investigation of the Federal Bureau of Investigation's (FBI) procurement and implementation of its new case management system called Virtual Case File (VCF). The investigation determined that:

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

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

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

-- The FBI's IT program management business structure and processes are now, for the most part, in place, although some of these processes need to mature.

Trilogy Program

Since September 11, 2001, the FBI has increased its terrorism efforts and its staff has grown from approximately 28,000 in FY 2001 to a projected 33,000 in FY 2006. Even with additional staff, success on all investigative fronts is highly dependent on Information Technology (IT). Trilogy is the FBI's effort to modernize the capabilities and functions of its legacy systems and related IT systems into an integrated, up-to-date IT infrastructure. After September 11, 2001, Trilogy's development strategy changed and, as a result, its cost increased from $379.8 million to $581.1 million, of which $170 million was for the User Applications Component, now known as VCF.

As initially planned, Trilogy had three components: the Information Presentation Component involving the upgrading of agent workstations, servers, and peripherals needed to gain access to FBI investigative applications; the Transportation Network Component which involved replacing the network and communications infrastructure providing connectivity between workstations and applications servers; and the User Applications Component which would replace five legacy applications. The Information Presentation Component and the Transportation Network Component portions of Trilogy are complete and operating.

The User Applications Component contract, to be developed in three phases, was awarded to the Science Applications International Corporation (SAIC) in June 2001. Work on Phase I, which was to "web-enable" the Automated Case Support system, was stopped after September 11, 2001. FBI officials decided they needed to move more quickly and, as a result, skipped Phase II and moved directly to Phase III to identify a case management system for the enterprise solution. Phase III began in January 2002, and by November 2002, FBI officials believed that VCF's requirements were adequately defined. SAIC's first product delivery, known as Delivery 1, was scheduled for December 2003, and was to replace the Automated Case Support system and another smaller application.

Termination of Virtual Case File

VCF was terminated on March 8, 2005. In early 2003, some officials involved in VCF's development began to see problems with the software development efforts which were attributed to contracting and program management oversight deficiencies. Technical and functional deficiencies became apparent following delivery of VCF's first product in December 2003. As a result, the FBI initiated several internal and external studies evaluating VCF Delivery 1.

In December 2003, the FBI's Cyber Division examined the VCF delivery and found issues with the database design and testing approach. The FBI's further examination of the VCF software identified functional deficiencies. In a March 2004 functional review, FBI personnel built several scenarios that would take an investigation through its life cycle, from opening the case through closure. The FBI identified 400 problems but did not share them with SAIC because it did not want the contractor to think these were the only issues remaining. On January 21, 2005, the Aerospace Corporation delivered its independent report on VCF which recommended discarding VCF Delivery 1 and starting over with a Commercial-Off-The-Shelf-based solution. Furthermore, SAIC advised it would cost $56.5 million more to complete VCF Delivery 1, which the FBI found unacceptable.

Contracting and Management Problems

Various contracting and program management weaknesses contributed to the failure of VCF. The FBI used a Governmentwide Acquisition Contract for Trilogy because of insufficient contracting personnel resources. The downside of this type of contract was that the FBI had to relinquish management control of the contract, which several officials believed negatively impacted VCF. Although the FBI used a cost plus award fee contract, which is appropriate for a software development effort, it lacked the necessary strong management and controls to effectively oversee the contract. Also, the failure to establish firm milestones or "control gates" before the project could move to the next phase resulted in the effort proceeding even after difficulties were identified.

The FBI also lacked a sound program management structure. This resulted in reports on VCF's progress being pushed down to lower management levels. Furthermore, those management processes that were in place were often circumvented. Deficiencies in program management included the lack of an empowered Chief Information Officer and the lack of documented, sound business processes, including life cycle management guidance for IT

development efforts. The FBI also had a shortage of skilled program managers and engineers. When the Trilogy effort, which initially was to be developed by one contractor, was awarded to two contractors, the already limited resources for contract oversight were further diluted. Finally, the FBI experienced high turnover among key program managers during Trilogy; for example, four Chief Information Officers in 4 years.

Virtual Case File's Workflow Test

Because of VCF's technical and functionality deficiencies, the FBI decided to only develop and test its automated workflow capability, which was a small portion of the functionality that was to be included in VCF. At the same time VCF was terminated, the FBI also decided to discontinue the automated workflow test of VCF. The test ran from December 2004 through March 2005, and provided agent and analyst users the ability to create case packages, such as a report of an interview, and submit them through an automated process. SAIC's delivery of the workflow capability was considered a complete success due to multiple factors including sound requirements, appropriate milestones, and high-level management involvement and oversight. It cost the FBI $17 million to conduct the workflow test. Several officials knowledgeable of software development and contracting procedures questioned the value of proceeding with the test in the first place, saying it was only done for political reasons because the FBI believed it had to deliver something.

Overarching Information Technology Management Issues

The FBI's efforts to effectively manage its IT investments have been adversely affected by overarching problems that impacted VCF and other IT initiatives. These problems included: (1) fragmented control over the management of IT resources, (2) lack of a disciplined approach to conducting program management, (3) limited number of qualified program managers, and (4) lack of an Enterprise Architecture. The FBI has made progress in addressing these problem areas. It is believed that the FBI's appointment of a new Chief Information Officer in May 2004, and the new management processes he has established have positioned the FBI for success in managing future IT investments. Furthermore, as part of the FBI's IT resources reorganization in June 2004, the FBI established the Office of Chief Information Officer to centrally manage IT responsibilities, activities, policies, and employees across the FBI. Also, in an effort to build a stronger project manager workforce, the Office of Chief Information Officer has begun to train additional personnel to be certified as Program Management Professionals. Finally, the FBI is working on its Enterprise Architecture, which it plans to complete by September 2005. Once complete, all IT projects will be required to be consistent with the Enterprise Architecture.

Enterprise Information Systems

The FBI's new case management effort, called the Enterprise Information Systems, has been approved "in principle" by the FBI Director, the Department of Justice, and the Office of Management and Budget; it has not yet been approved as an IT investment. The project is scheduled to take 39 months with incremental deliveries beginning 12 months after its start. FBI

officials advised that this new effort will be consistent with the Federal Investigative Case Management System, a framework of standards for Federal investigative agencies' core case management requirements.

The requirements developed for Enterprise Information Systems are now being vetted. FBI officials used, as a foundation, the results of the 2002 VCF requirements development process and lessons learned from the workflow test pilot. New capabilities, beyond those envisioned for VCF, will be included in the new system. The FBI started the system requirements and Concept of Operations prior to having an approved business case. Although working these efforts in parallel is contrary to the FBI's best practice life cycle management principles, a Bureau official advised that they are "scrambling" to meet senior management's desire to move ahead quickly. However, other FBI officials, while noting this parallel approach introduces some risk, advised that the risk will be mitigated since the project will not be allowed to go forward until approved by the FBI's Investment Management/Program Review Board.

FBI officials advised that they will be applying best practices in developing the Enterprise Information Systems. However, this does not always ensure success. A Government official advised that, with the program management changes adopted by the FBI, the "stars are aligned" for them to succeed. To be successful, an IT system needs, over and above good hardware and software, users to enter information into the system. The FBI, with specific guidance, is working to insure information is appropriately shared, both internally and with other law enforcement and intelligence agencies.

I. INTRODUCTION

A. Directive

By letter dated January 18, 2005, the Committee directed an investigation of the Federal Bureau of Investigation's (FBI) procurement and implementation of a new case management system called Virtual Case File (VCF). This investigation included a review of: (1) budget requests for FY 2000 through FY 2006; (2) procurement policies and procedures used to select and oversee the contractor; (3) issues which led to the product delivered not meeting FBI case management needs; and (4) FBI management practices related to VCF. This investigation also explored whether the FBI has applied lessons learned from past mistakes and has identified shortfalls in program management that, if corrected, would increase the likelihood for success in its future Information Technology (IT) development initiatives.

B. Scope of Inquiry

This investigation was conducted through interviews and the examination of documents provided by officials at the FBI and the General Services Administration's (GSA) Federal Systems Integration and Management Center (FEDSIM). In addition, interviews were conducted at the Office of Management and Budget (OMB) and the Department of Justice (DOJ) with officials knowledgeable about the FBI's IT efforts. Interviews were also conducted with former FBI officials and representatives of software development/systems engineering companies and non-profit technology and independent research organizations.

C. Background

The FBI has dual responsibilities as both a law enforcement and an intelligence agency. Following September 11, 2001, the FBI's efforts under both of these missions increased as a result of the focus on detecting and preventing terrorism. FBI staff has grown from approximately 28,000 in FY 2001 to a projected 33,000 in FY 2006. Even with additional personnel, success on all investigative fronts rests with a strong IT foundation. The FBI's overall FY 2006 budget request totals $5.7 billion, of which $1 billion, or approximately 18 percent, is for IT.

Trilogy is at the forefront of the FBI's efforts to modernize its IT systems into an integrated up-to-date infrastructure to support the agent's information handling needs. Trilogy, a three part program, was designed to provide a high-speed network, modern computer workstations and software, and a user application, VCF, to enhance the ability of agents to organize, access, and analyze information. This effort involved installing some 500 computer network servers, 1,600 scanners, and more than 20,000 desktop computers throughout the United States and overseas. The FBI has had problems in the past with respect to developing and implementing some IT systems. While the FBI embarked on a comprehensive overhaul and revitalization of its IT infrastructure with Trilogy, these problems persisted, particularly during the VCF part. VCF, as well as its related automated workflow test, was terminated in FY 2005.

Trilogy was originally expected to be developed and delivered by mid-2004. With the events of September 11, 2001, due to the urgent need for improved IT, Trilogy's development strategy changed and additional funding was provided. As a result, Trilogy's cost increased from $379.8 million to $581.1 million, an increase of $201.3 million, or 53 percent. The User Applications Component of Trilogy, which eventually became known as VCF, was originally estimated at slightly more than $100 million but eventually grew to $170 million.

II. TRILOGY PROGRAM

A. Program Description

Trilogy consists of three components: Information Presentation Component, Transportation Network Component, and User Applications Component. The FBI awarded the contract for the Information Presentation Component and the Transportation Network Component to DynCorp in May 2001; and the contract for the User Applications Component to Science Applications International Corporation (SAIC) in June 2001. While implementation of the first two Trilogy components have been completed, development and implementation of the User Applications Component failed and was terminated.

-- Information Presentation Component: This component's objective was to provide agents with a modern, up-to-date desktop computer environment to include improved e-mail capabilities. Deployment to all 56 FBI Field Offices, Information Technology Centers, and Resident Agencies was completed in April 2004.

-- Transportation Network Component: This component's objective was to provide encrypted telecommunications connectivity between and within all FBI facilities. The wide area network connectivity would allow investigative and intelligence information to be shared among agents in an accurate and rapid manner. Implementation of this component also was completed in April 2004.

-- User Applications Component: This component was originally envisioned as three phases: Phase I was supposed to "web-enable" five FBI investigative legacy applications to allow users to move from an antiquated, menu-driven system of navigating through the applications, to a user-friendly, "point and click" interface that would give the user a more familiar Microsoft Windows-like environment; Phase II required SAIC to rebuild the FBI's intranet website; and Phase III was supposed to identify an enterprise solution for updating and modernizing all of the FBI's systems applications, including the FBI's case management system, called Automated Case Support (ACS).

For the first 6 months of the contract, from June 2001 through December 2001, SAIC primarily worked on Phase I creating the web-enabled interface. However, following September 11, 2001, FBI officials determined IT modernization efforts needed to be accelerated and stopped SAIC's work on Phase I, where little progress had been made. The FBI instructed SAIC to skip Phase II and begin working immediately on Phase III. Phase III work was to focus on developing an automated case management system, which became known as VCF.

Phase III began in January 2002, with the FBI and SAIC working together to identify user requirements and desired system capabilities for VCF. By November 2002, FBI officials believed that the requirements and capabilities were adequately defined. SAIC's June 2001 contract for the User Applications Component was modified to reflect the new tasks identified for VCF.

Although VCF system capabilities were revised several times, it was ultimately intended to provide a seamless case management system which would support: (1) case creation and viewing capabilities, (2) documentation creation, (3) automated electronic workflow, (4) lead management, (5) evidence management, (6) searching, (7) reporting, (8) ticklers and notifications, (9) collection of operation metrics, (10) security controls, and (11) electronic records management. All of these features were to facilitate information storing, analysis and retrieval, and information sharing. According to the VCF contract, SAIC's first product delivery, known as Delivery 1, was scheduled for December 2003. The Delivery 1 product would replace ACS and another smaller application. Other legacy applications and enhancements were to be addressed in subsequent product deliveries.

B. Program Funding

Trilogy originally was estimated to cost $379.8 million but after September 11, 2001, program costs started to increase. The increase was primarily due to internal and external pressures exerted to accelerate Trilogy's development. Acceleration resulted in the FBI pursuing new strategies and, as it did, estimated program costs increased to $581.1 million. FBI officials noted that at the peak of activity in FY 2002, Trilogy accounted for $357 million, or about 41 percent, of the FBI's $878.4 million IT budget for that year. The following table shows, by category, the original and final estimated costs associated with Trilogy.

Original and Final Estimated Costs For Trilogy --- $ In Millions ---

Cost Category	2000 Estimate	Final Estimate
Transportation Network Component/ Information Presentation Component	$216.4	$348.5
User Applications Component (Virtual Case File)	103.4	170.0
Virtual Case File Validation	0	5.3
Program Management	22.0	32.0
Integrator	0	5.4
Contract Computer Specialists	0	0.6
Management Reserve	38.0	19.3
TOTALS	**$379.8**	**$581.1**

The FBI budget requests for Trilogy were for the entire program and did not identify specific amounts for its three separate components. The majority of the funding, or $357.1 million, came in FY 2002, with $229.7 million, or almost 40 percent, derived from FY 2002 emergency supplemental appropriations. The following table shows Trilogy's funding stream, by source, for FY 1999 through FY 2003. No funds were requested for Trilogy after FY 2003.

Trilogy Funding Stream by Source
FY 1999 through FY 2003
--- $ in Millions ---

Source	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	TOTALS
Regular appropriations	$20.0	$20.0	$20.7	$ 58.1	$ 12.4	$131.2
Supplemental appropriations				229.7		229.7
Reprogrammings					110.9	110.9
Working Capital Fund transfers	40.0			29.6		69.6
Emergency Response Funding				39.7		39.7
TOTAL	**$60.0**	**$20.0**	**$20.7**	**$357.1**	**$123.3**	**$581.1**

Obligations for Trilogy total $563.7 million through FY 2005, broken down as follows: FY 2001, $98 million; FY 2002, $214.5 million; FY 2003, $233 million; FY 2004, $17.1 million; and FY 2005, $1.1 million. Trilogy's FY 2005 unobligated balance is estimated at $17.4 million.

FBI officials generally agreed that the overall funding for VCF was adequate. However, the FY 2003 reprogramming request for $137.9 million created a problem. FBI officials had discussions with the Congress about the need for additional funding in November 2002. The FBI did not forward the reprogramming request to DOJ until late March 2003. After DOJ and OMB review, the request was sent to the Congress in late May 2003. Congress approved the reprogramming request in July 2003 for $110.9 million. One FBI official stated that this delay negatively impacted certain efforts relating to the VCF project, specifically with regard to the need for a systems integrator for the two contracts.

The obligations/expenditures for the three aspects of the User Applications Component development are: $1.2 million for the web-enabling effort (June 2001 – December 2001); $105 million for VCF (January 2002 – May 2004); and $16.7 million to test a VCF component (June 2004 – March 2005). In addition, the FBI spent $40 million on equipment. As of April 4, 2005, the FBI reported an unspent balance of $7.1 million.

III. TERMINATION OF VIRTUAL CASE FILE ACTIVITIES

A. Program Termination

The FBI made the decision to terminate VCF on March 8, 2005. FBI documents and some FEDSIM and FBI officials suggested that, for some time, the FBI had been leaning toward abandoning VCF. FBI officials advised that, although they have terminated VCF, they estimate that about $50 million of the amount expended includes reusable services and hardware. The officials noted that the hardware purchased for the effort is currently a part of or will eventually be used in Trilogy's IT infrastructure. FBI officials advised that the final decision to terminate the project was based on multiple factors.

By early FY 2003, some officials involved in VCF development began to see problems with the progress of the software development efforts which were attributed to contracting and program management oversight deficiencies. Following delivery of VCF's first product, Delivery 1, in December 2003, technical and functional deficiencies became apparent. As a result, the FBI initiated several studies and assessments evaluating VCF Delivery 1.

In December 2003, the FBI Director asked the Bureau's Cyber Division to examine the VCF delivery from a database application, hardware, and network perspective. This work was performed by systems engineers within the Division's Special Technologies and Applications Section. The Cyber Division's March 2004 report, which reflected SAIC's responses to certain questions, found issues with the database design and testing approach. Although the report made no recommendations as to whether the VCF delivery should be retained or discarded, a Cyber Division official advised that he voiced serious concerns about the delivery. This official also stated that he recommended an independent in-depth review.

The FBI's further examination of the VCF software delivered in December 2003 identified functional deficiencies. By letter dated January 21, 2004, FEDSIM, which managed the contract for the FBI, advised SAIC it should address 17 deficiencies prior to deployment of VCF. These deficiencies included such things as providing the ability to find individuals by specialty and job title, renaming "State" as "State/Province/Territory" on the Graphical User Interface, and providing the capability to serialize an existing document into a different case without workflow approval being required. In its response, SAIC argued that some of the "deficiencies" identified by FEDSIM were in fact "changes." By letter dated March 12, 2004, FEDSIM advised of the results of its "change versus fix" arbitration. It found that, of the 65 issues and sub-issues derived from the 17 original deficiencies, 20 were requirement changes; the remaining were system fixes.

The FBI undertook another functional review in March 2004. FBI personnel built several scenarios that would take an investigation through its life cycle, from opening the case, to setting leads, through closure to determine if the system would meet the FBI's operational needs. As a result of the review, the FBI identified about 400 problems. However, an FBI official advised

that the findings were not shared with SAIC because they did not want SAIC to think these were the only issues remaining. Further, the purpose of this review was to provide FBI officials with additional information needed to assess what should be done with VCF Delivery 1.

By letter dated March 22, 2004, FEDSIM requested that SAIC provide an Estimate to Complete the contracted for deliveries/releases. In response, SAIC advised that it would cost approximately $56.5 million, including $4.7 million for changes, to complete delivery of SAIC's first product. A FEDSIM official advised that additional projected costs for completing the contract, totaled $30.5 million: $11.9 million for completing two additional releases as required in the June 2001 contract; $13.4 million for projected software maintenance costs; and $5.2 million for the records management application and other developments. The FBI determined that the cost estimate to complete the VCF delivery was unacceptable.

Yet another study was requested beginning in July 2003, to be conducted by the National Academies, created by Congress in the 1860s to provide the Federal Government with independent and objective advice. The National Academies issued a May 2004 report, entitled *A Review of the FBI's Trilogy Information Technology Modernization Program.* The National Academies reported that "The FBI's IT modernization program is not currently on a path to success." The report raised several concerns about VCF. It noted that in the interest of rapid deployment, the current VCF schedule "appears to give little consideration to testing and presumes success at every stage." The Academies also noted that the FBI must allow adequate time for testing before any IT application, including VCF, is deployed, even if dates of initial operating capability were delayed.

The National Academies report also noted that the design process for VCF was well underway prior to the expansion of the FBI's intelligence mission. Therefore, the requirements for the processes supporting the intelligence mission were not included in the VCF design. "[B]ecause of the significant differences in IT requirements between systems supporting investigation and those supporting intelligence, the [Academies] strongly recommends that the FBI refrain from using the VCF as the foundation on which to build its analytical and data management capabilities for the intelligence processes supporting the counterterrorism mission." According to one Academies' official, this report could be considered a tutorial in IT management and system development for senior FBI management. After a follow-up briefing by the FBI, which updated the status of its IT efforts, the Academies, in a letter to the FBI Director, dated June 7, 2004, noted that although many challenges remain, the FBI has taken a number of important steps since the prior year that moved the FBI ahead in its IT modernization program.

In June 2004, the FBI developed a two-track plan for VCF to rectify deficiencies in the VCF development effort and to modify the existing system design to support incremental deployments. The first track was to develop and pilot the initial operating capability, that is, the automated electronic workflow component of VCF. An FBI official advised that the Bureau chose this process from the VCF delivery as the portion to be tested because it was the most mature function in the delivery. However, this official noted that the functionality represents only a small part of the overall VCF effort. By letter dated June 10, 2004, SAIC was informed to stop all work that did not specifically relate to the workflow functionality. The second track of the plan included an independent evaluation of the VCF delivery to determine if the software, as

designed, met the FBI's operational, security, and performance requirements. It also involved an examination of current Commerical-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) technologies and vendors.

In December 2004, Aerospace Corporation delivered the *COTS/GOTS Trade Study*. FBI officials advised that, compared to when the VCF project began, there are now many COTS applications products that address investigative case management needs. On the other hand, they noted that VCF, as developed by SAIC, uses custom coding with little COTS application software. The officials advised that the use of custom-developed software significantly increases the Government's operations and maintenance costs by requiring specialized personnel with knowledge of how the system was coded. Therefore, COTS products would be easier and cheaper to maintain. In addition, several FBI officials noted that it would be easier to upgrade or provide new capabilities to a system design or architecture based on using COTS applications products.

In response to the need for an independent review, on January 21, 2005, the Aerospace Corporation delivered its *Independent Verification and Validation of the Trilogy Virtual Case File, Delivery 1* report. An FBI official advised that Aerospace was provided the March 2004 version of the VCF delivery, which reflected changes SAIC made up to that point. Although some have suggested that Aerospace should have examined the December 2004 workflow capability delivery, an FBI official advised that, although SAIC corrected problems impacting the workflow capability, it is unlikely that it would have addressed other problems identified with the initial delivery in view of the stop work order of June 2004. Aerospace officials stated that, by applying best practices, they conducted a detailed engineering assessment of VCF delivery requirements and design documentation, source code, and artifacts. In short, because of the issues identified and pending the outcome of trade studies, Aerospace recommended discarding VCF Delivery 1 and starting over with a COTS-based solution.

B. Contracting Issues

FBI officials advised that the Bureau recognized it did not have the contracting personnel resources needed to conduct a full and open competition in the timeframe identified or to properly manage Trilogy's contract. Therefore, the FBI decided to use a Governmentwide Acquisition Contract, which is a task order or delivery order contract for IT established by an agency for governmentwide use. The benefits of a Governmentwide Acquisition Contract include being able to: (1) compete efforts between pre-qualified contractors, and (2) award contracts which are not protestable, that is, awards cannot be challenged or contested. The FBI chose GSA's Millennia Governmentwide Acquisition Contract, managed by FEDSIM. One of the primary benefits of using this type contract was that it enabled the FBI to move more quickly on its Trilogy efforts. However, an FBI official advised that the downside of using the Governmentwide Acquisition Contract was that the FBI had to relinquish control over managing the contract. Another FBI official advised that he attributed part of the problem with VCF's development to the fact that the FBI had no full-time contracting officer assigned to the effort. The official noted that, for a major project to succeed, one cannot have a part-time contracting officer.

1. Contract Awards

FBI officials advised that they had initially planned to identify one contractor to complete all three parts of Trilogy. However, these officials stated that DOJ, in an attempt to reduce risk, required the FBI to divide the Trilogy effort into more than one contract. As a result, the effort was split between two contractors: DynCorp and SAIC. FBI officials advised that two major problems evolved from splitting the contract. First, the FBI's already limited engineering and program management support were now divided between the efforts. This became more of an issue after September 11, 2001, when the sense of urgency resulted in the FBI pushing to develop the software faster. Second, some FBI officials advised that this change actually created more program risk, since the FBI assumed responsibility for integrating the work of two contractors. As one FBI official noted, the Government is generally not a good systems integrator. The FBI's efforts, according to another official, were not very effective due, in part, to its shortage of systems engineers. It was not until November 2002 that the FBI formally recognized the need for a systems integration contractor. The reprogramming to accomplish this did not occur until July 2003, which was too late to be of much help, according to one FBI official.

The FBI and FEDSIM received and evaluated five bids for the User Applications Component portion of the contract. Criteria used to evaluate the bids included cost reasonableness, quality of the technical approach, key personnel and project team knowledge and experience, and practicality of the management approach. The evaluation factors were weighted to reflect their relative importance, with the technical approach considered most important. An FBI official advised that, in selecting the winning contractor, cost was not a real discriminator, since the FBI and FEDSIM had disclosed the independent cost estimate for the work to be performed, and all those bidding on the contract came in with about the same cost estimate. DynCorp, which later merged into Computer Sciences Corporation, was awarded the contract for the hardware and network portions of Trilogy, while SAIC was awarded the contract for the User Applications Component portion of Trilogy.

According to an FBI official, SAIC won the User Applications Component portion of the contract because of the strength of its proposal to perform the web-enabling part of the effort. However, in view of the contract's change of direction after September 11, 2001, and the slow progress being made on the web-enabling effort, several FBI and FEDSIM officials commented that perhaps the SAIC contract should have been terminated and the effort recompeted. Because recompeting would further delay software development and since SAIC was already familiar with FBI systems, had security clearances, and could participate in the requirements development process, the FBI decided to go forward with the existing contract.

2. Lack of Firm Milestones

According to an FBI official, another contract issue was the failure to include firm milestones or establish "kill gates" having predetermined criteria. The kill gate or control gate concept, which was not familiar to one FBI program management official during VCF development, is designed to ensure that, as the program progresses, there are formal evaluation points where the Government can assess the contractor's progress. The contractor must

successfully complete the work up to that point or the contract can be terminated. Although several FBI officials and software development contractor representatives argued there were milestones for the development of the initial web-enabling effort and VCF, these slipped without repercussions, except for the impact on the contractor's award fee. One FBI official advised that there were several occasions during VCF development when problems were identified which could serve as a "perfect kill gate" for stopping further development. For example, this official advised that issues with the contractor's progress which were identified in March and September 2003 might have been an opportunity to terminate the effort, if firm milestones had been in place.

3. Contract Modifications

Although the FBI has been criticized for the number of contract changes, the fact that the contract was modified 37 times "means nothing," according to a FEDSIM official. One cannot draw any inferences from the number of modifications. In fact, according to this official, only 6 or 7 contract modifications for this IT contract were considered significant changes impacting scope, deliverables or schedule; the remaining changes were administrative or routine.

However, a major problem, according to some FEDSIM officials, was the fact that FBI officials were in discussions with SAIC and, without the Contracting Officer's knowledge, making changes that impacted the contract. This fact, along with confusing language in a contract modification, contributed to a misunderstanding as to the nature of the VCF scheduled delivery of December 2003. Specifically, on December 4, 2002, Contract Modification 12 established December 2003 as the date for a deployable VCF Delivery 1 product. On September 4, 2003, Contract Modification 22, although not specifically mentioning VCF, provided that the period of performance for the task order runs "through TBD [To Be Determined] years." A FEDSIM official characterized this change as an "administrative error" and advised that the scheduled December 2003 delivery could only be relieved by specific reference in the contract modification. However, one FBI official advised that, based on discussions with SAIC representatives, the FBI knew certain things would be missing from the December 2003 product delivery. FBI officials advised SAIC that it would not be evaluated on those missing items, which could not be tested because of delays in Computer Sciences Corporation's hardware delivery. Another FBI official stated the FBI had accepted the fact that it would be getting an evaluation copy. Further, SAIC maintained that based on the TBD language in the contract modification and discussions with FBI officials, it was known that the December 2003 product delivery would be an information or evaluation copy and not a deployable version.

By letter dated January 23, 2004 to FEDSIM, SAIC wrote that the December 2003 delivery was a "draft submission." In addition, SAIC advised that, at the FBI's request, SAIC adjusted its plans for VCF in September 2003 recognizing the product would not be deployed in December 2003 due to schedule changes for Trilogy's Information Presentation Component and Transportation Network Component. When the new scheduled date for completion of these components was provided in mid-November 2003, SAIC forecasted acceptance testing starting in February 2004 and system deployment in June 2004. However, by

letter dated February 9, 2004, FEDSIM advised SAIC that the Government did not recognize a draft submission as the deliverable. Further, FEDSIM wrote that "submitting a draft version of the product on the date the final was to be deployed does not meet the requirements of the task order."

4. Lack of Acceptance Criteria

According to FBI and FEDSIM officials, the initial contract and the modification addressing VCF did not have acceptance criteria for contract deliverables. As one of these officials remarked, acceptance criteria is needed so that the receiving agency can articulate a basis for accepting or rejecting a delivery. FBI officials declined to develop formal acceptance criteria. According to another official, the FBI's attitude was "I'll know it when I see it."

5. Cost Plus Award Fee Contract

The SAIC contract was a cost plus award fee contract. Although there has been some criticism of this type of contract, most officials from Government and systems/software development companies advised that a cost plus award fee contract is the best approach for a software development effort, particularly when user requirements are uncertain. Both the Government and the contractor share the risk of development with a cost plus contract. If VCF had used a firm-fixed price contract, the risk would have shifted to the vendor and the cost of the contract would have been very high. An FBI official advised that he doubted if any contractor would have bid on the VCF proposal, if the firm-fixed price contract was used. However, all officials cautioned that a cost plus award fee contract requires strong management and controls to ensure success. According to FBI officials, the FBI lacked these controls during this effort. One DOJ official suggested it would have been appropriate to rewrite the contract as fixed price once the requirements had been established in November 2002. However, both SAIC and the FBI objected. As it turned out, the requirements of November 2002 were not sufficiently detailed.

C. Program Management Issues

Several FBI officials advised that VCF was a high risk/high visibility project that did not receive adequate upper level management attention. Recognizing it lacked a sound program management structure, the FBI initiated efforts to formalize program management processes about the time the User Applications Component began development. However, as development progressed, FBI program managers began reporting to lower management levels, with more levels of managers in between. This slowed the decision-making process which created problems. By 2002, progress was being made with regard to the development of program management processes, with more focus on training and expertise. However, an FBI official advised that rigorous processes were not in place throughout the User Applications Component, including VCF, and, because of the pressure to deliver the needed software application, the processes that were in place were often circumvented.

1. Inexperienced Managers

FBI officials advised that the Bureau has had a shortage of experienced program managers. For example, one of VCF's project managers, who lacked project management experience and formal training, was also assigned to concurrently manage a second IT project. The second assignment began in mid-summer 2003, which was a critical period during VCF development. However, an FBI official advised that the Bureau attempted to address the deficiency with technical assistance contractor support.

In addition to a shortage of experienced program managers, the FBI was also experiencing high turnover of management, including Chief Information Officers. There were four Chief Information Officers during the VCF development. One DOJ official remarked that, for much of 2002, the FBI did not have a permanent Chief Information Officer. An FBI official advised that when upper management changed, some requirements would also change which led to misunderstandings in what was expected to be developed. However, a DOJ official remarked that if there were good experienced project managers at the lower level, the changes at the upper levels might have had less of an impact. An OMB official advised that, recognizing that people do not always stay in their Government jobs, it is important to have good documentation so that future management can pick up and continue the project without disruption.

2. Key Document Development

Representatives of a systems engineering company stated that the three key documents that define system development are the Concept of Operations, system architecture, and system requirements. Officials from the FBI, FEDSIM, and systems engineering firms identified issues with some or all of these documents that related to the User Applications Component, including VCF. These documents were considered inadequate and lacking in engineering rigor. Of particular concern, was the lack of good requirements and the resulting "requirements volatility" which, according to a systems engineering company representative, was a key driver in causing cost and schedule growth. Another systems engineering company representative commented that a good requirement is one that is measurable, and can be tested and verified. "Build me a nice house," is not a good requirement. A good requirement should be unambiguous and clear to anyone with appropriate technical background. It should trace back to what has been identified as the user's needs. This company representative noted that the need for clarity is important; if you only request a tire, the tire you receive might not have air in it.

Opinions as to the quality of the requirements varied. Several FBI officials advised that by November 2002, they did have "baseline" requirements for VCF, which were good enough for them to go forward with development. However, at the other extreme, a systems engineering company representative advised that during the initial User Applications Component development there were no requirements and, for VCF, the requirements were poorly defined. Several representatives of a software development company advised that, throughout the development of VCF, FBI representatives were making changes to or "tinkering" with these requirements. To the contrary, FBI officials argued that the FBI did not change or tinker with these requirements; what the FBI did provide was "useful clarifications" of what the

requirements meant. However, one FBI official commented that the baseline requirements were really "abstract requirements." Another FBI official acknowledged that the contractor had to interpret some of the requirements. In the end, still another FBI official advised that history tells them that these requirements were not good enough.

A systems engineering company representative advised that efforts to translate requirements could be perceived as clarification by some and tinkering by others; the issue as to what is "tinkering" is somewhat subjective. However, representatives of one systems engineering company advised that, although requirements can evolve, allowing requirements to change excessively is an undisciplined practice. The buyer and seller have a shared responsibility for such changes. A smart buyer knows changes will impact cost, schedule, and performance. A smart seller will tell the buyer that changes will impact cost, schedule, and performance. An undisciplined buyer and seller will have requirement changes throughout development with no regard for the impact on cost, schedule, and performance. However, disagreement exists between the contractor and the FBI as to whether the contractor had advised the FBI that the "tinkering" was having an impact on cost and schedule.

During 2002, while the FBI and SAIC were defining the requirements for VCF, the FBI was also engaged in re-engineering its business practices. Several FBI officials commented that it was appropriate to concurrently develop the requirements and re-engineer business processes. However, one FBI official remarked that, because of time constraints, doing both of these activities was difficult. The official remarked that the FBI was, in fact, trying to do too much at one time. A software engineering firm representative stated that changing business processes while identifying requirements was not a good course of action. The re-engineering of the business processes should be done first.

3. Risks Taken

Several FBI officials advised that the VCF approach was overly ambitious and there was a risk in doing a "big bang" development. These officials advised that an incremental approach to software development is preferable. Further, both FBI and SAIC officials stated that the rush to meet the December 2003 delivery schedule created risks; shortcuts were taken. However, one contracting representative noted that, after September 11, 2001, those individuals working on the project felt the country was at war. As a result, there was pressure to get a system in place quickly. However, as one FBI official remarked, when an initiative is schedule driven, the Government will usually have to give on cost and performance. Further, representatives of one non-profit independent research organization advised that the pressure to meet schedule can lead to failure in a software development effort. Finally, a Government contracting official stated the fact that there was a sense of urgency because of national security concerns should not have resulted in eliminating best practices relating to software development. In the end, as one FBI official advised, if one is going to let schedule drive the initiative, one should have a good plan in place to manage the risk.

D. Termination of Virtual Case File's Automated Workflow Test

At the same time that the FBI decided to terminate VCF, the decision was also made to not continue with the automated workflow test. From December 2004 through March 2005, the FBI conducted the automated workflow pilot test in its New Orleans Field Division and in the Criminal Investigative Division, Drug Unit at headquarters. This workflow test provided agent and analyst users the ability to create case packages, such as a report of an interview, and submit them through an automated process. Users were able to review, comment, and approve the insertion of the document package into appropriate FBI case files. The workflow test supported the upload or entering of the now approved documents into the existing Automated Case Support system for serialization.

Representatives of both the FBI and SAIC agreed that SAIC's delivery of the workflow capability in December 2004 was 100 percent of what SAIC was asked to do. Success of this delivery was attributed to the following: both the contractor and the FBI brought in their "A-teams" to work on the effort; the contract modification had appropriate milestones and "kill gates;" the requirements were reviewed and revalidated; there was little "tinkering" with the requirements; the Chief Information Officer at DOJ and executives at OMB were actively involved in the planning and program oversight; and the FBI selected a manageable piece for development that could be done in the timeframe allowed. However, as one FBI official advised, they "spent a lot of money," about $17 million, to make this workflow capability succeed.

Several officials knowledgeable of software development and contracting procedures questioned the value of proceeding with the workflow test in the first place, saying it was only done for political reasons because the FBI believed it had to deliver something. One official commented that "on no planet I know does it make sense" to spend $17 million on a pilot so that 250 users can participate in a test. On the other hand, FBI officials advised that the test provided lessons learned that can be applied to future software development efforts. One FBI official commented that, in deciding whether to proceed with a test, the FBI evaluated the best and worst case scenarios. The best case would be that the test would prove so successful that it would be rolled out throughout the rest of the FBI. According to this official, the worst case would be that they would not only be able to evaluate the system but would gain relevant information which would be helpful for future efforts.

Some FBI officials have argued that the workflow capability test is a success story. From the FBI's perspective, the workflow capability enabled them to test and evaluate the following: electronic workflow; the human machine interface; how the system interfaced with ACS; the network performance; and training effectiveness. However, the workflow test was not without criticism. Users' criticisms of the workflow process were initially identified in a March 2005 test evaluation and subsequently updated. In general, according to an FBI official, the evaluation showed that about 70 percent of the users saw more deficiencies than benefits to having this automated workflow capability. An FBI official advised that the Bureau will have its final report on the test results by April 30, 2005. This report will address all aspects of the test, to include the users' input, lessons learned with regard to managing the project within the FBI's new processes, and any issues related to training.

An FBI official provided a "rough-order of magnitude cost estimate" of $22.7 million for rolling out this workflow capability across the rest of the FBI, including the legal attachés located overseas, through the end of FY 2005. According to this official, the FBI preferred to use this money to build its future system as opposed to spending it on the tested workflow capability, which provided limited capability of questionable value to the users.

IV. OVERARCHING INFORMATION TECHNOLOGY MANAGEMENT ISSUES

A. New Program Management Initiatives

The FBI's efforts to effectively manage its IT investments have been adversely affected by overarching problems that impacted VCF and other FBI IT initiatives. These problems include: (1) fragmented control over the management of IT resources, (2) lack of a disciplined approach to program management, (3) a limited number of qualified program managers, and (4) lack of an Enterprise Architecture. The FBI has made progress in addressing many of these problem areas, such as the adoption of a systematic life cycle approach to managing IT projects. However, it will take time for these processes to mature and to see results.

Currently, the FBI's program management capability is still hampered by a shortage of project managers and systems engineering personnel. Building this capability, which is the Chief Information Officer's highest priority, is considered a formidable challenge that the FBI must be able to meet; otherwise, what the FBI is attempting to build today will unravel in the future. However, according to an FBI official, the FBI did not get internal support for the additional funds it sought in the FY 2006 budget to support IT. Nonetheless, it should be noted that the President's FY 2006 budget submission for the FBI reflects an increase of: (1) about $500 million over the FY 2005 appropriations request, and (2) over 1,400 staff positions above the FY 2005 level.

OMB and DOJ officials believe the FBI's appointment of a new Chief Information Officer in May 2004 and the new management processes he has put in place, many of which are considered industry best practices, have positioned the FBI for success in managing future IT investments. The officials stated the new Chief Information Officer is highly qualified and will bring much needed stability to the position. The officials pointed out, however, that long term success is dependent on the FBI's ability to effectively use the new management processes and to institutionalize them, that is, they must outlive the current Director and Chief Information Officer. An FBI official advised it generally takes 3 to 7 years for a Government agency to embrace program management principles. However, according to an Office of Chief Information Officer official, the most significant achievement to date in the FBI's efforts to improve IT management is the strong and unambiguous support provided by the Director.

1. Control of Information Technology Resources

Prior to June 2004, management of the FBI's IT resources was fragmented among the Information Resources Division and the various operating divisions having IT investments. As a result, there were a variety of processes and procedures for developing new IT investments. As part of the FBI's IT resources reorganization in June 2004, the FBI established the Office of Chief Information Officer to centrally manage all IT responsibilities, activities, policies, and employees across the FBI. The Office of Chief Information Officer is divided into four components: (1) policy and planning, (2) program management, (3) technology development,

and (4) operations and maintenance. Under this new organization, all IT projects will fall under the Office of Chief Information Officer. The Office of Chief Information Officer is responsible for the FBI's overall IT efforts, including developing an operating budget, developing and maintaining the FBI's technology assets, and providing technical direction for the reengineering of FBI business processes.

A high level Office of Chief Information Officer official stated it would take another 18 months for the reorganization to be 80 percent complete. This official described the Office's current status as "we are still crawling," and stated that although the Office of Chief Information Officer has formal authority to control all IT programs and services, the organization is not mature enough, in some areas, to assume that authority. For example, in the area of security and information assurance, the official stated that while the Office of Chief Information Officer has the authority for accreditation of information security, it is still working to get the resources needed to go with this authority. In addition, the official stated it would take time for the Office of Chief Information Officer to build effective working relationships with counterparts in other FBI divisions to facilitate resolution of differences arising over the transfer of IT resources. Part of the difficulty has to do with the differing opinions as to what is or is not an IT resource.

A high level Office of Chief Information Officer official stated that while the major technology issues are currently being handled by the Office of Chief Information Officer, there is concern as to whether there is sufficient support in the field to ensure the success of developed programs. According to this official, the transformation of the Office of Chief Information Officer is moving on one track, while IT modernization efforts are moving on another track. The remaining transformation challenge is to ensure that when an IT system delivery is made, the Office of Chief Information Officer organization and personnel are ready to support it.

2. Disciplined Program Management Approach

Recognizing its lack of a disciplined, systematic approach for executing its program management function, in September 2004, the FBI established an IT life cycle framework that fundamentally changed how it manages IT projects. The IT Life Cycle Management Directive, Version 2, dated November 19, 2004, governs how IT projects are to be managed "cradle to grave." It provides guidance to FBI personnel on the technical management and engineering practices covering the entire IT systems life cycle, including planning, acquisition, development, testing, operations and maintenance, refreshing, and disposition. Under this process, all IT projects are required to undergo rigorous project and executive level "control gate" reviews for each life cycle stage. The management process is comprised of seven gates, nine phases, and 14 key supporting processes. Decisions are made at each control gate review regarding the next steps for the project, including allowing the project to proceed to the next phase, directing rework before proceeding to the next phase, or terminating the project. An Office of Chief Information Officer official advised that this document is being revised to provide additional detail for the investment management process. This official stated that

Version 3 should be available around June 30, 2005. An Office of Chief Information Officer official ranked the Life Cycle Management Directive as one of the top three FBI initiatives undertaken to improve its management of IT projects.

Under its new management approach, the FBI has established five review boards to review IT projects. For example, an Investment Management/Project Review Board is to review and approve all new IT investments at specified stages of each project's life cycle. This is the most important of the review boards, according to an Office of Chief Information Officer official. A Technical Review Board reviews, coordinates, and provides technical guidance to ensure projects comply with technical requirements and meet FBI needs. The other boards are the: (1) Change Management Board, (2) IT Policy Review Board, and (3) Enterprise Architecture Board. In addition, the Chief Information Officer chairs the Information Technology Advisory Board, consisting of FBI Assistant Directors and Executive Assistant Directors, which meets quarterly to discuss IT matters with stakeholders.

One of the tools the FBI is developing to assist the review boards is the establishment of an IT metrics program that identifies and measures performance according to industry standards and Government regulations. According to FBI plans, when a project metric varies by more than 10 percent of the acceptable thresholds for cost, schedule and performance, it will trigger closer scrutiny and remediation by the Investment Management/Project Review Board.

3. Oversight of Information Technology Projects

As a part of centralizing management of all IT projects in the Office of Chief Information Officer, as of January 2005, the FBI had identified 89 existing IT projects and began evaluating them for overall health and placement within the Systems Development Life Cycle. Under the reorganized Office of Chief Information Officer, the Office of Information Technology Program Management is responsible for managing or overseeing all high priority projects. As of March 21, 2005, the Office of Information Technology Program Management had only 10 project managers and was responsible for managing 17 high priority projects. An Office of Chief Information Officer official stated there was no capacity to take on more work. Other operating divisions and the Chief Technology Officer continue to manage their own IT projects. However, since all projects, wherever managed, must be registered, the Office of Information Technology Program Management will have insight into the progress of these projects as they proceed through the life cycle management process. This is by virtue of its co-chair position on the Investment Management/Project Review Board.

The Office of Chief Information Officer's goal is to assign a project manager, systems engineer, and contracting officer technical representative to every IT investment project. A high ranking Office of Chief Information Officer official stated that currently his office only has about 50 percent of the project managers and systems engineers it needs. In an effort to mitigate this situation, the FBI has also obtained project management and engineering support

from contractors and will seek to get certified project managers from the Intelligence Community on a temporary basis. Increased staffing for the Office of Chief Information Officer is the Chief Information Officer's top priority.

According to an Office of Chief Information Officer official, to support IT agency-wide in FY 2006, the FBI requested 18 additional full-time positions and $29 million for non-personnel items, which is mostly to pay for contractor support. Included were 5 positions and $6 million for non-personnel costs to support the Office of Information Technology Program Management. However, DOJ and OMB budget cuts eliminated all 18 positions requested and reduced the non-personnel funding request from $29 million to $7 million. For FY 2007 and beyond, annual budget requests are to be based on an assessment of existing personnel strength and projected needs.

According to an Office of Chief Information Officer official, it is imperative the FBI establish a career service to attract and retain project manager expertise and adopt succession planning techniques to ensure retention of this capability for the long term. In an effort to build a stronger project manager workforce, the Office of Chief Information Officer has begun to train personnel to be certified as Program Management Professionals. According to the Office of Chief Information Officer, as of January 2005, it had two certified Government and five contractor program management professionals. Another 25 program managers, some of whom are from other FBI headquarters divisions, have completed the Program Management Professional review course and plan to take the certification test; an additional 20 were enrolled in the training program.

A high level Office of Chief Information Officer official stated the FBI is considering engaging a Federally Funded Research and Development Center to supplement its personnel resources and to help manage its IT investments. A Federally Funded Research and Development Center is a not-for-profit entity that is expected to operate in the public interest with objectivity and independence, and is free of organizational conflicts of interest. Agencies which have Federally Funded Research and Development Centers use them to meet special long-term research or development needs that cannot be met as effectively by existing in-house or contractor resources. An Office of Chief Information Officer official stated a primary benefit of a dedicated Federally Funded Research and Development Center is its ability to provide "just in time" resources. It is able to do this because it forms a partnership with the Chief Information Officer and is involved with the agency's total IT effort. As a result, the Federally Funded Research and Development Center would be able to develop an understanding of what the Chief Information Officer is trying to accomplish and can anticipate his needs.

4. Enterprise Architecture

For a number of years the FBI carried out its IT investment program without the benefit of an Enterprise Architecture. An Enterprise Architecture, which depicts the connection between an organization's business processes and the IT infrastructure that supports them, is intended to ensure the alignment of IT with an agency's strategic goals. IT management experts stated that although it is possible to successfully complete an IT project in the absence of an Enterprise Architecture, it is dangerous to develop IT projects in isolation because they may not work well with the agency's other systems. It was not until December 2004 that the FBI first

completed a baseline, or "as is" Enterprise Architecture. It is currently working on a target, or "to be" Enterprise Architecture, which it plans to complete by September 2005. All future IT projects will be required to be consistent with the Enterprise Architecture. According to the FBI, it has already identified all of the IT systems, applications, networks, and databases in the FBI in an IT master systems list.

In its May 2004 report, the National Academies stressed the importance of top FBI management's involvement in the creation of the Enterprise Architecture. It pointed out development of the Enterprise Architecture cannot be delegated to the Chief Information Officer or to a contractor, as only the FBI's senior leadership can establish the policies, define the operational frameworks and priorities, and make the tradeoffs necessary to formulate the new strategic view. According to Office of Chief Information Officer officials, top managers with the FBI are actively engaged in developing the target Enterprise Architecture. This includes the Director, Executive Assistant Directors, and Assistant Directors. Of particular importance in building the Enterprise Architecture is top management's communication of their business practices and performance criteria, in other words, how they do business and what they want to achieve. The Office of Chief Information Officer has reconstituted the Enterprise Architecture Board to include senior representatives of 11 operational divisions of the FBI; Executive Assistant Directors will be asked to approve the Enterprise Architecture. According to an Office of Chief Information Officer official, the Executive Assistant Directors regularly attend Enterprise Architecture Board meetings.

B. Additional Information Technology Management Initiatives

In addition to the major initiatives, the FBI has undertaken a number of additional IT management improvement initiatives. Included are: (1) a Strategic Information Technology Plan; (2) Information Technology Portfolio Management; (3) Information Technology Portfolio Management Automation Project; and (4) a Master Information Technology Policy List.

1. Strategic Information Technology Plan

The Office of Chief Information Officer completed a Strategic Information Technology Plan in December 2004. The Plan maps out how IT will support the FBI's Strategic Plan and mission goals over the next 5 years. According to FBI officials, all IT projects are now required to be consistent with this Plan.

2. Information Technology Portfolio Management Program

The Information Technology Portfolio Management Program focuses on performance assessments of IT investments in the operations and maintenance phase of their life cycle. According to FBI officials, the majority of their IT investments reside in this phase. The program's primary objective is to provide senior managers with information to help them make

more informed decisions about IT investments. Management recommendations from this program are expected to focus on investments that should be leveraged, replaced, outsourced, or retired. The estimated completion date for this initiative is December 31, 2005.

3. Information Technology Portfolio Management Automation Project

The Information Technology Portfolio Management Automation Project is intended to develop the FBI's Enterprise Information Technology Tool. This is a software package designed to identify and track sanctioned IT projects with baselined plans, schedules, scope, and costs. Also, the FBI plans to use the tool to electronically track all IT projects throughout their life cycle. This feature is intended to help ensure new IT investments are aligned with mission goals. The estimated completion date for this initiative is July 31, 2005.

4. Master Information Technology Policy List

The Office of Chief Information Officer is establishing a Master Information Technology Policy List to coordinate IT. According to FBI officials, once this list is established any new IT policies or modifications will have to be reviewed and approved by the Information Technology Policy Review Board. Over 100 policies relating to IT have been identified. The Master Information Technology Policy List will enable the Office of Chief Information Officer to enforce all applicable IT policies. The estimated completion date for this initiative is April 30, 2005.

V. ENTERPRISE INFORMATION SYSTEMS: THE LASTEST CASE MANAGEMENT SYSTEM

A. System Development

The FBI has developed and is now vetting requirements for the Enterprise Information Systems, a new case management system which will enable modular expansions with new capabilities. The FBI made use of the results of the 2002 VCF requirements development process and lessons learned from the workflow test in New Orleans in developing the new system. Enterprise Information Systems, which also has been referred to as VCF Track II and Project Z, is being designed to replace the Automated Case Support system and certain other legacy applications. Current plans call for the Automated Case Support system to be phased out incrementally as Enterprise Information Systems deliveries take over specific functions and related data has been migrated to the new system's databases. An Office of Chief Information Officer official advised that there is considerable risk to this data migration effort, which will require existing data to be reviewed and evaluated for relevance and accuracy. The FBI is, however, conducting an internal analysis to identify a data migration strategy that can be used to mitigate the risk. Officials expect to complete the analysis by December 2005.

Other applications supporting analysis, although initially included in VCF, will be handled outside the Enterprise Information Systems. There will be a linkage allowing access to information stored in Enterprise Information Systems' case file database. Enterprise Information Systems will also satisfy new requirements by delivering capabilities currently provided by other legacy applications, including the Bank Robbery Statistical Application and the Financial Institution Fraud/Suspicious Activity Report. These applications capture pertinent statistical information relevant to measuring performance. The last phase of Enterprise Information Systems will provide interfaces to the remaining FBI legacy systems.

FBI officials advised that the Enterprise Information Systems team, consisting of FBI personnel and contractor support, will develop its new case management system primarily with the use of COTS products. However, according to recognized software engineering experts, there is some risk attached to building systems with COTS products. Without careful program management and business stakeholder attention, the often touted benefits of using COTS products, such as reduced operations and maintenance costs and ease of introducing newer capabilities, may not be achieved. FBI program managers stated they are sensitive to these risks. Although they recognize that end-users may have some specific requirements that the selected COTS products cannot meet, the intent is to maintain the efficacy of the selected COTS software packages. According to an FBI official, they will not open any COTS products to make modifications. If the package does not meet the FBI's needs they will reconfigure the systems within the allowable constraints of the COTS package, reengineer FBI processes to fit the COTS capability, or request the vendor add features the FBI would like, to its commercial offering.

FBI officials also advised that Enterprise Information Systems will be consistent with the Federal Investigative Case Management System. In May 2004, as a part of its E-Government and Federal Enterprise Architecture effort, OMB chartered five cross-Federal Government groups, called Line of Business Task Forces, to determine the feasibility of common IT solution platforms to support various Federal agencies' like-business processes, such as human resources, financial management, and case management. DOJ was named Managing Partner for the Case Management Line of Business. The FBI became the Executive Agent to assess the feasibility of a standard architecture and solutions addressing investigative agencies' core case management requirements. The Federal Investigative Case Management System is the investigative portion of this Federal case management effort.

Office of Chief Information Officer officials advised that, by using software development management best practices documented in the FBI's Life Cycle Management Directive, they will be able to better control the development process for Enterprise Information Systems. However, an FBI official advised that they were concurrently developing the program business case, the Concept of Operations, and the requirements. This official advised that they were undertaking these efforts in parallel rather than sequentially, contrary to life cycle management principles, due to the time pressure to award the contract in early FY 2006. One official commented that the project team was "scrambling" to meet senior management's desire to move ahead quickly. This official commented that this parallel approach to the life cycle phases does add some risk. However, he advised that the risk will be mitigated since the project will not be allowed to go forward until approved by the Investment Management/Program Review Board.

B. Program Cost

FBI officials advised that they are analyzing independent cost estimates from two not-for-profit technical services contractors to gain a better understanding of what it will cost to build the new system. Those cost projections were not available as of April 19, 2005. However, FBI officials stated that, for FY 2006, the cost of Enterprise Information Systems will "come out of hide." One Office of Chief Information Officer official noted that with the planned consolidation of IT activities and funds, he believed there would be opportunities to identify IT funds that could be reprogrammed for higher priority needs.

Although the Enterprise Information Systems approach has been approved "in principle" by the FBI, DOJ and OMB, it has not yet been approved as an IT investment for inclusion in the FY 2007 budget. The total life of the project is planned to be 39 months with incremental deliveries beginning 12 months after its start.

C. Program Success

An FBI official advised that the Bureau is focused on ensuring the use of best practices in its future IT development efforts. However, as the representative of one non-profit independent research organization advised, applying best practices is important; but these will not always ensure success. An OMB official advised, however, "the stars are aligned" for the future management of the FBI's IT program to be successful.

Notwithstanding the FBI's planned improvements, hardware and software are only two components of a successful IT system. A third component is the need for the users to adopt the system and to enter information into its database. For example, a representative of the National Academies advised even if an IT effort is executed perfectly, that does not mean that it will be successful if the system is not used and necessary information is not placed in the system. This representative noted that if, for example, an agent has information that may be helpful in making an arrest or other activity by which the agent's performance is evaluated, then the agent might not want to share that information and run the risk of another agent using it to make an arrest or achieve the accomplishment.

A subject matter expert in IT strategic thinking also advised that, for an organization to succeed in its IT efforts, it must ensure its business processes are appropriate. This includes ensuring that an agency's performance review processes reward the right activity, in this case, sharing information. However, experts agree it is difficult to measure whether an organization's culture has changed with regard to recognizing the need to communicate and share information.

The need to appropriately share information is not lost on the FBI. An FBI official advised that the field offices have been told to follow FBI Intelligence Collection and Reporting Guidance, which are specific to different types of investigations, cases, and programs. This guidance is updated periodically and specifies dissemination instructions. Further, any restrictions controlling access to case information must be approved at a senior management level. As one FBI official stated, the culture of the FBI, as it relates to sharing information, has changed significantly in the last few years. "The days of agents not sharing information, either internally or externally, are over." Another FBI official advised that there is not an agent out there who would want to risk knowing something that could prevent a terrorist attack and not sharing it; if anything, agents are going to the other extreme with regard to sharing information. A third official commented "telling Agents to share information is like telling them to be investigators; it's basic to what they do."

To demonstrate how things have changed in the FBI, an official discussed the Bureau's inspection process by which it can evaluate whether relevant investigative information is being uploaded into the FBI's system. FBI officials noted that most FBI investigations are now worked jointly with other law enforcement agencies; not only is case information shared but sources/informants are also worked jointly. When an inspection team visits a field office it reviews each squad's top 10 cases; any gaps in the investigation case file would be noted and action pursued to correct issues identified. In addition, to ensure cooperation with other agencies, the inspectors meet with representatives of state, local and other Federal law enforcement agencies to identify any issues which would reflect a lack of cooperation on the FBI's part. In this inspection process, statistical accomplishments reflecting arrests, convictions, etcetera, are no longer emphasized because it is recognized that the quality of the investigation is of greater importance.

* * * * *