Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice
before the
Senate Committee on Appropriations
Subcommittee on Commerce, Justice, State and the Judiciary
concerning
The Federal Bureau of Investigation's
Trilogy Information Technology Modernization Project

I. INTRODUCTION

Mr. Chairman, Senator Leahy, and Members of the Subcommittee on Commerce, Justice, State and the Judiciary:

I appreciate the opportunity to testify before the Subcommittee as it examines the Federal Bureau of Investigation's (FBI) Trilogy information technology (IT) modernization project. The Trilogy project was designed to upgrade the FBI's IT infrastructure and replace its antiquated case management system with the Virtual Case File (VCF).

Successful implementation of the Trilogy project is essential to modernizing the FBI's inadequate information technology systems. The FBI's systems currently do not permit FBI agents, analysts, and managers to readily access and share case-related information throughout the FBI. Without this capability, the FBI cannot perform its critical missions as efficiently and effectively as it should.

In March 2004, this Subcommittee held a hearing on the status of the Trilogy project, and I testified about the schedule delays and cost increases of the Trilogy project. At that time, I stated that I was skeptical about the FBI's proposed schedule to deploy a fully functional, complete version of the VCF before the end of calendar year 2004. Shortly before the hearing, the Office of the Inspector General (OIG) initiated a follow-up audit to assess the FBI's management of the Trilogy project.

Today the OIG released the results of this follow-up audit. Our audit found that the FBI successfully has completed the Trilogy IT infrastructure upgrades – albeit with delays and significant cost increases. However, the FBI has failed to complete and deploy the VCF, the critical component of Trilogy that was intended to provide the FBI with an effective case management system. The VCF still is not operational after more than 3 years of development and the allocation of $170 million. We found that the VCF either will require substantial additional work or need to be scrapped and replaced by a new system. Moreover, the FBI has not yet provided a realistic timetable or cost estimate for implementing a workable VCF or a successor system.

Our audit also examined the causes for the delays and cost increases in the Trilogy project. Among the problems were poorly defined and slowly evolving design requirements for Trilogy, weak IT investment management practices at the FBI, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on the Trilogy project, unrealistic scheduling of tasks on Trilogy, and inadequate resolution of issues that warned of problems in Trilogy's development.

In this statement, I describe the OIG's examination of the Trilogy project. The statement is organized into five parts. First, I provide a brief description of prior OIG assessments and testimony about the FBI's IT systems in general and Trilogy in particular. Second, I provide background information on the Trilogy project. Third, I discuss the results of the OIG's recently completed audit regarding Trilogy's cost increases and schedule delays. Fourth, I discuss the OIG's assessment of the causes for the problems in Trilogy's development and implementation. And fifth, as requested by the Subcommittee, I conclude my statement by briefly highlighting several ongoing and recently completed OIG reviews that examine a variety of other issues in the FBI.

II. PRIOR OIG REVIEWS OF FBI INFORMATION TECHNOLOGY

In a series of reviews over the past several years, the OIG has identified problems in the FBI's IT systems, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training.

For example, a July 1999 OIG review examined the actions of the Campaign Finance Task Force that investigated allegations of improper fundraising practices during the 1996 Presidential campaign. The Task Force relied on the FBI's antiquated case management system, the Automated Case Support (ACS) system, and other FBI databases to obtain information on the individuals and organizations that had become subjects of the investigation. In this review, the OIG noted that deficiencies in the ACS system and the way search results were handled within the FBI resulted in incomplete data being provided to the Task Force.

Another OIG review issued in March 2002 examined how the FBI had failed to turn over to defense attorneys hundreds of FBI documents that should have been disclosed prior to the trials of Timothy McVeigh and Terry Nichols. The OIG again concluded that the FBI's computer systems were antiquated, inefficient, and badly in need of improvement. We found that the ACS could not handle or retrieve documents in a useful, comprehensive, or efficient way, and it did not provide FBI employees with the type of support they need and deserve.

An OIG audit issued in December 2002 examined the FBI's IT investment management practices. This audit concluded that that the FBI had not effectively managed its IT investments because it had failed to: 1) effectively track and oversee the costs and schedules of IT projects; 2) properly establish and effectively use IT investment boards to review projects; 3) inventory the existing IT systems and projects; 4) identify the business needs for each IT project; and 5) use defined processes to select new IT projects. We concluded that the FBI continued to spend hundreds of millions of dollars on IT projects without adequate assurance that the projects would meet their intended goals. Our audit made eight recommendations with respect to Trilogy, including urging the FBI to establish schedule, cost, technical, and performance baselines and track significant deviations from these baselines.

In a September 2003 audit, the OIG examined the FBI's implementation of the OIG's prior IT-related recommendations. While we found that the FBI had made substantial progress by implementing 93 of 148 total recommendations, we concluded that full implementation of the remaining recommendations was needed to ensure that the FBI's IT program effectively supported the FBI's mission.

As noted above, in March 2004 this Subcommittee held a hearing to examine Information Technology in the FBI, at which the FBI Director testified about the status of the FBI's Trilogy project. At that hearing, the FBI stated that it planned to have "a network with Full Site Capability by late spring" and that it was "closing in on the goal of completion" of the Trilogy project.

The OIG initiated our follow-up audit to assess the FBI's management of the Trilogy project. In December 2004, the OIG completed a draft of this audit report and concluded that the VCF was not operational after more than 3 years of development and the obligation of $170 million, and the FBI did not know when the VCF or a replacement system would be implemented.

Pursuant to our standard practice, in late December 2004 the OIG provided the draft audit report to the FBI for its response. In early January 2005, the FBI publicly acknowledged problems and delays in the development of the VCF. In a written response to our audit report dated January 26, 2005, the FBI acknowledged that the VCF had not met its goals with respect to development of an automated case management system. Nevertheless, the FBI stated that the "VCF project remains the highest IT priority for the FBI."

After receiving the FBI's comments, the OIG completed this audit report and released it today.

I will now provide background on the Trilogy project and the VCF before summarizing the main findings of our audit.

III. BACKGROUND ON TRILOGY

Trilogy is the largest of the FBI's IT projects. As originally designed, the Trilogy project had three main components:

1) the Information Presentation Component (IPC) – which was intended to upgrade the FBI's hardware and software;

2) Transportation Network Component (TNC) – which was intended to upgrade the FBI's communication networks; and

3) User Applications Component (UAC) – which was intended to replace the FBI's most important investigative applications, including the ACS, the FBI's antiquated case management system. Among its major shortcomings, the ACS does not permit FBI agents, analysts, and managers to readily access and share case-related information throughout the FBI. Without this capability, the FBI cannot efficiently bring together all of the investigative information in the FBI's possession to solve crimes or help prevent future terrorist attacks.

The first two components of Trilogy provide the infrastructure needed to run the FBI's various user applications, while the UAC was intended to upgrade and consolidate the FBI's investigative applications. After the September 11 attacks, the FBI decided to replace the ACS with an entirely new case management system, the VCF.

It is important to note that Trilogy was not intended to replace all 42 of the FBI's investigative applications or the FBI's approximately 160 other non-investigative applications. Rather, Trilogy was intended to lay the foundation so that future enhancements would allow the FBI to achieve a state-of-the-art IT system that integrates all of the agency's investigative and non-investigative applications.

Our audit found that in late April 2004, the FBI completed the first two components of the Trilogy project. The FBI deployed new hardware and software, including 22,251 computer workstations, 3,408 printers, 1,463 scanners, and 475 servers, and it installed new communications networks.

However, as I describe in the next section of this statement, this deployment was not done as quickly as the FBI hoped or expected. Despite the fact that after the September 11 attacks Congress appropriated the FBI an additional $78 million to accelerate deployment of Trilogy's infrastructure components, the FBI completed the two infrastructure components by late April 2004, just before the FBI's original target date of May 2004. Consequently, the FBI missed by some 22 months the completion date for the two infrastructure components under the accelerated schedule funded by

Congress. In addition, the total costs for the infrastructure components of Trilogy increased from $238.6 million to $377 million over the course of the project.

And while the infrastructure components are now in place to support improved investigative applications, the FBI still is far from implementing the third component of Trilogy, the VCF.

IV. RESULTS OF OIG AUDIT OF TRILOGY PROJECT

A. Trilogy Costs

Trilogy originally was planned in 2000 as a 3-year, $380 million project. Over its life, Trilogy has become a $581 million project that has suffered a continuing series of missed completion estimates and associated cost growth.

Initially, in November 2000, Congress appropriated $100.7 million for the first year of the project. In May 2001, the FBI hired DynCorp (which later merged into Computer Sciences Corporation (CSC)) as the contractor for the IPC/TNC infrastructure components of Trilogy. At that time, the scheduled completion date for the Trilogy infrastructure was May 2004. In June 2001, the FBI hired Science Applications International Corporation (SAIC) to develop the user applications component of Trilogy (which became the VCF), with a scheduled completion date of June 2004.

In early 2002, the FBI informed Congress in its *Quarterly Congressional Status Report* that with an additional $70 million in FY 2002 funding, the FBI could accelerate the deployment of Trilogy. Congress supplemented the Trilogy budget with $78 million from the Emergency Supplemental Appropriations Act of January 2002, thereby raising projected costs to $458 million.

In December 2002, the FBI estimated it needed $137.9 million more to complete Trilogy, in addition to the $78 million it had received to accelerate completion of the project. Congress approved a $110.9 million reprogramming of funds that took into account the estimates to complete the IPC/TNC portions of Trilogy, as well as an estimate of the 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 – $201 million more than originally estimated.

The following table describes the cost of Trilogy under the original plan and under the current plan:

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

B. Schedule for Trilogy Infrastructure Components

Despite the increased money provided for Trilogy, its implementation has been delayed significantly. Part of the problem we found was that a stable schedule for Trilogy never was firmly established for much of the project's history. Beginning in 2002 the FBI's estimated dates for completing the Trilogy project components began to swing back and forth and were revised repeatedly.

The original completion date for deploying the Trilogy infrastructure (the first two components of Trilogy) was May 2004. After the September 11 attacks, the FBI recognized the urgency of completing the project and moved up the completion date for deploying the Trilogy infrastructure to June 2003. Later, the FBI said the infrastructure would be completed by December 31, 2002. Still later, the FBI informed Congress that with an additional $70 million it could accelerate deployment of Trilogy and complete the two infrastructure components by July 2002 and also deploy the most critical analytical tools in the user applications component.

Yet, the timetable for completing the infrastructure components slipped from July 2002 to October 2002 and then to March 2003. On March 28, 2003, CSC completed a communications network, the Wide Area Network, for Trilogy. The FBI reported that the Wide Area Network, with increased bandwidth and three layers of security, had been deployed to 622 sites. In April 2003, the FBI also reported to Congress that more than 21,000 new desktop computers and nearly 5,000 printers and scanners had been deployed.

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 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 General Services Administration (whose Federal Systems Integration and Management Center, known as FEDSIM, had awarded contracts for Trilogy on behalf of the FBI) formally announced that CSC had failed to meet the deadline for completing work on infrastructure portions of Trilogy that were required to support the VCF user application under development.

On December 4, 2003, CSC signed a commitment letter agreeing to complete the infrastructure components of the Trilogy project by April 30, 2004, for an additional $22.9 million, including an award fee of over $4 million. An award fee is used when the government wants to motivate a contractor with financial incentives. 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 the April 30, 2004, deadline was not met. In addition, the revised statement of work provided for cost sharing at a rate of 50 percent for any work remaining after the April 30 deadline.

CSC met the revised deadline of April 30, 2004, for completing the two infrastructure components of Trilogy. As a result, the FBI met the original target set in 2001 for the infrastructure components of Trilogy, but missed the accelerated schedule funded by additional money from Congress by some 22 months.

C. Schedule for the Virtual Case File

In June 2002, the FBI decided to deploy the VCF user application component of Trilogy 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 was supposed to consist of the initial version 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. Deliveries two and three under the contract were supposed to consist of enhancements and additional operational capabilities to the VCF.

SAIC provided the first version of the VCF to the FBI in December 2003, in accordance with the accelerated schedule. However, the FBI did not accept that version because the FBI said it was not a functional system and did not meet the FBI's requirements. Deliveries two and three never occurred because of the difficulties experienced in completing the initial version of the VCF. The FBI informed the OIG that these deliveries are not being pursued now given the problems in the first delivery and the FBI's plans to seek a common interagency platform for a case management system (the Federal Investigative Case Management System or FICMS, which is discussed below).

In fact, the FBI has abandoned the intended three VCF deliveries and instead announced a new two-track approach for continuing development of the VCF. Track one, which the FBI refers to as the "Initial Operational Capability," includes a 6-week test of an electronic workflow process scheduled to be completed by March 2005. During this test, the FBI's New Orleans field office and a smaller resident agency office will enter investigative lead and case data into a prototype VCF file system, and this information will be approved electronically and uploaded into the ACS. The FBI intends to obtain user comments on, and assess the performance of, this new workflow system being tested in track one.

However, it is important to make clear that the version of the VCF being tested in track one will not provide the FBI with the case management applications as envisioned throughout the Trilogy project because it represents just one developmental step in the creation of a fully functional investigative case management system. It does not offer full case management capabilities. Rather, it 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 ACS. In track two, the FBI plans to identify user activities and processes for creating and approving documents and managing investigative leads, evidence, and cases. As a result of the information gleaned during track two, the FBI is updating and confirming the case management requirements and evaluating whether currently available software can be adapted for a case management system rather than creating a completely new system.

In commenting on the findings in our audit report about the delays in the VCF, the FBI stated that "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." This suggests that the current VCF effort may be obsolete and that the FBI may implement an entirely new system to replace it.

Moreover, our audit found that the FBI still does not have a clear timetable or prospect for completing the project. The VCF case management application was intended to replace the ACS and be the sole system within the FBI that would contain all investigative lead and case file information in a paperless system. Due to the failure to complete the VCF, the FBI continues to lack a modern case management system containing complete and accessible investigative lead and case information. While the FBI cites in its response to our report advances in other FBI IT systems, such as its newly created Investigative Data Warehouse, 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. Various lead and case information easily could be associated for analysis. The Investigative Data Warehouse, while perhaps a useful tool, does not manage case workflow, does not provide immediate access to case information, 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.

D. Federal Investigative Case Management System

As a parallel effort to the VCF, the FBI recently has stated that it is pursuing an effort to develop the Federal Investigative Case Management System (FICMS). FBI officials have variously described this effort to the OIG during the course of our audit as a continuation of the VCF, a new investigative case management system to replace the failed VCF, or a "framework" for the future development of an investigative case management system platform.

In its January 26, 2005, formal response to the OIG audit report, however, the FBI stated that the VCF and the 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."

The FBI also stated in its response that it is continuing to pursue the VCF through development of an implementation plan. The FBI hired the Aerospace Corporation to evaluate currently available software products to determine if they meet the FBI's requirements for a case management system. 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.

Yet, the timetable for the FICMS and the VCF still does not appear to be rapid or clear. In conjunction with the OIG's audit, the FBI told the OIG that it hopes to award a contract for FICMS by April 30, 2005. But the FBI has not provided its estimated costs, a revised schedule for completing the VCF, or a schedule for developing a new case management system to replace the VCF through the FICMS effort.

V. CAUSES OF TRILOGY'S PROBLEMS

We believe the responsibility for ensuring the success of the Trilogy project is shared by several parties: the FBI; the Department of Justice; FEDSIM – the component of GSA that awarded Trilogy contracts on behalf of the FBI; and the two contractors – CSC for the two infrastructure components, and SAIC for the user applications component that became the VCF. These entities, to varying degrees, did not appropriately contract for, manage, monitor, or implement the Trilogy project.

In our view, the main responsibility for the problems with Trilogy rests with the FBI. The FBI acted on a legitimate and urgent need to upgrade its IT infrastructure and replace the antiquated ACS. However, in the FBI's desire to move quickly on the Trilogy project, it engaged FEDSIM to handle the contracting for this very large and complex project without providing or insisting upon:

- defined requirements,
- specific milestones,
- critical decision review points, and
- penalties for poor contractor performance.

The resulting cost-plus-award-fee contract yielded control to the contactors for developing Trilogy's technical requirements, while leaving the FBI little leverage to direct the project. In essence, the contract terms required paying the contractors regardless of whether they met schedules or were even technically capable of completing such a challenging project.

In addition, the FBI failed to adequately develop and articulate the design requirements at the outset of the project, and consequently the requirements repeatedly changed as the project progressed, with too much contractor control and too little input from FBI management.

In its response to the audit report, the FBI alluded to its lack of control over requirements as a reason for the current VCF problem by stating that "[T]he VCF project suffered in part from runaway scope." The FBI response also stated that to guard against runway scope in the future, "the IT system will be designed, developed, and deployed incrementally against specified and planned parameters."

In addition to the poor choice of contracting method and sketchy requirements, neither the FBI, the Department, nor FEDSIM ensured that adequate schedule, cost, technical, and performance baselines were established to allow the project to be adequately monitored and to identify and rectify schedule slippages or technical problems. Since none of the responsible parties ensured that realistic milestones were established to complete various segments of the project, it was difficult to ensure that the contractors successfully met overall schedule, cost, technical, or performance targets for the project.

In addition, the Department expected the FBI to assume the role of project integrator to ensure all three Trilogy components meshed properly and were on track, even though the FBI lacked this capability or experience. The FBI's ability to manage the Trilogy project, even with the help of contractor personnel, was crippled further by a revolving door of Chief Information Officers (CIOs) and Trilogy project management personnel at the FBI.

A variety of audits by the OIG and the Government Accountability Office, as well as internal FBI reviews, had identified deficiencies in the FBI's management of IT projects, including Trilogy. However, the FBI's corrective action was slow. Only recently has the FBI made substantial progress in its IT investment management processes.

More specifically, in our audit report the OIG detailed the following eight causes for the FBI's problems with the Trilogy project:

1. Poorly defined and slowly evolving design requirements: One of the most significant problems with managing the schedule, cost, technical, and performance 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 still evolving as the project progressed. 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 the 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 schedule and cost were not established. In addition, 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.

2. Contracting weaknesses: The FBI's current and former CIOs told the OIG that a primary reason for the schedule and cost problems associated 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.

3. IT investment management weaknesses: As described in the OIG's December 2002 audit report, *The Federal Bureau of Investigation's Management of Information Technology Investments*, at Trilogy's inception and over much of its life, the FBI's IT Investment Management process was not well-developed. Although our recent audit found that while the FBI had started centralizing its project management structure, appropriate project management was not consistently followed by Trilogy's IT project managers. In essence, the FBI took risks to expedite Trilogy's implementation, and that approach failed because the management practices to oversee Trilogy simply were not in place.

4. 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. The development, maintenance, and implementation of Enterprise Architectures are recognized hallmarks of successful public and private organizations. While the FBI has agreed to develop a comprehensive Enterprise Architecture, this recommendation has not yet been fully implemented. The FBI has contracted for an Enterprise Architecture to be completed by September 2005. Without a complete Enterprise Architecture, the FBI needed to conduct reverse engineering to identify existing IT capabilities before developing the infrastructure and user applications requirements for the Trilogy project.

5. Lack of management continuity and oversight: Turnover in key positions hurt 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 suffered from a lack of engineering expertise, process weaknesses, and decision making by committees instead of knowledgeable individuals.

6. 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. The unrealistic scheduling of project tasks led to a series of raised expectations

followed by frustrations when the completion estimates were missed. According to an FBI official who monitored the development of the Trilogy infrastructure, Computer Sciences Corporation had problems producing an appropriate work schedule given the resources provided for the project. 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 in early 2003 to establish a realistic work schedule for completing the infrastructure components.

7. Lack of adequate project integration: Despite the use of two contractors to provide the three major Trilogy project components, the FBI did not retain 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.

8. Inadequate resolution of issues raised in reports on Trilogy: Within a matter of months after initiation of the Trilogy project, the FBI recognized significant issues that needed resolution. Internal reports issued by the FBI's Inspection Division, Criminal Justice Information Services Division, and consultants identified a lack of a single project manager, undocumented requirements, and a baseline that was not frozen. Based on internal reports, the FBI was aware of the risks that it faced during the development of 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 still continues, more than three years after these internal reports were issued. Because the FBI did not act timely to resolve the findings of these reports, many problems involving project management weaknesses, poorly-defined requirements, and lack of firm targets unnecessarily continued throughout much of the Trilogy project's history.

I believe it is important to note that, despite the troubled history of the Trilogy project, the FBI recently has made some improvements in its management of information technology. One major improvement in the FBI's IT management was the appointment of a new CIO in May 2004 and the consolidation of the FBI's previously fragmented management of IT resources and responsibilities under the Office of the CIO. A significant problem in the

FBI's management of IT investments was that all of the FBI divisions with IT investments were not under a single authority and, as a result, had a variety of processes and procedures for developing new systems. Under the reorganization, the CIO is responsible for all of the FBI's IT assets, projects, plans, processes, and budgets.

In December 2004, the Office of the CIO completed an initial version of an IT Strategic Plan, which describes how IT will support the FBI's Strategic Plan and mission goals for the next five years. All IT projects now are required to be consistent with the FBI's Strategic Plan.

The Office of the CIO also has 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 FBI Program and Project Managers and, if fully and effectively implemented, will help prevent the delays and problems that occurred during the Trilogy project.

As noted above, the FBI also is in the process of creating an Enterprise Architecture by September 2005. The Enterprise Architecture will provide a blueprint to aid the FBI in coordinating and managing its current and future IT infrastructure and systems. The FBI also is working on an IT Portfolio Management Program to list and technically document all of its IT systems. The FBI anticipates that recommendations stemming from its completed IT portfolio will be included in the development of its fiscal year 2007 IT budget.

In commenting on the OIG's Trilogy audit report, the FBI cited a number of other improvements it has begun to make, such as an IT metrics program to identify and measure IT performance, an initiative to standardize and automate IT procurement actions, a Program Management Professional certification training program, a Master IT Policy List to coordinate and control IT policies, standardized technology assessments, and an Information Assurance Program. Further, the FBI told us that VCF track one, or Initial Operating Capability, used the FBI's new IT management approach, including identifying project objectives, requirements, and constraints before proceeding to control gates designed to keep the project on track and to regulate the release of funds. Also, the FBI said it developed a cost-sharing arrangement as part of the renegotiated UAC contract. These initiatives were beyond the scope of our audit, and we could not examine the FBI's claims on these systems. However, they appear to represent progress in the FBI's IT system. But none of them diminish the urgent need for the FBI to fully implement a fully functioning case management system like the VCF to create, organize, share, and analyze case information.

VI. OIG CONCLUSIONS REGARDING TRILOGY PROJECT

In sum, the FBI has made progress with its management of IT and its implementation of the first two phases of Trilogy. Trilogy's infrastructure improvements have been completed, including the delivery of thousands of modern computer workstations and other hardware throughout the FBI. Although the Trilogy infrastructure improvements were characterized by delays and increased costs, the infrastructure now is in place to support improved user applications, including the VCF or its successor case management system, which the FBI recognizes as its top IT priority.

Yet, the VCF effort is incomplete, and the prospects for timely completion remain unclear. After more than 3 years, multiple missed deadlines, and a price tag of $170 million, the FBI still does not have an investigative case management system to replace the antiquated ACS system. Further, we are not confident that the FBI has a firm sense of how much longer and how much more it will cost to develop and deploy a usable system, whether the FBI continues to pursue the VCF system or decides to implement a new case management system.

Finally, we disagree with the FBI's assertion in its response to our draft report that the delays in deploying the VCF and the lack of an adequate case management system do not have national security implications. To the contrary, we believe there is a critical need to replace the ACS to enable FBI agents and analysts to effectively perform the FBI's mission. The archaic ACS system – which some agents have avoided using – is cumbersome, inefficient, and limited in its capabilities, and does not manage, link, research, analyze, and share information as effectively or timely as needed. While the FBI has made strides in other IT areas – including installing a number of systems to share intelligence information and upload numerous documents into a data warehouse – the continued delays in developing the VCF affects the FBI's ability to carry out its critical missions.

VII. ADDITIONAL OIG REVIEWS IN THE FBI

To conclude this statement, in response to a request from the Subcommittee, I summarize briefly the OIG's ongoing reviews of other priority issues in the FBI. The following are examples of ongoing and recently completed OIG reviews that may be of interest to the Subcommittee.

A. Ongoing OIG Reviews in the FBI

- **Terrorist Screening Center.** The OIG is examining the operations of the Terrorist Screening Center to determine how it has managed terrorist-related information to ensure that complete, accurate, and current watch lists are developed and maintained.

- **Implementation of the Attorney General's Guidelines.** The OIG is reviewing the FBI's compliance with the revised Attorney General Guidelines that govern the use of confidential informants; undercover operations; investigations of general crimes, racketeering enterprises, and terrorism enterprises; and warrantless monitoring of verbal communications.

- **Intelligence Analysts.** The OIG is reviewing the FBI's recruitment, selection, training, and staffing of intelligence analysts.

- **FBI's Handling of the Brandon Mayfield Matter.** The OIG is reviewing the FBI's conduct in connection with the erroneous identification of a fingerprint found on evidence from the March 2004 Madrid train bombing as belonging to Brandon Mayfield, an attorney in Portland, Oregon.

- **Alleged Mistreatment of Detainees at Military Detention Facilities:** The OIG is examining any involvement of FBI employees in either observing or participating in the alleged abuse of detainees at the military's Guantanamo Bay and Abu Ghraib facilities. In addition, the OIG is reviewing when FBI employees reported the allegations of abuse and how FBI managers handled the employees' reports.

- **The FBI's Chinese Counterintelligence Program.** At the request of the FBI Director, the OIG is examining the FBI's performance in connection with the handling of Katrina Leung, an asset in the FBI's Chinese counterintelligence program.

- **The Department's Counterterrorism Task Forces.** The OIG is evaluating the Department's counterterrorism task forces to: 1) determine if they are achieving their stated purposes; 2) evaluate gaps, duplication, and overlap in terrorism coverage; and 3) identify how the performance of each task force is measured.

- **Implementation of the Communications Assistance for Law Enforcement Act (CALEA).** The OIG is conducting a follow-up audit of the implementation of CALEA, which allows reimbursement to communications carriers for modifications of equipment to allow the capability for lawful electronic surveillance. The FBI has expended more than $500 million under CALEA. The OIG's objectives are to review the progress and impediments to the FBI's implementation of CALEA; review CALEA's costs; and determine how the implementation of CALEA has impacted federal, state, and local law enforcement in their ability to conduct electronic surveillance.

- **FBI's Reprioritization Efforts.** The OIG is reviewing how the FBI's operational changes resulting from its reorganization and change in priorities after the September 11 attacks have affected other law enforcement agencies.

B. Recently Completed OIG Reviews in the FBI

The following are some examples of recently completed OIG reviews related to FBI operations:

- **Follow-up Review of the Status of IDENT/IAFIS Integration (December 2004).** This OIG review examined ongoing efforts to integrate the federal government's law enforcement and immigration agencies' automated fingerprint identification databases. Fully integrating the automated fingerprint systems operated by the FBI and the DHS, known as IAFIS and IDENT respectively, would allow law enforcement and immigration officers to more easily identify known criminals and known or suspected terrorists trying to enter the United States, as well as identify those already in the United States that they encounter. This latest OIG report is the fourth in four years that monitors the progress of efforts to integrate IAFIS and IDENT.

  This OIG report found that while deployment of new IDENT/IAFIS workstations to Border Patrol offices and ports of entry represents a significant accomplishment, full integration of IDENT and IAFIS has yet to be realized. Federal, state, and local law enforcement authorities still do not have complete access to information in the IDENT database. Without such access, the FBI and DHS fingerprint systems are not fully interoperable, and it is more difficult for federal, state, and local law enforcement agencies to identify illegal aliens they encounter.

  This OIG report found that the congressional directive to fully integrate the federal government's various fingerprint identification systems has not been accomplished because of high-level policy disagreements among the Departments of Justice, Homeland Security, and State regarding such integration. In addition, the Department and the DHS still have not entered into a memorandum of understanding (MOU) to guide the integration of IAFIS and IDENT. This MOU has not been completed because of fundamental disagreements between the Department and the DHS over the attributes of an interoperable fingerprint system and the number of fingerprints to be taken from individuals by each agency.

- **Effects of the FBI's Reprioritization (September 2004).** The OIG reviewed the changes in the FBI's allocation of its personnel resources since the September 11 terrorist attacks. The report provided detailed statistical information regarding changes in the FBI's allocation of resources since 2000. The OIG determined that the FBI has reallocated resources in accord with its shift in priorities from traditional criminal investigative work to counterterrorism and counterintelligence matters. In addition, the OIG review identified specific field offices most affected by changes in FBI priorities within various investigative areas, such as shifting agent resources from organized crime or health care fraud cases to terrorism investigations. The OIG report recommended that the FBI regularly conduct similar detailed analyses of its agent usage and case openings to provide a data-based view of the status of FBI operations and to assist managers in evaluating the FBI's progress in meeting its goals.

- **Handling of Information Prior to September 11 Terrorist Attacks (July 2004).** This classified OIG report, conducted at the request of the FBI Director, examined the FBI's handling of intelligence information prior to the September 11 terrorist attacks. The review focused on the FBI's handling of an electronic communication written by its Phoenix Division in July 2001 regarding extremists attending civil aviation schools in Arizona, the Zacarias Moussaoui investigation, and information related to September 11 terrorists Nawaf al-Hazmi and Khalid al-Mihdhar.

  The OIG made 16 recommendations for improving the FBI's intelligence handling and counterterrorism efforts, including recommendations targeted towards the FBI's analytical program. The OIG provided the classified version of this report to the 9/11 Commission and to Congress. In response to requests from members of Congress, the OIG is working with the Department to produce an unclassified version of this report that can be publicly released.

- **Foreign Language Translation Program (July 2004).** The OIG audited the FBI's translation of counterterrorism and counterintelligence foreign language materials. The audit found that the FBI did not translate all the counterterrorism and counterintelligence material it collected. The OIG attributed the FBI's backlog of unreviewed material to difficulties in hiring a sufficient number of linguists and limitations in the FBI's translation information technology systems. The review also found problems in the FBI's quality control program for language translations. The report made 18 recommendations for improving the FBI's foreign language translation program.

In response to the OIG report, the FBI stated that it plans to implement a national integrated statistical collection and reporting system for its translation program in FY 2005 that will allow foreign language program management to accurately determine the amount of unreviewed material that needs to be translated. The FBI also plans to increase its digital collection systems' storage capacity so that unreviewed audio material for critical cases is not deleted by the system. In addition, it plans to implement controls to ensure that the forwarding of audio among FBI offices via its secure communications network is accomplished reliably and timely. The FBI further reported that it plans to assess the linguist hiring process, implement measures to reduce the time it takes to bring linguists on board, and strengthen quality control procedures to ensure that translations are accurate and that all pertinent material is being translated.

- **Edmonds Case (June 2004).** The OIG examined the FBI's actions in connection with allegations raised by former FBI contract linguist Sibel Edmonds. Edmonds alleged that her concerns about aspects of the FBI translation program were not appropriately handled by the FBI and that her services as a contract linguist were terminated in retaliation for her raising these allegations. The OIG review concluded that many of Edmonds' core allegations relating to the co-worker had some basis in fact and were supported by either documentary evidence or witnesses other than Edmonds. The OIG concluded that the FBI should have investigated Edmonds' allegations more thoroughly. With respect to Edmonds' claim that she was fired for raising these concerns, the OIG concluded that while Edmonds does not fall within the protection of the FBI's whistleblower regulations, Edmonds' allegations were at least a contributing factor in why the FBI terminated her services.

- **DNA Reviews.** During the past year, the OIG completed three reviews examining various aspects of DNA laboratories or DNA grant programs. In the first review, completed in May 2004, the OIG examined vulnerabilities in the protocols and practices in the FBI's DNA Laboratory. This review was initiated after it was discovered that an examiner in DNA Analysis Unit I failed to perform negative contamination tests. The OIG's review found that certain DNA protocols were vulnerable to undetected, inadvertent, or willful non-compliance by DNA staff, and we made 35 recommendations to address these vulnerabilities. The FBI agreed to amend its protocols to address these recommendations.

In a separate review, the OIG audited several laboratories that participate in the FBI's Combined DNA Index System (CODIS), a national database maintained by the FBI that allows law enforcement agencies to search and exchange DNA information. The OIG's CODIS audits identified concerns with some participants' compliance with quality assurance standards and uploading of unallowable and inaccurate DNA profiles to the national level of CODIS.

In a third review dealing with DNA matters, issued in November 2004, the OIG audited the Office of Justice Programs' DNA backlog reduction grant program. This program provides funding to states for the analysis of DNA samples collected in cases where no suspect has been identified. The audit found that many of the DNA profiles that had been analyzed by the states using grant funding had not been uploaded into the FBI's CODIS system and that grantees were not using the funds on a timely basis to reduce DNA backlogs.