United States Department of Justice
Office of the Inspector General
Audit Division

AUDIT REPORT

FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF INFORMATION TECHNOLOGY INVESTMENTS

DECEMBER 2002

03-09

FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF INFORMATION TECHNOLOGY INVESTMENTS

EXECUTIVE SUMMARY

Following the September 11, 2001, terrorist attacks, the Attorney General and the Director of the Federal Bureau of Investigation (FBI) made clear that prevention of terrorism is the top priority of the Department of Justice (DOJ) and the FBI. Effective use of information technology (IT) is crucial to the FBI's ability to meet this priority as well as its other critical responsibilities.

However, reviews conducted by the Office of the Inspector General (OIG) and the General Accounting Office (GAO) have found major weaknesses associated with the FBI's IT. The FBI has listed upgrading its information technology as one of its top ten highest priorities. In June 2002 Congressional testimony, the FBI acknowledged that its IT infrastructure is severely outdated.

Because of the importance of the FBI's management of its IT systems, we performed this audit to: (1) determine whether the FBI was effectively managing its IT investments; and (2) assess the FBI's IT-related strategic planning and performance measurement activities.[1] We also examined the FBI's efforts to develop enterprise architecture[2] and project management capabilities.

In this audit, we conducted approximately 85 interviews with 70 officials from the FBI, DOJ, GAO, and the Office of Management and Budget (OMB). The FBI officials interviewed were from the Director's office, Information Resources Division, Criminal Justice Information Services Division, Laboratory Division, Inspection Division, and Finance

[1] During our audit fieldwork, we initiated work relating to a third objective: to determine if the FBI has implemented prior information technology related recommendations directed toward improving information technology. We will issue a separate report on this objective.

[2] Enterprise architecture is the organization-wide blueprint that defines an entity's functions and systems, including IT systems. It provides a comprehensive view (through models, narratives, and diagrams) of the interrelationships of an organization's operations and structures and how these structures align with the organization's mission. The Clinger-Cohen Act of 1996 recognizes the interrelationship between enterprise architecture and IT investment management by requiring federal agencies to develop an enterprise architecture.

Division. Additionally, OIG auditors and analysts traveled to FBI laboratory facilities in Quantico, VA, and five FBI field offices to conduct interviews and assess the FBI's implementation of IT initiatives. We also reviewed more than 200 documents, including the FBI's IT management policies and procedures, project management guidance, strategic and program plans, IT project proposals and management plans, budget documentation, organizational structures, Congressional testimony, and prior OIG and GAO reports.

1. Summary of Audit Findings

We concluded that the FBI has not effectively managed its IT investments because it has not fully implemented the management processes associated with successful IT investments. The foundation for sound IT investment management (ITIM) includes the following fundamental elements:

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

The FBI failed to implement these critical processes. We found that the FBI does not have fully functioning IT investment boards that are engaged in all phases of IT investment management. The FBI was not following a disciplined process of tracking and overseeing each project's cost and schedule milestones. The FBI failed to document a complete inventory of existing IT systems and projects, and did not consistently identify the business needs for each IT project. The FBI did not have a fully established process for selecting new IT project proposals that considered both existing IT projects and new projects.

Because the FBI has not fully implemented the critical processes associated with effective IT investment management, the FBI continues to spend hundreds of millions of dollars on IT projects without adequate assurance that these projects will meet their intended goals.

We concluded that these shortcomings primarily resulted from the FBI not devoting sufficient management attention in the past to IT investment management.

However, FBI management has recognized that its past methods to manage IT projects have been deficient, and the FBI recently has committed to changing those practices. In January 2002, the FBI developed a conceptual model for selecting, controlling, and evaluating IT investments. The model seeks to define a process that will promote a Bureau-wide perspective on IT investment management, so that only IT projects with the best probability of improving mission performance are selected. Further, the process is intended to provide the methods, structures, disciplines, and management framework that governs the way IT projects are controlled and evaluated.

In addition to developing a conceptual model for a new ITIM process, in early 2002 the FBI began a pilot test of the new process for the selection of IT proposals. We found that the FBI made improvements during the pilot testing of the new selection process. Pursuant to the new process, the FBI created three IT investment review boards that reviewed IT proposals for technical compliance and "mission fit." These boards, comprised of the FBI Director, FBI executives and IT managers, selected new IT proposals that will be considered for inclusion in the Fiscal Year (FY) 2004 budget request.

While the FBI has made efforts to improve its IT investment management practices, the FBI must take further actions to ensure that it can implement the fundamental processes necessary to build an IT investment foundation, as well as the more mature processes associated with highly effective IT investment management. These actions include:

- fully developing and documenting its new IT investment management process – which is necessary to completely implement the activities defined in the FBI's conceptual model;

- requiring increased participation from IT program managers and users – which is necessary to ensure senior management acceptance and foster understanding and institutionalization of the ITIM process; and

- further developing the FBI's project management and enterprise architecture functions – which is necessary to execute the

control and evaluate components of the ITIM process as well as advance its investment management capability.

Our audit also reviewed the FBI's management of Trilogy, the FBI's largest and most critical IT project. We found that the lack of critical IT investment management processes contributed to missed milestones and led to uncertainties about cost, schedule, and technical goals. Specifically, despite $78 million in additional funding, the FBI missed its July 2002 milestone date for completing the physical IT infrastructure upgrades to field offices, including new computer hardware and networks.[3] FBI officials stated that they are not expecting the physical infrastructure components of Trilogy to be completed until March 2003. In addition, the user application component of Trilogy, recognized by FBI officials as the most important aspect of the project in terms of improving agent performance, is at high risk of not being completed within the funding levels appropriated by Congress. In our judgment, the management problems associated with Trilogy demonstrate the FBI's urgent need for enhanced IT investment management.

We also concluded that the FBI's IT strategic planning and IT performance measurement are inadequate. We found that the FBI's strategic plan does not include goals for IT investment management, and the FBI's strategic plan and performance plan are not consistent with the DOJ's annual performance plan.

The remainder of this executive summary provides more background and details on our audit findings and recommendations to help improve the FBI's management of its IT investments.

2. Background

The Clinger-Cohen Act of 1996 requires each federal agency to implement a process for maximizing the value of its IT investments. This process is intended to ensure that IT projects are being implemented at acceptable costs and within reasonable time frames, and that the projects are contributing to enhanced mission performance. Specifically, the Clinger-Cohen Act requires federal agencies to: (1) develop an enterprise architecture framework, and

[3] With the $78 million in additional funding, Trilogy's total appropriation was $458 million as of June 2002.

(2) follow a "select/control/evaluate" approach to managing IT investments.

In May 2000, the GAO developed the IT Investment Management Framework (Framework) to provide a common methodology for assessing IT capital planning and investment management practices at federal agencies. The Framework specifically describes the organizational processes required to carry out sound IT investment management.

The Framework, based on best practices of leading organizations, is a hierarchical model comprised of five maturity stages. These maturity stages represent steps toward achieving stable and mature investment management processes. As agencies advance through these stages, their capability to effectively manage IT increases. With the exception of the first stage, each maturity stage is comprised of critical processes that must be implemented and institutionalized for the agency to satisfy the requirements of that stage. These critical processes are further broken down into key practices an agency should perform to successfully implement each critical process.

An agency using these critical processes is in a better position to successfully invest in IT and use its IT investments to achieve its priorities. Conversely, an agency that does not have these critical processes in place is at high risk that its IT projects will fail to support the achievement of priorities.

To determine whether the FBI was effectively managing its IT investments, we utilized the Framework because it is: (1) a standardized tool for internal and external evaluations of an agency's IT investment management process; (2) a consistent and understandable mechanism for reporting the results of these assessments; and (3) a road map agencies can use for improving their IT investment management process.

In addition, the Government Performance and Results Act of 1993 (Results Act) requires strategic planning and performance measurement throughout the federal government. The Results Act seeks to improve the effectiveness, efficiency, and accountability of federal programs by requiring federal agencies to establish goals for program performance and measurement. The Results Act requires agencies to prepare a strategic plan, annual performance plan, and annual performance report.

While IT strategic planning is a function somewhat independent of IT investment management, these two functions are interrelated and complementary. The DOJ has recognized the importance of integrating strategic planning with IT management. In July 2002, the DOJ released its IT Strategic Plan that included a strategic initiative to establish and improve investment management processes.

3. The FBI's Management of IT Investments

Our audit found that the FBI has not established an IT investment foundation and therefore is in Stage One maturity according to the ITIM Framework. Stage One maturity is characterized by inconsistent, unstructured, and unpredictable investment processes. Our observations of the FBI's IT investment processes found that the FBI's actual processes are consistent with these Stage One deficiencies.

The critical processes necessary to establish an IT investment foundation include: (1) defining investment review board operations, (2) developing project-level investment control processes, (3) identifying IT projects and systems, (4) identifying the business needs for each IT project, and (5) developing a basic process for selecting new IT proposals.

We found that the FBI failed to implement these critical processes. The FBI did not have a fully established investment review board operation because the FBI did not provide adequate resources for operating the IT investment boards. Additionally, we found insufficient evidence to demonstrate that: (1) organization executives and line managers supported and carried out IT investment board decisions and (2) board members understood the investment board's policies and procedures and exhibited core competencies in using the IT investment approach via training, education, or experience. Specifically, the FBI did not provide ample time to adequately prepare and train IT board members prior to initiating the pilot test of its recently developed ITIM process. This resulted in inadequate training of board members and minimal preparation time to develop IT proposals. For example, Technical Review Board members had only three business days to review over 50 IT proposals prior to their first board meeting.

Additionally, we found that the FBI is not effectively overseeing its IT projects. For example, while the FBI has issued project management guidance, the guidance is not being followed on a

consistent basis. Depending on whom we talked to, we obtained different answers as to which document represented the FBI's official project management guidance.

Without effective oversight of IT projects, FBI officials do not have adequate assurance that IT projects are being developed on schedule and within established budgets. According to a former Chief Information Officer at the FBI, the lack of effective oversight of IT projects has prevented IT project managers from being held accountable for cost and schedule overruns and the ultimate performance of projects. Senior FBI officials also told us that the Bureau's budget formulation process focuses only on the acquisition costs for IT projects and not the full life-cycle costs, especially operations and maintenance costs.

We also found that the FBI's investment review boards are not aware of all the IT projects and resources for which the boards are responsible. FBI Divisions maintained some version of an IT inventory for the projects and systems under their jurisdiction, and there was no centralized office responsible for maintaining a uniform listing Bureau-wide. FBI managers told us they were in the process of developing an IT asset inventory, but at the time of our audit they were unable to provide an estimated date for completing the inventory.

FBI personnel told us that staff shortages are the primary cause for the incomplete IT asset inventory. In our judgment, staff shortages may be a contributing factor, but the lack of centralized management over IT investments was the significant reason for this problem. Until June 2002, the FBI did not have a centralized project management office to assist the investment boards in overseeing IT projects. The FBI maintained three separate division-level project management offices to manage IT projects.

We also determined that the FBI did not have a fully established process for selecting IT proposals. FBI officials told us that, prior to March 2002, individual divisions determined IT needs in a "stovepipe," without knowledge of the business needs and priorities of the Bureau as a whole. The FBI did not have a clearly designated official to manage the proposal selection process. According to Information Resources Management Section personnel, the Finance Division managed the IT selection process. However, according to Finance Division personnel, the Information Resources Management office was responsible for managing the proposal selection process.

Without a comprehensive proposal selection process that includes adequate resources and training, the FBI cannot ensure that it is selecting the best IT projects that meet mission-critical needs.

Because the FBI did not fully implement any of the critical processes associated with Stage Two, the FBI continues to spend hundreds of millions of dollars on IT projects without having adequate selection and project management controls in place to ensure that IT projects will deliver their intended benefits.

The FBI began pilot testing the select phase of its new ITIM process in March 2002, and since then has made measurable progress towards implementing the key practices that comprise the critical processes – particularly in the area of selecting new proposals for IT projects. Specifically, at the beginning of our audit in January 2002, the FBI only was executing 4 of the 38 required key practices; however, as of June 2002, the FBI was executing 14 of the key practices.

With the pilot testing of its new ITIM process, the FBI created an IT investment process guide containing policies and procedures to direct board operations, and created and defined three investment review boards integrating both IT and business knowledge. Additionally, the FBI has designated an official responsible for managing the IT project and system identification process and ensuring that the inventory meets the needs of the investment management process. Further, during the test pilot of the ITIM process, the board reviews of IT project proposals provided assurance that business needs were clearly identified and defined. Also during the test pilot, we determined that FBI IT investment board members analyzed and prioritized new IT proposals according to established selection criteria for the FY 2004 budget cycle.

Despite the progress made, full implementation of the ITIM process will require the FBI to (1) fully develop and document its new ITIM process; (2) require more input and participation from IT managers and users; and (3) further develop its project management and enterprise architecture functions. Completion of the initial steps taken by the FBI will ensure that IT projects are developed within cost and schedule requirements, and meet performance expectations. The Trilogy project provides an example of how the non-implementation of fundamental IT investment management practices can put a project at risk of not delivering what was promised, within cost and schedule requirements.

4. Trilogy

We also performed a case study of the FBI's implementation of its Trilogy project. We selected Trilogy because it is the FBI's largest ongoing IT project and is considered vital to the FBI's ability to perform its mission. Trilogy is intended to upgrade the FBI's: (1) hardware and software – referred to as the Information Presentation Component (IPC), (2) communication networks – referred to as the Transportation Network Component (TNC), and (3) five most important investigative applications – referred to as the User Applications Component (UAC). The IPC and TNC upgrades will provide the physical infrastructure needed to run the applications from the UAC portion. The UAC portion is intended to upgrade and consolidate five of the FBI's 42 investigative applications. Because of the 37 other investigative applications and approximately 160 non-investigative applications that Trilogy will not cover, Trilogy is only a starting point towards upgrading the FBI's entire IT infrastructure. According to the FBI, Trilogy is not designed to provide the FBI with state-of-the-art IT; it is intended to provide the foundation so that the FBI can eventually attain state-of-the-art IT.

In November 2000, Congress appropriated $100.7 million for the first year of the $379.8 million Trilogy project, which was to be funded over a three-year period (from the date contractors were hired). The $100.7 million was a combination of new program funding and a re-direction of base resources. When the FBI requested contractor support for Trilogy, it combined the IPC and TNC portions for continuity as both encompass physical IT infrastructure enhancements. The contractor for the IPC/TNC portions was hired in May 2001, and the originally scheduled completion date for these components was May 2004. A different contractor was hired in June 2001 to complete the UAC portion of Trilogy by June 2004.

After the terrorist attacks on September 11, 2001, the urgency of completing Trilogy increased, and the FBI explored options to accelerate the deployment of all three components of Trilogy. The FBI informed Congress in February 2002 that, with an additional $70 million, the FBI could accelerate the deployment of Trilogy. This acceleration would include completion of the IPC/TNC phase by July 2002 and rapid deployment of the most critical analytical tools included as part of the UAC phase.

In January 2002, Congress supplemented Trilogy's FY 2002 budget with $78 million[4] to expedite the deployment of all three components. This supplemental appropriation increased the total funding of Trilogy from approximately $380 million to $458 million.

Even with these additional funds, the FBI missed its July 2002 milestone date for completing the IPC and TNC phases. FBI officials stated that they are not expecting these components of Trilogy to be completed until March 2003. In addition, the user application component of Trilogy, recognized by FBI officials as the most important aspect of the project in terms of improving agent performance, is at high risk of not being completed within the funding levels appropriated by Congress. Further, despite receiving an additional $78 million from Congress in January 2002, FBI managers have acknowledged to us that the last phase of UAC will not be completed any sooner than originally planned (in June 2004).

In terms of a cost baseline, FBI officials told us that the rapid procurement and deployment of Trilogy has prevented the project managers from performing earned value management,[5] as promised to Congress. While FBI officials were confident they know how much money has been spent on Trilogy to date, and how much funding has been committed, they have less assurance as to whether Trilogy is on budget, over budget, or under budget.

A schedule baseline for Trilogy has never been well-established. First, FBI officials said they would complete IPC/TNC deployment in May 2004. Then, they said it could be finished in June 2003. Next, they said it would be finished by December 2002. After receiving $78 million of supplemental funding, they said it would be done by July 2002. Then, they said they could not make the July 2002 deadline and moved it to October 2002. As of June 2002, FBI officials have said deployment will probably not be complete until March 2003. Also as of June 2002, the FBI was still in the process of building a comprehensive schedule of Trilogy milestones.

Regarding the technical requirements for Trilogy, we were told that some aspects of Trilogy as submitted to Congress did not turn out to be technically feasible. For example, FBI officials told us that the

[4] The $78 million is comprised of the $70 million that FBI requested for acceleration, plus $8 million for contractor support.

[5] Earned value management is a project monitoring method that compares the value of products and services received with funds that have been expended.

thin-client strategy was not pursued because it was found that this type of network could not be achieved given the technical requirements of the FBI.[6] Another example is web-enablement of the Automated Case Support (ACS) system, which was also discontinued when it was realized that it would require more resources than anticipated.[7] Had a more rigorous proposal selection process been in place to require sufficient documentation of the technical requirements and risks of the project, the expending of time and resources on thin-client technology and web-enablement of ACS may have been minimized.

Another technical issue involves the development of the UAC portion of Trilogy. Because the UAC portion is focused on making significant changes to, or possibly complete replacements of, five of the FBI's investigative systems, documentation for the exact configuration of these systems is critical to designing the requirements for UAC. According to a senior FBI official, the FBI must know what it has before it can define the right solution to fix the problem. Lack of documentation for the configuration of these five investigative systems has caused the FBI to engage in a process of reverse engineering, which is trying to determine the structure and components of the systems after deployment. Because the FBI has to perform reverse engineering on the FBI's five investigative systems, there are limitations as to how rapidly UAC can be developed and deployed.

Our observations at five FBI field offices indicated that deployment of the IT physical infrastructure was still ongoing as of June 2002. For two field offices, additional installation work remained to be completed, and for four field offices hundreds of desktop computers still remained to be delivered. A lack of clear communication between FBI Headquarters and the field offices contributed to the confusion over the number of desktop computers to be delivered and shortages of fiber optic cable. Additionally contractor maintenance support for the Trilogy architecture was inefficient, resulting in agents being without computers for weeks at a time. Improvements in agent and support personnel training, procurement of trouble-shooting equipment for the Trilogy architecture, and timely

[6] According to the FBI, a thin-client strategy would utilize application software that is run from the server computer, and consequently permit desktop computers to function with few hardware resources such as processors and memory.

[7] Web-enablement refers to the ability of the software application to interface with the Internet through a browser, thereby extending information access.

completion of FBI unique macros for Microsoft Word will enhance user utilization of the Trilogy architecture.

The new Trilogy project executive, hired in March 2002, has taken a different approach to managing Trilogy. She has emphasized the importance of having more structured oversight of the project. She has been developing a comprehensive schedule for all three components. Additionally, she has indicated that there are limitations to how fast Trilogy can be deployed, without risking the security of the system. In our judgment, while these actions taken since March 2002 represent positive changes to Trilogy's project management function, the project's completion time, final cost, and ultimate performance remain uncertain. Also, we concluded that for the Trilogy project management function to be effective, it must include oversight from IT investment review boards to provide much needed monitoring.

5. FBI's IT Strategic Planning and Performance Measurement

We also assessed the FBI's IT strategic planning and performance measurement. We found that the FBI's strategic plan does not include IT investment management goals and the FBI's strategic plan and performance plan are not consistent with the DOJ's annual performance plan. Also, as of the end of June 2002, the FBI did not have a current strategic plan dedicated to IT. Instead, individual FBI divisions had program plans that included the use of IT within particular programs.

This occurred because the FBI has not updated its strategic plan since 1998, and its performance plan does not include the same strategic objectives, goals, and strategies relating to IT as does the DOJ's annual performance plan. We believe that the FBI will have difficulty improving its IT investment management process without incorporating it into the strategic plan. Additionally, without adequate strategic planning and performance measurements, there is a heightened risk that the FBI may not be appropriately allocating resources to meet the DOJ's strategic priorities.

In our judgment, the FBI must change the division-specific IT focus and implement a Bureau-wide IT strategic plan. The purpose of the FBI's ITIM process is to move away from the decentralized IT focus to a centralized one. As a result, we recommend that the FBI update its IT strategic plan and performance plans to (1) fully integrate these plans with the FBI's ITIM process; and (2) include those performance goals and indicators defined in the DOJ's IT Strategic Plan.

6. OIG Recommendations

In this report, we make 30 recommendations that focus on specific and immediate steps the FBI should take to help improve its IT investment management. These recommendations include:

- Ensure that the FBI continues its efforts to establish a comprehensive enterprise architecture that is integrated with the ITIM process.

- Require the ITIM Program Office to plan for and allocate sufficient time for IT investment review board members and other ITIM users to execute assigned responsibilities competently.

- Ensure that members of IT investment boards and other ITIM users receive sufficient training to execute assigned responsibilities effectively.

- Ensure that official project management guidance is used for all FBI IT projects through management oversight from the IT investment review boards.

- Ensure that each IT project has a project management plan, approved by the IT investment review boards, that includes cost and schedule controls.

- Ensure that a complete IT asset inventory is developed, and information from the IT asset inventory is made available to, and used by, the IT investment review boards as necessary.

- Ensure that the FBI develops written policies and procedures for identifying the business needs (and the associated users) of each IT project.

- Ensure that identified users participate in project management throughout a project's life-cycle.

- Ensure that the policies and procedures of the ITIM process are expanded, documented, and made available to ITIM users.

- Ensure that the ITIM Program Office and the ITIM contractor incorporate the input from various ITIM users through

working group sessions as the ITIM process is being further developed and refined.

- Ensure that the FBI develops and implements a specific plan detailing how and when it will integrate the ITIM process with a system development life-cycle methodology.

7. Conclusion

The underlying practices we assessed are fundamental to any project management endeavor. However, the FBI has not executed the majority of these tasks to select and manage its IT resources. For example, organizational policies were not clearly established to ensure that critical IT investment policies endure. Additionally, there were no clearly defined, uniform procedures for project management, tracking project performance, and taking corrective actions as necessary. Prior to the development of its ITIM process in early 2002, the FBI did not give sufficient attention to IT investment management. Since the FBI developed its ITIM process in early 2002, it has focused more management attention in this area and has made progress towards attaining a basic IT investment management foundation. Despite the progress, the FBI did not fully implement any of the critical processes necessary to build an IT investment foundation. As a result, the FBI continues to spend hundreds of millions of dollars on IT projects without having adequate selection and project management controls in place to ensure that IT projects will deliver their intended benefits.

TABLE OF CONTENTS

INTRODUCTION

1. Background

The Federal Bureau of Investigation (FBI or Bureau) is the principal investigative arm of the Department of Justice (DOJ). To execute its responsibilities, the FBI's Headquarters in Washington, D.C. provides program direction and support services to 56 field offices, approximately 400 satellite offices known as resident agencies and more than 40 foreign liaison posts.

As of June 2002, the FBI had over 11,000 Special Agents and over 16,000 other employees who performed professional, administrative, technical, clerical, craft, trade, or maintenance operations. The FBI's budget authority increased 31 percent from $3.339 billion in FY 2001 to nearly $4.371 billion in FY 2002.[8] Of this budget authority, $714 million was allocated to information technology (IT) projects in FY 2002 compared to $353 million in FY 2001.

The terrorist attacks of September 11, 2001, prompted the Attorney General to make counterterrorism the DOJ's highest priority. The DOJ reflected these new priorities in its Strategic Plan for Fiscal Years 2001 – 2006, which was issued in November 2001. In the Strategic Plan, the Attorney General recognized that the fight against terrorism requires the DOJ "to improve the integrity and security of its computer systems and make more effective use of information technology."

In response to the DOJ's new priorities following September 11, 2001, the FBI proposed fundamental changes in its strategic priorities and business practices. In May 2002, the Director of the FBI announced a major reorganization that dedicates more resources to the prevention of terrorism.[9] Although the core missions of the FBI remain intact, the proposed changes would transform the Bureau's role from reactive to preventive. To accomplish this transition, FBI officials have repeatedly told Congress that new and improved IT is required to support a redesigned and refocused FBI. In testimony

[8] These figures were taken from the DOJ's website (www.usdoj.gov). They include a $745 million Counterterrorism Supplemental for FY 2002 and exclude Federal Retiree and Health Benefit Costs.

[9] This reorganization was approved by Congress on July 31, 2002.

before the Senate Judiciary Committee on June 6, 2002, the Director released the FBI's top ten priorities in the post-September 11 era, with the number one priority being protecting the United States from terrorist attacks. Number ten on the list of priorities is upgrading technology to successfully perform the FBI's mission. Clearly, the FBI's future ability to prevent terrorism and other crimes depends on modern information technology and effective management of technology.

2. The FBI's Management of IT Infrastructure

The FBI has three divisions that manage major IT projects: the Information Resources Division (IRD), the Criminal Justice Information Services Division (CJIS), and the Laboratory Division. As discussed below, the FBI is attempting to centralize the management of IT, rather than manage IT within divisions.

The IRD provides the day-to-day support services to manage the information systems of the FBI. The IRD's responsibilities include management of all hardware, software, and IT peripheral equipment located at the FBI's Headquarters, field offices, and other offsite locations.

The IRD has been restructured in recent years to increase the oversight and jurisdiction of the Chief Information Officer. Until November 2001, the Chief Information Officer of the FBI was the Assistant Director of IRD who reported to the Director. However, to give the Chief Information Officer greater authority over the entire FBI, the Chief Information Officer was moved out of IRD and into the Director's office, pursuant to a restructuring approved by Congress on November 30, 2001. Additionally, to support the Chief Information Officer, the Information Resources Management Section[10] was moved out of IRD and into the Chief Information Officer's office, following another restructuring in February 2002. Also, in February 2002, the IT Investment Management Program Office was formed (within the Information Resources Management Section) and was staffed with one individual whose responsibility was to manage the FBI's IT investment management program. Based on these actions, the FBI recognizes that centralizing the management of IT requires a Chief Information Officer to have Bureau-wide oversight and jurisdiction, rather than be isolated within a division.

[10] The Information Resources Management Section is responsible for managing IT investments and enterprise architecture.

The CJIS Division uses several significant IT systems to manage and disseminate relevant criminal justice information to the FBI and other law enforcement agencies. For example, the National Crime Information Center 2000 is a nationwide information system that supports federal, state, and local law enforcement agencies. Additionally, the CJIS Division is responsible for managing the Integrated Automated Fingerprint Identification System and the National Incident-Based Reporting System. To support the management of these systems, the CJIS Division maintains a Contract Administration Office, which provides quality assurance, configuration management, and project management support services necessary to manage these and other systems under its jurisdiction.

The Laboratory Division manages several forensic computer systems that provide forensic and technical services to law enforcement agencies. A significant system includes the Combined DNA Index System (CODIS), which provides software and support services to state and local laboratories to establish databases of criminals, unsolved crime scenes, and missing persons. A component of CODIS, the National DNA Index System, shares DNA profiles from convicted offenders and crime scenes to laboratories throughout the United States. To manage these systems, the Laboratory Division maintains its own project management office.

The FBI has recognized that its IT infrastructure was significantly outdated and did not effectively support user needs. Although recent upgrades have changed these numbers, as of September 2000, over 13,000 desktop computers were 4 to 8 years old and could not run basic software packages, some communication networks were up to 12 years old and were obsolete, and multiple user-applications existed that were neither web-enabled[11] nor user-friendly.[12] On June 6, 2002, the Director stated to the Senate Judiciary Committee:

> You've heard me talk about the necessity for upgrading our technology. And upgrading our technology means not just getting the computers on board, the hard drives. It means everybody from top to bottom becoming facile with the

[11] Web-enablement refers to the ability of the software application to interface with the Internet through a browser, thereby extending information access.

[12] According to FBI officials, the FBI acknowledged these needs to Congress in the late 1990s, in addition to the technology upgrade plan prepared in September 2000.

computer, understanding the computer and understanding how technology can assist us to do our jobs better. And that is somewhat of a transformation for an organization such as the FBI, which is years behind where it should be, in terms of having the technological infrastructure.

3. Prior Reports on the FBI's IT and DOJ Oversight of Components' IT

Reports issued by the Office of the Inspector General (OIG) over the past 12 years have highlighted many IT inefficiencies at the FBI. In 1990, the OIG issued a report entitled, "The FBI's Automatic Data Processing General Controls." This report found 11 major internal control weaknesses, many of which are still applicable today. Specifically the report stated that:

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

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

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

- the FBI had not adequately involved top management in FBI Headquarters or the field offices in systems development through an Executive Review Committee; and

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

Regarding the first weakness, the FBI's IT infrastructure is still severely outdated, as we previously mentioned. Regarding the second weakness, the FBI has recently restructured the IRD and Information Resources Management Section to reduce the fragmented management structure that existed among the three divisions responsible for managing IT. Regarding the third weakness, as discussed later in the report, the FBI is still developing an enterprise architecture framework, which includes the technical or data architecture. Regarding the fourth weakness, as discussed later in the

report, the FBI did not have formally established IT investment review boards or committees until March 2002. Regarding the fifth weakness, the FBI's major investigative systems remain labor intensive, complex, non-user friendly, and many Special Agents still do not use these systems.

The OIG's July 1999 special report on the handling of intelligence information related to the DOJ's campaign finance task force[13] stated that FBI personnel were not well versed in the Automated Case Support (ACS) system[14] and other databases. Additionally, a November 1999 report on the death of a federal inmate, Kenneth Michael Trentadue, noted deficiencies in uploading key evidence into the ACS.

A March 2002 report entitled, "An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case," analyzed the causes for the belated production of many documents in the Oklahoma City bombing case. This report concluded that the ACS system is extraordinarily difficult to use, has significant deficiencies, and is not the vehicle for moving the FBI into the 21st century. The report noted that inefficiencies and complexities with the ACS combined with the lack of a true information management system were contributing factors in the FBI's failure to provide hundreds of investigative documents to the defendants in the Oklahoma City Bombing Case. These reports illustrate that the FBI has not given sufficient attention to correcting its deficiencies in information management and the ACS.

In May 2002, pursuant to the FY 2002 Government Information Security Reform Act, the OIG issued a report on the FBI's administrative and investigative mainframe systems. This report identified continued vulnerabilities with management, operational, and technical controls. Significant vulnerabilities were noted in the following areas:

[13] The report, "Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation," was issued in July 1999.

[14] The ACS is the FBI's primary investigative computer application that uploads and stores case files electronically.

- security policies, procedures, standards, and guidelines;
- physical controls;
- system and network backup and restoration controls;
- password management;
- logon management;
- account integrity management;
- system auditing management; and
- system patches.

The report stated that these vulnerabilities occurred because the DOJ and FBI security management had not enforced compliance with existing security policies, developed a complete set of policies to effectively secure the administrative and investigative mainframes, or held FBI personnel responsible for timely correction of recurring findings. Further, the report indicated that FBI management has been slow to correct identified weaknesses and implement corrective action. Therefore, many of these deficiencies repeat year after year in subsequent audits.

In March 2002, the Commission for the Review of FBI Security Programs issued a report titled, "A Review of FBI Security Programs." This Commission, chaired by former FBI Director William H. Webster, was established to investigate the espionage of a FBI Supervisory Special Agent, Robert Hanssen.[15] The report identified a wide range of problems affecting the FBI's computer systems and information security policies, including the following:

- Classified information had been moved into systems not properly accredited for its protection.

[15] According to the report, over a period of 22 years, Robert Hanssen gave the Soviet Union and Russia vast quantities of documents and computer diskettes filled with national security information of incalculable value.

- Until recently, the FBI had not begun to certify and accredit most of its computer systems, including many classified systems.

- Inadequate physical protections placed electronically stored information at risk of compromise.

- The FBI's approach to system design has been deficient. It has failed to ascertain the security requirements of the "owners" of information on its systems and identify the threats and vulnerabilities that must be countered.

- Classified information stored on some of the FBI's most widely utilized systems was not adequately protected because computer users lacked sufficient guidance about critical security features.

- Some FBI inspectors had insufficient resources to perform required audits. When audits were performed, audit logs were reviewed sporadically, if at all.

According to the report, these findings resulted from the FBI's lack of attention to IT security in developing and managing computer systems.[16]

Additionally, the General Accounting Office (GAO) has issued several reports and related testimony that highlight deficiencies with the FBI's IT. In June 2002, the Comptroller General provided the following testimony before a subcommittee of the United States House of Representatives Appropriations Committee:

> Communications has been a longstanding problem for the FBI. This problem has included antiquated computer hardware and software, including the lack of a fully functional e-mail system. These deficiencies serve to significantly hamper the FBI's ability to share important and time sensitive information with the rest of the FBI across other intelligence and law enforcement agencies. We [the GAO] do not believe the FBI will be able to successfully change its mission and effectively transform itself without significantly upgrading its communications

[16] Although the focus of our audit does not assess the FBI's IT security practices, the two prior reports mentioned above indicate that the FBI's effective use of IT must address information assurance as part of an overall IT governance model.

> and information technology capabilities. This is critical, and it will take time and money to successfully address.[17]

In a review of the DOJ's Campaign Finance Task Force, the GAO reported in May 2002 that the FBI lacked an adequate information system that could manage and interrelate the evidence that had been gathered in relation to the Task Force's investigations.[18] Also, as part of a government-wide assessment of federal agencies, the GAO reported in February 2002 that the FBI needed to fully establish the management foundation that is necessary to successfully develop, implement, and maintain an enterprise architecture.[19]

The deficiencies in IT management are not solely attributable to the FBI itself, but are also attributable in part to DOJ actions. In December 2000, the GAO issued a report on the Immigration and Naturalization Service's (INS) investment management capability.[20] This report stated that the DOJ was not guiding and overseeing the INS's IT investment management (ITIM) approach. The report highlighted the DOJ's responsibility, as required by the Clinger-Cohen Act of 1996, to ensure that its components implement an effective ITIM process. According to the report, the DOJ had not provided the INS, or any other component, sufficient direction, guidance, and oversight of ITIM activities. Further, the report stated:

> While Justice [the Department of Justice] issued guidance in January 2000 describing its high-level investment management process, the guidance does not address the need or requirements for Justice's components to implement an IT investment management process. Specifically, this guidance does not instruct the components to establish IT investment management processes nor does it establish expectations for doing so. Until Justice issues its policy and guidance and begins monitoring its components' progress, it has no assurance

---

[17] This testimony, titled "FBI REORGANIZATION: Initial Steps Encouraging but Broad Transformation Needed" (GAO-02-865T), was released on June 21, 2002.

[18] This report, titled "CAMPAIGN FINANCE TASK FORCE: Problems and Disagreements Initially Hampered Justice's Investigation" (GAO/GGD-00-101BR), was released on May 31, 2000.

[19] This GAO report is discussed later in this report.

[20] "INFORMATON TECHNOLOGY: INS Needs to Strengthen Its Investment Management Capability" (GAO-01-146) was issued by the GAO in December 2000.

that it has the necessary investment management processes in place to maximize the value of its IT investments and manage the risks associated with the investments.

The DOJ issued ITIM guidance in August 2001 and required the components to develop an ITIM process by January 2002. This guidance, and the FBI's ITIM process, are further discussed later in this introduction.

4. The FBI's Current IT Investment Efforts

In a statement before the House Subcommittee on Appropriations in March 2002, FBI Director Mueller stated: "Without question, we all believe [information infrastructure] is the number one problem confronting the FBI today, recognize that for a number of reasons the situation developed over time, and know that in the future a better approach to technology upgrades must be used."

In the FBI Information Technology Upgrade Plan (FITUP), prepared and submitted to Congress in September 2000, the Bureau stated that a lack of funding was the cause for not making meaningful upgrades to its IT infrastructure since 1994. Congress responded to this concern by appropriating a total of approximately $2.2 billion for FBI IT projects and systems for FYs 1997 to 2002.[21] The FBI received $335.6 million of this amount in January 2002 from the Emergency Supplemental Appropriations Act for information technology. The following table summarizes the funds appropriated for FBI IT investments since FY 1997.

[21] This appropriation includes operation and maintenance costs of existing IT systems, enhancements to existing IT systems, and funding for new IT projects. The appropriation also includes personnel costs for managing the IT projects and systems.

Funds Appropriated for FBI IT Investments Since FY 1997

Fiscal Year	Total IT Investments (in millions)
2002	$714.0
2001	$352.8
2000	$293.0
1999	$332.0
1998	$241.2
1997	$309.2
Total	**$2,242.2**

Source: Exhibit 53s[22] prepared by the FBI

The FBI has several critical initiatives underway to upgrade its infrastructure and investigation applications. Additionally, the FBI has undertaken a major hiring initiative to recruit private sector IT experts who can assist in designing and managing the sizable IT projects recently funded by Congress. For example, the FBI's last two Chief Information Officers were hired from the private sector. Also, in March 2002, the FBI announced the hiring of a project executive from the private sector to manage Trilogy. Further, in June 2002, the FBI announced the hiring of an executive from the private sector to become the new Executive Assistant Director for Administration.

5. Trilogy: The FBI's Largest IT Investment

Currently, the FBI's largest IT project designed to improve IT infrastructure and office automation is the Trilogy project, formerly known as the FITUP. In September 2000, the FITUP was established to enhance the investigative support for FBI agents. The FITUP noted the following IT needs:

[22] The Exhibit 53 for each fiscal year lists funds appropriated for major IT projects. The FBI prepares the Exhibit 53 and submits it to the DOJ, which submits it to the Office of Management and Budget (OMB). Total IT investments include operation and maintenance costs of existing IT systems, enhancements to existing IT systems, and funding for new IT projects. These investment costs also include personnel costs associated with managing IT projects and systems.

- getting all case files into electronic databases (since the ACS is not consistently used);

- making IT more user friendly for agents;

- providing access to all databases via one search engine; and

- providing reliable, high-speed flexible communications.

To address the above needs, the FITUP, renamed to Trilogy, is intended to upgrade the FBI's: (1) hardware and software – referred to as the Information Presentation Component (IPC), (2) communication networks – referred to as the Transportation Network Component (TNC), and (3) five most important investigative applications – referred to as the User Applications Component (UAC). The IPC and TNC upgrades will provide the physical infrastructure needed to run the applications from the UAC portion of Trilogy. The UAC portion is intended to upgrade and consolidate five of the FBI's 42 investigative applications. Because there are 37 other investigative applications and approximately 160 non-investigative applications that Trilogy will not address, Trilogy is only a starting point towards upgrading the FBI's entire IT infrastructure.

In November 2000, Congress appropriated $100.7 million for the first year of the $379.8 million Trilogy project, which was to be funded over a three-year period (from the date contractors were hired). The $100.7 million was a combination of new program funding and a re-direction of base resources. The FBI combined the IPC and TNC portions for continuity when it requested contractor support, since both encompass physical IT infrastructure enhancements. The contractor for the IPC/TNC portions was hired in May 2001. As a result, the originally scheduled completion date for these initiatives was May 2004. A separate contractor was hired in June 2001 to complete the UAC portion of Trilogy by June 2004.

After the terrorist attacks on September 11, 2001, the importance of giving FBI agents and analysts the technological tools necessary to perform their duties was heightened in the eyes of Congress, the Attorney General, and the Director. Because the goal of Trilogy is to address many of the technological needs of the FBI, successful completion of the project in the shortest amount of time possible was viewed as increasingly critical to the FBI's fight against terrorism. Rather than wait three years for the benefits of Trilogy, Congress fully funded the FBI's original request of $379.8 million and

provided an additional $78 million in January 2002 to speed up its deployment.[23] With the supplemental funding, the FBI indicated to Congress that it would complete the deployment of hardware (including new desktop computers), networks, and software by July 2002. Additionally, the FBI would seek to accelerate upgrades to the five user applications. However, as discussed later in this report, the FBI did not meet its July 2002 milestone and is not expecting to complete the deployment of hardware, software, and networks until March 2003.

Although we believe the FBI must have sufficient resources to upgrade its technology through Trilogy and other projects, it must also have the management processes in place to effectively utilize those resources. With the recent influx of funding to the FBI, Congress expects the FBI to make significant strides in upgrading its IT infrastructure. But we believe the FBI will be successful in doing so only if it has effective IT management control processes in place. Later in this report, we provide an assessment of the FBI's management of Trilogy.

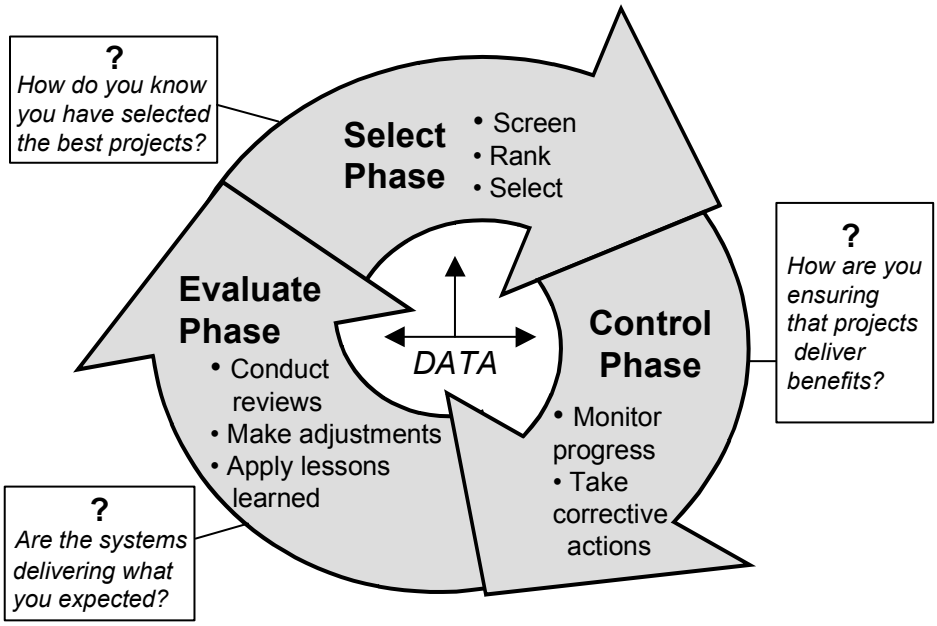
6. Framework for Assessing IT Investment Management

Several recent management reforms have required federal agencies to improve their management processes for selecting and managing IT investments. In particular, the Clinger-Cohen Act of 1996 requires the head of each agency to implement a process for maximizing the value of the agency's IT investments and for assessing and managing the risks of its acquisitions. A key goal of the Clinger-Cohen Act is for agencies to have processes in place to ensure that IT projects are being implemented at acceptable costs and within reasonable time frames, and that the projects are contributing to tangible, observable improvements in mission performance.

The Clinger-Cohen Act defines requirements for capital planning and control of IT investments and mandates a select/control/evaluate approach that federal agencies must follow. The following graphic describes the fundamental phases of this IT investment approach.

[23] The $78 million was part of the $745 million received from the Emergency Supplemental Appropriations Act.

Fundamental Phases of the IT Investment Approach



Source: GAO

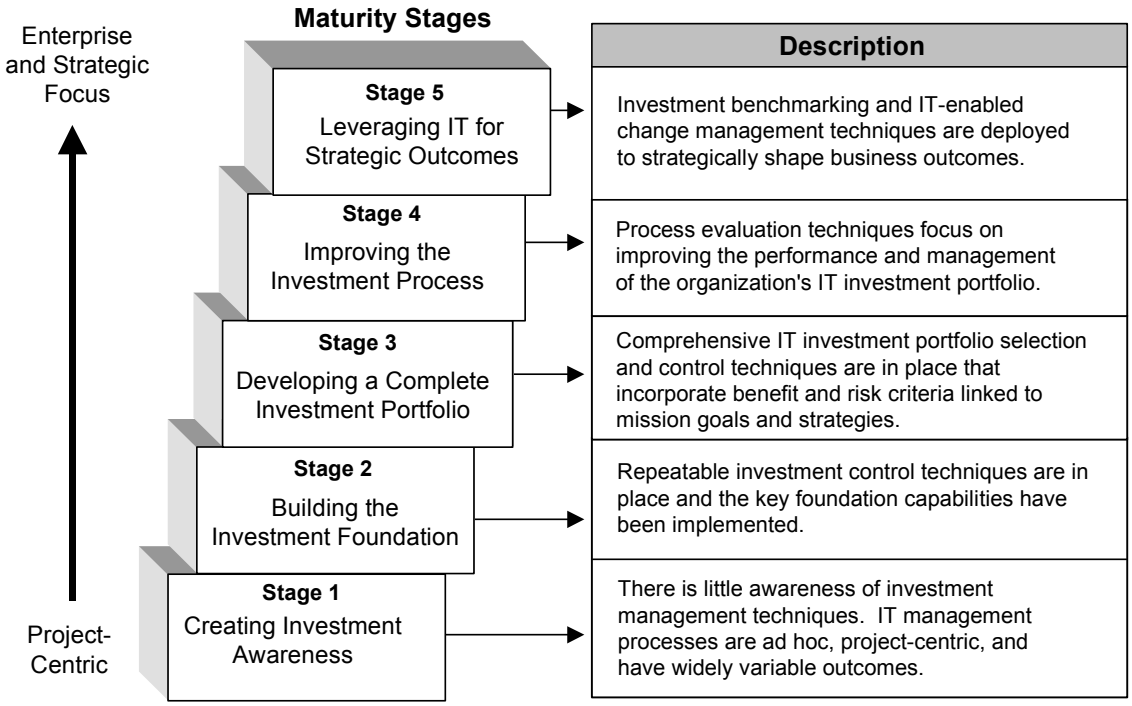
According to a GAO report, while almost all federal agencies have created some type of IT investment management process, none has implemented stable processes that address all three phases of the select/control/evaluate approach.[24] One barrier to implementing stable IT investment processes has been the lack of specific guidance regarding what processes are required to build a stable, reliable IT investment management organization. The select/control/evaluate approach provides sound advice, but it does not provide a comprehensive discussion of the organizational processes involved.

To address this concern, in May 2000 the GAO developed the IT Investment Management Framework (Framework) to provide a common methodology for discussing and assessing IT capital planning and investment management practices at federal agencies. The Framework enhances previous federal IT investment management guidance by embedding the select/control/evaluate approach within a framework that explicitly describes the organizational processes required to carry out good IT investment management.

[24] "Information Technology Investment Management: An Overview of GAO's Assessment Framework" (GAO/AIMD-00-155) was issued in May 2000.

The Framework, based on best practices of leading organizations, is a hierarchical model comprising of five maturity stages. These maturity stages represent steps toward achieving stable and mature investment management processes. Each stage builds upon the lower stages and enhances the organization's ability to manage its investments. As agencies advance through these stages, the agencies' capability to effectively manage IT increases. The following graphic describes the five maturity stages of the Framework.

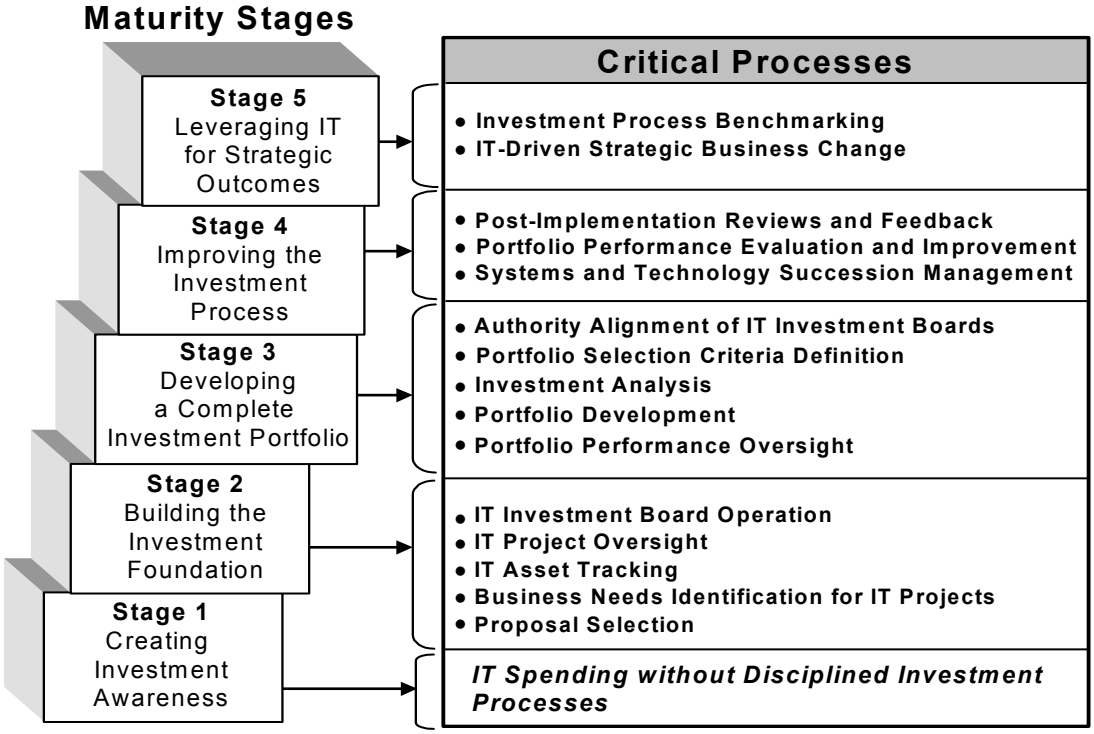
The Five Maturity Stages of the ITIM Framework



Source: GAO

With the exception of the first stage, each maturity stage is composed of critical processes that must be implemented and institutionalized for the organization to satisfy the requirements of that stage. These critical processes are further broken down into key practices that describe the types of activities that an agency should be engaged in to successfully implement each critical process. An organization that has these critical processes in place is in a better position to successfully invest in IT. The following graphic describes the Framework's five stages and associated critical processes.

The ITIM Framework's Stages of Maturity with Critical Processes



Source: GAO

As established by the Framework, each critical process contains five core elements that indicate whether the implementation and institutionalization of a process can be effective and repeated. The five core elements are:

- **Purpose:** This element is the primary reason for engaging in the critical process and states the desired outcome for the critical process.

- **Organizational commitment:** This element comprises management actions that ensure that the critical process is established and will endure. Key practices typically involve establishing organizational policies and engaging senior management sponsorship.

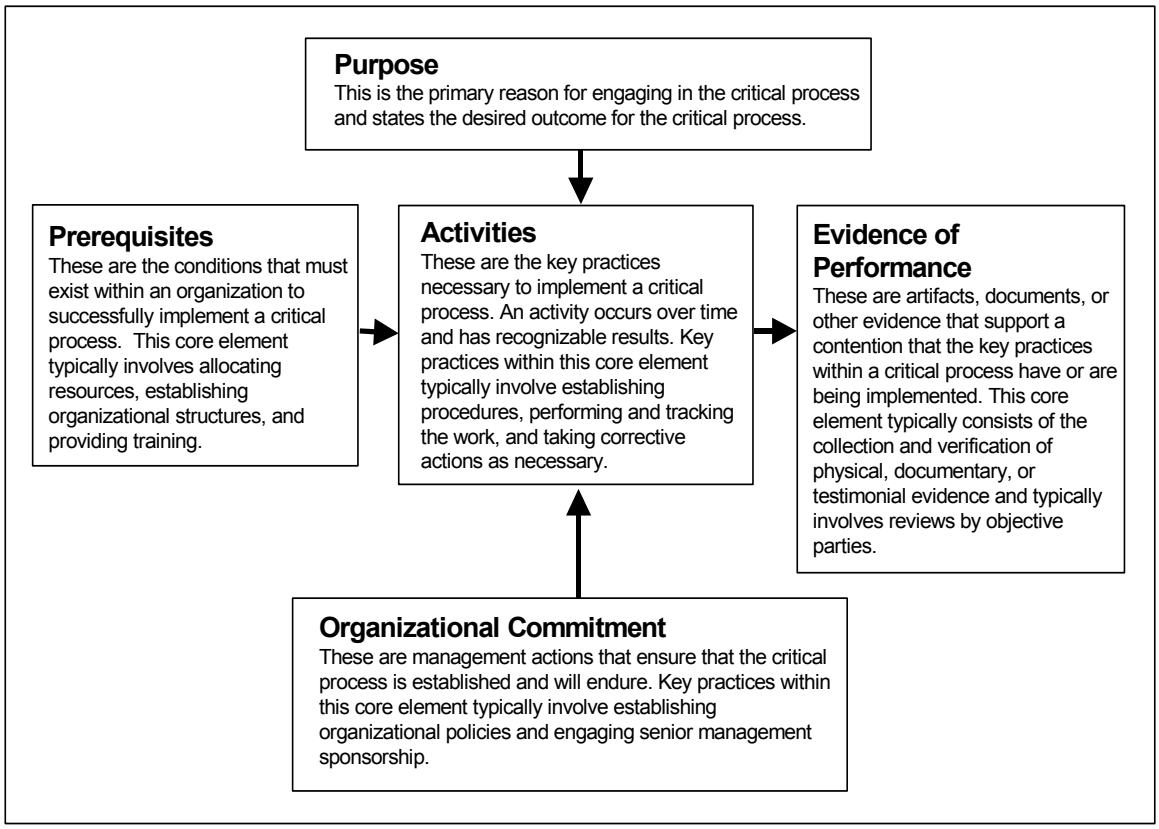
- **Prerequisites:** These elements are the conditions that must exist within an organization to successfully implement a critical process. These conditions typically involve allocating resources, establishing organizational structures, and providing training.

- **Activities:** These elements are the key practices necessary to implement a critical process. An activity occurs over time and has recognizable results. Key practices typically involve establishing procedures, performing and tracking the work, and taking corrective actions as necessary.

- **Evidence of performance:** This element comprises artifacts, documents, or other evidence that supports a contention that the key practices within a critical process have been or are being implemented. This core element typically consists of the collection and verification of physical, documentary, or testimonial evidence and often involves reviews by objective parties.

With the exception of the "purpose" core element, each of the other core elements contains key practices. The key practices are the attributes and activities that contribute most to the effective implementation and institutionalization of a critical process. The following graphic summarizes the interrelationships of components in an ITIM critical process.

Components of an ITIM Critical Process



Source: GAO

7. The DOJ's ITIM Guidance

In August 2001, the DOJ's Justice Management Division (JMD) issued the Guide to the Department of Justice Information Technology Investment Management Process (Guide). In response to various regulations and guidelines issued in the last several years (including the Clinger-Cohen Act, Executive Order 13011, and the Office of Management and Budget (OMB) Circular A-130), the DOJ issued the Guide to fulfill its obligation and responsibility to make measurable improvements in mission performance and service delivery to the public through the strategic application of IT.

The Guide uses the select/control/evaluate methodology to implement the strategic and performance directives of the Clinger-Cohen Act and other statutory provisions affecting IT investments. The Guide is intended to promote a process that builds on existing structures to provide maximum benefit across the entire DOJ and with other federal agencies. This process allows the DOJ to focus IT management on the strategic missions of the DOJ. Further, it

promotes an investment review process that drives budget formulation and execution for information systems, and restructures the way the DOJ performs its functions before investing in IT. In addition, this process provides the methods, structures, disciplines, and management framework that govern the way IT is deployed throughout the DOJ. The Guide applies to all IT projects from all DOJ components.

The Guide requires each component to:

- designate a component Chief Information Officer consistent with the DOJ's ITIM policy;

- establish an Executive Review Board that will approve the entire component IT portfolio and oversee the decisions made about specific investments; and

- establish a component ITIM process that incorporates the DOJ's ITIM process, but is customized to function within the component's unique environment.

Further, by January 2002 each component was required to submit to the DOJ an ITIM plan incorporating the above stipulations.

8. The FBI's Recent Efforts to Implement an ITIM Process

In an effort to improve its IT investment management practices and comply with DOJ and other statutory regulations, the FBI developed the "ITIM Model and Transition Plan" (Plan) with support from a contractor. The initial draft of the Plan was completed and submitted to JMD in January 2002. The FBI has retained this contractor to assist in the ongoing implementation of the ITIM process. The FBI estimates total costs for developing its ITIM process will be in excess of $4 million through FY 2003.

The purpose of the Plan is to establish and define the FBI's Stage Two[25] methodology and build the foundation for enhanced IT investment management. It identifies the gaps between the FBI's current IT investment processes and the required IT management practices for Stage Two maturity.

[25] "Stage Two" refers to Stage Two of the Framework, Building the IT Investment Foundation.

The following excerpts from the FBI's Plan provide an overview of how the FBI's select, control, and evaluate processes for IT investment management are intended to operate upon implementation.[26]

Select

In the Select phase, potential projects will be initiated by the project sponsor via the development of a preliminary feasibility analysis (concept paper), followed by the development of a more-robust business case analyses (OMB Exhibit 300). The project proposal package will be submitted to the Technical Review Board[27] to be assessed for any technical risks and then submitted to the Project Oversight Committee[28] for a business review. The Project Oversight Committee will assemble the multiple requests and prioritize these requests against predefined selection criteria. A "candidate" fiscal project portfolio will then be developed and presented to the Executive Review Board[29] for final evaluation and approval, and ultimately for submission to the fiscal budget process.

Control

In the Control phase, the current fiscal year IT portfolio will be tracked by the functional project management office and individual project teams. Monthly status reports will be created and presented to the Project Oversight Committee, who will work to mitigate any project related risks. Projects with exceptions to the baseline plans will be subsequently presented to the Executive Review Board for

[26] See Appendices 2 and 3, respectively, for flowcharts on the Plan's control and evaluate processes.

[27] According to the Plan, the Technical Review Board must be established to review each proposed ITIM initiative for enterprise architecture compliance, IT security compliance, and other technical risks.

[28] According to the Plan, the Project Oversight Committee must be established to perform the program management and oversight duties of the ITIM process, such as making recommendations to the Executive Review Board on selecting IT proposals and disposing of IT projects.

[29] According to the Plan, the Executive Review Board must be established to make the final IT investment decisions.

decisions about budget, scope, timeline and/or projected outcomes. During the control phase, a project will be able to receive approval to: proceed "as is," proceed with modified funding levels and/or modified functionality, or be terminated.

Evaluate

In the Evaluate phase, IT investments that are in the operations and maintenance mode will be monitored by the Executive Review Board to ensure that expected benefits are being realized. Periodic program reviews will be conducted, wherein each IT investment will be evaluated against predefined performance metrics and criteria. Based on the reviews, decisions will be made about: future phases of existing projects; and the current policies and procedures governing the entire IT investment management, the systems development life-cycle, and other related processes. Advocacy arguments (to modify existing management practices and procedures) are also constructed during this phase, if applicable.

JMD officially approved the FBI's Plan in May 2002, although officials from the IRD told us that in February 2002 they received verbal approval to initiate their ITIM process.[30] The May 2002 approval letter states that the FBI ITIM process conforms to the guidelines defined by the GAO, OMB, and DOJ. Further, it states that the Plan is clear and comprehensive in its statement of the ITIM policy and its definition of organizational roles, responsibilities, and deliverables. Additional JMD comments, as well as our own independent assessment of the Plan, are discussed later in this report.

The FBI started its ITIM process in February 2002 by appointing the three oversight review boards discussed above (the Technical Review Board, the Project Oversight Committee, and the Executive Review Board). Also, in February 2002 the FBI held training seminars for each division to introduce the concepts of the Plan. In March 2002, the FBI began pilot testing the select phase of the Plan for FY 2004 proposed IT project enhancements. In May 2002, the pilot test of the

[30] JMD officials told us that the delay in providing written approval of the FBI's ITIM process was because JMD did not have a Chief Information Officer early in 2002.

select phase was completed and the ITIM contractor issued the, "Post Implementation Review: FBI ITIM Pilot."

The Plan recognizes that as the FBI's ITIM process moves through the maturity stages, other key components of IT infrastructure must evolve to optimize the IT investment function. These components include an IT strategic plan, an enterprise architecture framework, and project management. According to the Framework, an effective IT function will include these components and mature IT investment management processes are dependent on the components being in place.

OIG FINDINGS AND RECOMMENDATIONS

1. The FBI's Management of IT Investments

The FBI is not effectively selecting, controlling, and evaluating its IT investments because it has not fully implemented any of the critical processes necessary for successful IT investment management. In the past, the FBI has not given sufficient attention to information technology investment management. As a result, the FBI continues to spend hundreds of millions of dollars on IT projects without having adequate selection and project management controls in place to ensure that IT projects will meet intended goals. However, since the FBI developed its ITIM Model and Transition Plan in January 2002, it has focused more management attention in this area and has made progress towards attaining a basic IT investment management foundation. Much of the progress has been in the "select" phase of the Plan, which was pilot tested in the Spring of 2002.

The ability of the FBI to completely implement the "control" and "evaluate" phases of the Plan, and achieve mature IT investment processes that can lead to enhanced mission performance, will require the FBI to increase its efforts in: (1) fully developing and documenting its new ITIM process; (2) requiring more input and participation from ITIM managers and users; and (3) further developing its project management and enterprise architecture functions. While the FBI recognizes many of these needs and has taken initial steps to address the needs, further action in these areas is needed to ensure that IT projects are developed within cost and schedule requirements, and meet performance expectations. The Trilogy project provides an example of how the non-implementation of fundamental IT investment management practices can put a project at risk of not delivering, within cost and schedule requirements, what was promised.

A. The FBI's Progress Toward Attaining a Basic IT Investment Management Foundation

Although the FBI made measurable progress in improving its IT investment capability since it initiated a new ITIM process in early

2002, the FBI still lacks a complete foundation to build its IT investment maturity processes, and therefore is still in Stage One maturity.[31] In the past, the FBI has not given sufficient management attention to IT investments. Because of the lack of management attention in the past, the FBI failed to implement the critical processes necessary to build an IT investment foundation. These critical processes include: (1) IT investment review board operation, (2) IT project oversight, (3) IT system and project identification and tracking, (4) business needs identification for IT projects, and (5) IT proposal selection.

(1) Importance of Attaining a Basic IT Investment Management Foundation

The primary purpose for attaining a basic IT investment management capability (Stage Two maturity) is to build the foundation for repeatable, successful IT project-level investment control and selection processes. Effective control processes over IT projects ensure that deviations from cost and schedule baselines can be identified and corrected. Selection processes ensure that the FBI has an effective methodology for approving only IT projects that are consistent with its needs and goals. According to the Framework, an organization can only achieve Stage Two maturity if it fully implements the following five critical processes:

1. defining investment review board operations,

2. developing a basic process for selecting new IT proposals,

3. developing project-level investment control processes,

4. identifying IT projects and systems, and

5. identifying the business needs for each IT project.

To implement these critical processes, the FBI must execute a total of 38 key practices as defined in the Framework, or have alternative practices in place that are designed to achieve the same outcome.

[31] Stage One maturity is the lowest level of maturity designated by the GAO ITIM Framework. According to the Framework, an organization is in Stage One maturity when it has not fully implemented the five critical processes associated with Stage Two maturity.

At the start of our audit in January 2002, FBI officials told us that the Bureau was in the process of developing its new ITIM process. Although its ITIM process was still in the development stages, FBI officials told us that the FBI was executing certain key practices from Stage Two of the Framework. Additionally, the FBI officials said in March 2002 that they would pilot test ITIM processes pertaining to the selection of new IT proposals for the FY 2004 budget cycle. Further, the Plan establishes the FBI's goal to fully attain Stage Two maturity for the FY 2005 budget cycle that starts in March of 2003, thereby establishing the foundation for enhanced investment capability.

(2) Summary of the FBI's Progress Toward Attaining Stage Two Maturity

Based on the FBI's responses to the self-assessment[32] (and our validation of those responses), the FBI did not yet have in place any of the five critical processes associated with Stage Two maturity. However, since the FBI began pilot testing the select phase of its Plan in March 2002, it has made progress towards implementing the 38 key practices comprising the five critical processes - particularly in the area of selecting new proposals for IT projects. Specifically, at the beginning of our audit in January 2002, the FBI was only executing 4 of the 38 required key practices; however, as of June 2002, the FBI was executing 14 of the key practices. The following table provides a summary of the FBI's progress toward implementing the key practices required for each critical process.

[32] To facilitate our assessment of the FBI's IT investment maturity, the FBI completed a self-assessment regarding the key practices from the Framework that it was executing, or planning to execute, upon implementation of its new ITIM process.

FBI Progress Toward Attaining Stage Two Maturity

Critical Process	Status of Implementing Critical Process	Total Key Practices Required	Key Practices Executed Prior to March 2002	Key Practices Executed as of June 2002
1. IT Investment Board Operation	Not Implemented	6	0	2
2. IT Project Oversight	Not Implemented	11	1	2
3. IT Project Identification	Not Implemented	7	1	2
4. Business Needs Identification for IT Projects	Not Implemented	8	2	3
5. Proposal Selection	Not Yet Implemented, but Substantial Progress Made	6	0	5
Total		**38**	**4**	**14**

Source: OIG analyses

For the remainder of section A of this finding, we provide detailed narratives of the FBI's progress toward implementing each of the five critical processes. We also provide specific recommendations for expediting implementation of the critical processes and establishing more timely Stage Two maturity.

Each critical process contains core elements that provide the common framework for the process. For example, the organizational commitment element addresses the management actions that ensure the critical process is established and will endure; the prerequisites element addresses the conditions that must exist within an organization to successfully implement a critical process; and the activities element consists of the key practices necessary to implement a critical process. The key practices are the tasks within a core

element that must be performed by an organization to effectively implement and institutionalize a critical process.

(3) Critical Process #1: IT Investment Review Board Operation

Depending on its size, structure, and culture, an organization may have more than one IT investment review board. The purpose of such boards is to ensure that basic policies for selecting, controlling, and evaluating IT investments are developed, institutionalized, and consistently followed throughout the organization. To establish a fully functioning investment review board, the FBI must execute the following six key practices:

1. create an IT investment process guide containing policies and procedures to direct board operations;

2. require executives and line managers to support and carry out board decisions;

3. allocate adequate resources for operating each board;

4. define board membership, policies and procedures, roles and responsibilities;

5. create and define board membership to integrate both IT and business knowledge; and

6. require the IT investment boards to follow the written policies and procedures as defined in the process guide.

The following table summarizes the FBI's progress toward implementing fully functioning investment review boards.

FBI Progress Toward Implementing Fully Functioning Investment Review Boards (Critical Process #1)

Key Practice	Key Practice Execution Status Prior to March 2002	Key Practice Execution Status as of June 2002
Organizational Commitment 1. An organization-specific IT investment process guide is created to direct each board's operations.	Not Executed	**Executed**
Organizational Commitment 2. Organization executives and line managers support and carry out IT investment board decisions.	Not Executed	Not Executed
Prerequisite 1. Adequate resources are provided for operating each IT investment board.	Not Executed	Not Executed
Prerequisite 2. Board members understand the investment board's policies and procedures and exhibit core competencies in using the IT investment approach via training, education, or experience.	Not Executed	Not Executed
Activity 1. Each IT investment board is created and defined with board membership integrating both IT and business knowledge.	Not Executed	**Executed**
Activity 2. Each IT investment board operates according to written policies and procedures in the organization-specific IT investment process guide.	Not Executed	Not Executed

Source: OIG analyses

a. The FBI Has Executed Two of the Six Key Practices Associated with IT Investment Board Operation

We determined that the FBI executed two of the six key practices associated with implementing this critical process. Specifically, the FBI created an IT investment process guide containing policies and procedures to direct board operations (Organizational Commitment 1), and it created and defined three investment review boards integrating both IT and business knowledge (Activity 1).

Regarding the IT investment process guide (Organizational Commitment 1), in January 2002 the FBI issued its IT Investment Model and Transition Plan[33] containing required guide elements prescribed by the Framework including:

- specifics about the roles of key people within the FBI investment process;

- an outline of the significant events and decision points within the processes;

- an identification of the external and environmental factors that will influence the processes; and

- the manner in which IT investment-related processes will be coordinated with other organizational plans and processes.

Regarding the investment review boards (Activity 1), in June 2002 the Director approved board charters for each of the three investment review boards (the Executive Review Board, the Project Oversight Committee, and the Technical Review Board) that defined board membership and the responsibilities of board members.

- The Executive Review Board is comprised of the FBI Director (as Chairperson), the Chief Information Officer, the FBI's four Executive Assistant Directors (EADs),[34] a Special Agent in Charge committee member, the Assistant Director of the Finance Division, and the Strategic Planning Manager.

  This Board's primary responsibility will be to evaluate and approve projects in the candidate fiscal project portfolios and forward approved projects to the fiscal budget process. This Board will also determine whether problematic projects should proceed "as is," proceed with modified funding levels and/or modified functionality, or be terminated.

- The Project Oversight Committee includes: the Chief Information Officer (as Chairperson), the Assistant Director from

[33] The Plan was issued in draft form because it is the intent of the FBI to modify and supplement the Plan as the ITIM process is being pilot tested.

[34] The EADs are for: (1) Criminal Investigations, (2) Counterterrorism and Counterintelligence, (3) Law Enforcement Services, and (4) Administration.

each division, a member from the Office of General Counsel, the Chief Contracting Officer, and the Strategic Planning Manager.

Once the Technical Review Board completes its assessment, the Project Review Board then performs a business review of the proposed projects, prioritizes these proposals against predefined selection criteria, and develops a "candidate" fiscal project portfolio for presentation to the Executive Review Board. The committee also reviews monthly status reports for ongoing projects to mitigate project related risks. Projects with exceptions to baseline plans will be presented to the Executive Review Board for corrective action.

- The Technical Review Board is comprised of: the Section Chief, Information Resources Management Office (as Chairperson); the Assistant Director of IRD; the IRD's section chiefs; and representatives from the Laboratory Division, CJIS Division, and Security Division. This board's primary responsibility will be to assess technical risks for proposed projects.

The boards actually began functioning as early as March 2002, in conjunction with the FBI's pilot testing of ITIM processes pertaining to the selection of new IT proposals for the FY 2004 budget cycle. Although board membership consists mostly of FBI managers who do not have extensive IT knowledge,[35] the use of subject matter experts and reliance on the Enterprise Architecture Technical Committee[36] can compensate for a lack of IT knowledge.

b. The FBI Must Execute Four of the Six Key Practices Associated with IT Investment Board Operation

Although progress has been made, the FBI does not have fully functioning IT investment boards because it still must execute four of the six key practices associated with this critical process. Specifically, the FBI must ensure that:

[35] Based on our interviews with FBI managers from the IRD, CJIS, and Inspection Divisions, most of the members on the investment boards are former agents with no specialized expertise, training, or competencies in IT.

[36] The Enterprise Architecture Technical Committee was created to provide technical expertise to the Technical Review Board. Members of this committee are comprised of IT specialists familiar with enterprise architecture, configuration management, and quality assurance.

- organization executives and line managers support and carry out IT investment board decisions (Organizational Commitment 2);

- adequate resources are provided for operating each IT investment board (Prerequisite 1);

- board members understand the investment board's policies and procedures and exhibit core competencies in using the IT investment approach via training, education, or experience (Prerequisite 2); and

- each IT investment board operates according to written policies and procedures contained in the investment process guide (Activity 2).

Regarding Organizational Commitment 2 and Activity 2, the approved charters for the investment review boards have been in effect since June 2002. Consequently, the FBI did not have sufficient data for us to assess whether managers and support staff effectively carried out board decisions and whether the boards operated according to the written policies and procedures contained in the Plan and board charters.

Regarding Prerequisites 1 and 2, in our judgment the FBI did not adequately plan sufficient time to ensure the IT investment boards operated effectively. Specifically, the FBI did not provide ample time between the initial draft of its Plan (January 25, 2002) and the March 2002 pilot testing of the select phase to adequately prepare and train IT board members. The DOJ originally instructed each component to begin developing an ITIM process in January 2001.[37] In June 2001, the DOJ required each component to complete and submit to JMD an ITIM process and transition plan by the end of 2001.[38] The DOJ also required each component to initiate the ITIM process for the FY 2004 budget cycle, which for the FBI began in March 2002. Consequently, the FBI had only one full month between the issuance of the Plan in late January 2002 and the initiation of the select phase of its ITIM process in early March 2002.

[37] This instruction originated from DOJ Order 2880.1A, policy on Information Technology Investment Management, issued in January 2001.

[38] This instruction originated from a DOJ memorandum dated June 28, 2001. This memorandum required each component to have an ITIM transition plan that will allow implementation for the FY 2004 budget cycle.

The ITIM Program Office Manager told us that the former FBI Chief Financial Officer would not approve the use of a contractor to assist in the development of the ITIM process earlier in the year. According to the former Chief Financial Officer, she had concerns that federal contracting regulations prohibited the FBI from using a contractor to perform a service that involves budget planning. However, following her transfer to another division in December 2001, the Information Resources Management Section received authorization to hire a contractor to assist with the development and implementation of the ITIM process.

We believe that without an ITIM contractor the FBI still had the opportunity to begin planning its ITIM process (including the training of board members) early in 2001. In fact, had the FBI better coordinated other ongoing efforts to develop processes that complement IT investment management, the FBI could have made significant strides in initiating its ITIM process during 2001 without expending additional resources. As discussed in section B of this finding, the FBI did not sufficiently incorporate (a) its enterprise architecture function (which was under development in 2001) and (b) the Project Management Process (issued in draft form in October 2001) into the development of its ITIM process. Enterprise architecture and project management not only complement the ITIM process, but also facilitate the maturation of ITIM. As discussed in section B of this finding, the FBI did not effectively utilize its internal resources when it developed its ITIM process through the use of a contractor because the FBI did not adequately consider the complementary, and potentially duplicative efforts that were already underway.

Not providing ample time resulted in inadequate training of board members and minimal preparation time to develop IT proposals. For example, Technical Review Board members had only 3 business days to review over 50 IT proposals prior to their first board meeting. FBI officials recognized these implementation issues in the Post-Implementation Review of the select phase pilot test.

In preparing board members for their duties, the FBI has thus far only provided one overview training session for board members and other users in the ITIM process. Additionally, while FBI officials have told us more ITIM training will be forthcoming, they have not provided us with any specific training plans for the future. Further, members of the Technical Review Board told us that board members, especially the Assistant Directors and EADs, do not have extensive

knowledge in managing IT and must rely heavily on knowledgeable staff and other subject matter experts.

For the ITIM process to become institutionalized, the FBI must have a better training program. According to the Framework, board members should understand the board's policies, roles, rules, and activities and be capable of carrying out their responsibilities competently. Education and training for members is needed in areas such as economic evaluation techniques, capital budgeting methods, and performance measurement strategies. The FBI's Post-Implementation Review of the select phase pilot testing recommends "role-specific" training sessions for the following ITIM roles: (1) ITIM Liaison representatives,[39] (2) Executive Review Board members, (3) Program Oversight Review Board members, (4) Technical Review Board members, and (5) ITIM stakeholders. It further recommends continuation of the overview training sessions previously provided, plus training for ITIM specific tools, such as the concept paper (containing the preliminary feasibility analysis), the OMB Exhibit 300 (containing the business case analyses), and IT proposal summaries.

FBI officials told us that time constraints were the main cause for not executing the four key practices identified above. As a result, there was insufficient time to introduce ITIM concepts to board members and other ITIM users. As mentioned above, the DOJ required each component to develop and begin implementation of an ITIM process for the FY 2004 budget cycle, which for the FBI begins in March 2002. Although FBI officials were aware of the requirement to initiate and adopt an ITIM process in January 2001, it was not until December 2001 that it began to develop its ITIM process. Had the FBI initiated more timely action to develop its ITIM process, it would have had significantly more time to prepare and train ITIM board members and other users. Without sufficient training and allocation of time to perform required tasks, the investment review boards cannot carry out their responsibilities to effectively select, control and evaluate projects.

[39] The FBI's ITIM process defines the ITIM Liaison Representative as an individual from a particular division/business unit that facilitates workflow and communications between that division/business unit and the ITIM program office.

c. Recommendations

We recommend that the Director of the FBI:

1. Require the ITIM Program Office to plan for and take more timely action to allow board members and other ITIM users to execute assigned responsibilities competently (Prerequisite 1).

2. Ensure that all members of IT investment boards receive sufficient education and training to execute assigned responsibilities effectively. We suggest that for each of the investment boards the FBI: (a) identify the core competencies required of members in using the IT investment approach, and (b) develop appropriate education and training development plans to ensure members acquire the required core competencies (Prerequisite 2).

(4) Critical Process #2: IT Project Oversight

The purpose of this critical process is to ensure that the FBI's investment review boards and project development teams provide effective oversight for its IT projects throughout all phases of the project life-cycle. IT investment boards generally review each project's progress toward predicted cost and schedule expectations as well as anticipated benefits and risk exposure. The board members also employ early warning systems that enable them to take corrective actions at the first signs of cost, schedule, and performance slippages. Individual project development teams are responsible for meeting project milestones within the expected cost and schedule parameters.

Effective project oversight requires, among other things:

- having written policies and procedures for project management;

- developing and maintaining an approved project management plan for each project;

- having written policies and procedures for oversight of IT projects;

- making up-to-date cost and schedule data for projects available to the investment review boards;

- reviewing each project's performance by comparing actual cost and schedule data to expectations regularly; and

- ensuring that corrective actions for each under-performing project are defined, implemented, and tracked until the desired outcome is achieved.

We concluded that the FBI is not effectively overseeing its ongoing IT projects. While the FBI maintained project management guidance and had three IT investment review boards in operation since March 2002, these activities have not adequately supported the FBI's IT project oversight function. Our testing of the key practices associated with this critical process indicates that the FBI is executing only two out of the eleven key practices required to implement this critical process. The following table summarizes FBI progress toward implementing IT project oversight.

FBI Progress Toward Implementing IT Project Oversight (Critical Process #2)

Key Practice	Key Practice Execution Status Prior to March 2002	Key Practice Execution Status as of June 2002
Organizational Commitment 1. The organization has written policies and procedures for project management.	**Executed**	**Executed**
Organizational Commitment 2. The organization has written policies and procedures for management oversight of IT projects.	Not Executed	Not Executed
Prerequisite 1. Adequate resources are provided to assist the boards in overseeing IT projects.	Not Executed	Not Executed
Prerequisite 2. Each IT project has and maintains an approved project management plan that includes cost and schedule controls.	Not Executed	Not Executed
Prerequisite 3. An IT investment review board is operating.	Not Executed	**Executed**
Prerequisite 4. Information from the IT asset inventory is used by the IT investment board as applicable.	Not Executed	Not Executed
Activity 1. Each project's up-to-date cost and schedule data are provided to the appropriate IT investment board.	Not Executed	Not Executed
Activity 2. Using established criteria, the IT investment board oversees each IT project's performance regularly by comparing actual cost and schedule data to expectations.	Not Executed	Not Executed
Activity 3. The IT investment board performs special reviews of projects that have not met predetermined performance standards.	Not Executed	Not Executed
Activity 4. Appropriate corrective actions for each under-performing project are defined, documented, and agreed to by the IT investment board and the project manager.	Not Executed	Not Executed
Activity 5. Corrective actions are implemented and tracked until the desired outcome is achieved.	Not Executed	Not Executed

Source: OIG analyses

a. The FBI Has Executed Two of the Eleven Key Practices Associated with IT Project Oversight

While the FBI has project management guidance (and is therefore executing the key practice relating to the existence of project management methodology), the guidance is not being followed on a consistent basis. In fact, depending on whom we talked to, we obtained different answers as to which document represented the FBI's official project management guidance.

For example, although IRD managers were aware that the DOJ's System Development Life-Cycle is the FBI's official project management methodology, they acknowledged that it is not consistently applied. Laboratory Division management officials told us that they do not follow the DOJ's System Development Life-Cycle methodology, but rather have adopted their own project management system based on one used at the Department of Defense because it better meets their needs. CJIS Division management officials told us that although its Contract Administration Office is responsible for project management functions, they were not following any specific project methodology.

Other FBI personnel from the Information Resources Management Section told us the Project Management Process, developed by the FBI's Inspection Division, was the FBI's project management guidance. However, Inspection Division personnel indicated to us that the Project Management Process was still pending approval from the Director, as of June 2002. As a result, there appeared to be confusion among FBI officials as to what the official project management guidance was. As of June 2002, the Project Management Process had not been approved, nor was it being used to manage IT projects.

As previously discussed in the prior report section pertaining to the investment review board critical process, the FBI established three IT investment review boards in March 2002 (the Executive Review Board, the Project Oversight Committee, and the Technical Review Board). Although the investment review boards are operating, the boards have not yet been involved in project oversight. As the ITIM process continues to evolve, project oversight by these boards should increase accordingly.

b. The FBI Must Execute Nine of the Eleven Key Practices Associated with IT Project Oversight

Based on our analyses, the FBI does not have effective IT project oversight because it has not yet executed nine out of the eleven key practices associated with this critical process. Specifically, the FBI must ensure that:

- written policies and procedures are developed for management oversight of IT projects (Organizational Commitment 2);
- adequate resources are provided to assist the investment boards in overseeing IT projects (Prerequisite 1);
- an approved project management plan is prepared for each IT project that includes cost and schedule controls (Prerequisite 2);
- information from the IT asset inventory is used by the IT investment boards as applicable (Prerequisite 4);
- each project's up-to-date cost and schedule data are provided to the appropriate IT investment board (Activity 1);
- using established criteria, the IT investment boards oversee each IT project's performance regularly by comparing actual cost and schedule data to expectations (Activity 2);
- the IT investment boards perform special reviews of projects that have not met predetermined performance standards (Activity 3);
- appropriate corrective actions for each under-performing project are defined, documented, and agreed to by the IT investment boards and the project manager (Activity 4); and
- corrective actions are implemented and tracked until the desired outcome is achieved (Activity 5).

Regarding Organizational Commitment 2, the FBI has not developed written policies and procedures for management oversight of IT projects. While the Plan provides a conceptual basis for board oversight of IT projects and the board charters define the boards' responsibilities, the FBI does not have the specific policies and procedures in place for overseeing and controlling projects. FBI

officials have acknowledged to us that the Plan was never intended to represent the complete and final policies and procedures for management oversight of IT projects. The Plan states that it is a fluid document that will need to be modified and supplemented as the pilot test is performed. As a result, FBI officials recognize that additional policies and procedures must be developed. As of June 2002, FBI officials have told us they are in the process of developing these specific policies and procedures for the control phase of the ITIM pilot test.

Regarding Prerequisite 1 (providing adequate resources to the boards), we concluded that this key practice has not been executed because as of June 2002, the FBI did not have a functioning project management office to assist the boards in overseeing IT projects. The Plan calls for a functioning project management office to assist the boards, especially the Project Oversight Committee, and consequently is a necessary resource for IT project oversight. As of June 2002, the FBI has not yet utilized its project management function to assist the Project Oversight Committee in IT investment decision-making.

The functioning project management office represents a critical resource to the Project Oversight Committee and thus to IT project oversight. In our judgment, the functioning project management office needs to have jurisdiction over IT projects throughout the Bureau, rather than limit its responsibilities to division-specific projects. Until June 2002, the FBI lacked a functioning project management office that had jurisdiction over IT projects throughout the Bureau. Rather than having a centralized project management office, independent of individual divisions, the FBI maintained three separate division-level project management offices to manage IT projects. These three separate project management functions were maintained in the IRD, CJIS, and Laboratory Divisions, contributing to inefficiencies in project coordination and the risk of "stove piping" projects. Because of its importance in supporting the ITIM process, the subject of establishing and maintaining a centralized project management office is further discussed later in this report.

Regarding Prerequisite 2, we determined that each IT project does not have an approved project management plan that includes cost and schedule controls. Personnel from the IRD project management office told us that generally IT projects with high visibility have project management plans that include cost and schedule controls. However, other lower visibility projects have less rigid controls in place. This condition developed because the IRD project

management office did not uniformly enforce the development of project management plans by all IT project managers. In our judgment, projects under the IRD's discretion have not been adequately controlled. Although personnel from the CJIS and Laboratory Divisions indicated that IT projects under their respective divisions did have management plans with cost and schedule controls, without a functioning board that approves and monitors these project management plans FBI managers have no assurance that IT projects are effectively managed in accordance with uniform standards.

Regarding Prerequisite 4, the FBI has not yet developed an IT asset inventory; consequently, the FBI's investment review boards are not aware of all the IT projects and resources for which the boards are responsible. FBI managers told us they were in the process of developing an IT asset inventory. However, at the time of our audit they were unable to provide an estimated date for completing the inventory. Unless the investment review board members are fully cognizant of the IT projects and resources for which they are responsible, the boards cannot exercise effective oversight of ongoing IT projects. Additional details pertaining to the FBI's plans to finalize the IT inventory are provided later in this report.

Finally, since the IT investment review boards were not involved in overseeing IT projects as of June 2002, we concluded that none of the five remaining key practices activities have been executed. These five key practices are the basic activities that investment review boards must implement to effectively oversee IT projects during the control phase. The FBI provided us documentation indicating that the Project Oversight Committee (the primary IT investment review board responsible for overseeing IT projects) met in June 2002 to discuss the FBI's intent to pilot test the control phase of the Plan by September 2002. The documentation stated that the FBI was still working on designing the specific procedures associated with the control phase, including integrating the ITIM process with the project management office. Additionally, the FBI has only provided us with summary information on when and how the control phase of the ITIM process will be rolled out. The information lacks specific details needed to effectively implement this critical process.

FBI personnel told us that the lack of established IT investment review boards (prior to March 2002) was the main cause for ineffective project oversight. Additionally, they stated that the control phase of the ITIM process would be pilot tested by September 2002. However, the FBI has not been able to provide us with a specific timeline as to:

(1) how the pilot test will be executed, and (2) details as to how the ITIM process will interface with a project management methodology. These issues are further discussed in Section B of this finding.

Without effective oversight of IT projects, FBI officials do not have adequate assurance that IT projects are being developed on schedule and within established budgets. As described in the following paragraphs, the lack of effective IT project oversight has contributed to the FBI's problems in managing IT projects, including a lack of accountability for cost and schedule overruns, a lack of consideration for full life-cycle costs, and lost credibility with Congress.

According to a former Chief Information Officer at the FBI, the lack of effective oversight of IT projects (as a result of not having IT investment review boards and a centralized project management office) have prevented IT project managers from being held accountable for cost and schedule overruns and the ultimate performance of projects. For example, the former Chief Information Officer told us that the CJIS Division completed the Integrated Automated Fingerprint Identification System and the National Crime Information Center 2000 years behind schedule and millions of dollars over budget. He also told us that management changes in the CJIS Division have not occurred, despite these overruns.

Senior FBI officials also told us that the Bureau's budget formulation process focuses only on the acquisition costs for IT projects and not the full life-cycle costs, especially operations and maintenance costs. For example, an assessment performed by the FBI's Inspection Division on the Trilogy project[40] noted that the life-cycle cost estimate is inadequate and only focuses on the term of the contract, not the life of the project. FBI personnel told us that a lack of consideration for full project costs is not limited to Trilogy, but also applies to other IT projects. Without accountability for significant deviations from project baselines, there is a lack of incentives for project managers to adequately control and evaluate projects.

According to FBI officials, the FBI's inability to effectively complete IT projects within budget and schedule reduced the FBI's credibility in the eyes of Congress. The lack of credibility contributed to delays in the FBI receiving Congressional funding to upgrade its IT infrastructure. This subject, along with how Trilogy may be adversely affected because of uncertainties in determining projected costs and

[40] The Trilogy project is discussed in greater detail in section C of this finding.

scheduled completion dates for project milestones, is further discussed in section C of this finding.

c. Recommendations

We recommend that the Director of the FBI ensure:

3. Official project management guidance is consistently followed by all FBI IT project managers.

4. Written policies and procedures are developed for management oversight of IT projects for use by the investment review boards (Organizational Commitment 2).

5. IT Investment Review Boards are supported by a centralized project management office that operates in accordance with ITIM policies and procedures (Prerequisite 1).

6. Each IT project has a project management plan, approved by the Project Oversight Committee, that includes cost and schedule controls (Prerequisite 2).

7. Information being developed in the IT asset inventory is made available to, and used by, the boards (Prerequisite 4).

8. Execution of the five key practices consisting of the activities necessary for the investment review boards to maintain effective oversight of IT projects during the critical control phase. These five key practices consist of:

   - Providing each project's up-to-date cost and schedule data to the appropriate IT investment board (Activity 1).

   - Establishing criteria for the boards to review each IT project's performance by comparing actual cost and schedule data to expectations (Activity 2).

   - Performing special reviews of projects that have not met predetermined performance standards (Activity 3).

   - Defining, documenting, and agreeing to corrective actions for each under-performing project by the appropriate IT investment board and the project manager (Activity 4).

- Tracking and implementing corrective actions until the desired outcome is achieved (Activity 5).

(5) Critical Process #3: IT Project and System Identification

For the FBI to make effective IT investment decisions, it must have at its disposal information about existing IT investments as well as the proposed investments being considered. The purpose of this critical process is to provide the IT investment boards the information required to fully evaluate the impacts and opportunities created by both the proposed and current IT investments. The key practices of this process require the FBI to identify and track the IT projects and systems within the organization to create a comprehensive inventory. According to the Framework, effective identification of IT projects and systems requires:

- identifying specific information about each IT project and system in an inventory, according to written procedures;

- updating information in the inventory as changes to projects and systems occur;

- making information from the inventory available to users as needed; and

- assigning responsibility for managing the IT system identification process.

While the FBI has taken steps to identify its IT projects and systems in an IT asset inventory, it still does not have a complete IT asset inventory that is being using by the IT investment review boards for investment management purposes. As part of an enterprise architecture data repository, the FBI is developing a comprehensive inventory of its IT projects and systems. In addition, FBI officials have told us that the enterprise architecture office is primarily responsible for developing and maintaining the data repository. However, the data repository has not been completed, nor have board members used its contents during the select phase of the ITIM process that took place during the Spring of 2002. The FBI's enterprise architecture function is further discussed in section B of this finding. The following table summarizes the key practice ratings for the IT project and system identification critical process.

FBI Progress Toward Identifying IT Projects and Systems (Critical Process #3)

Key Practice	Key Practice Execution Status Prior to March 2002	Key Practice Execution Status as of June 2002
Organizational Commitment 1. The organization has written policies and procedures for identifying its IT projects and systems and collecting an inventory that includes information about the IT projects and systems that is relevant to the investment management process.	**Executed**	**Executed**
Organizational Commitment 2. An official is assigned responsibility for managing the IT project and system identification process and ensuring the inventory meets the needs of the investment management process.	Not Executed	**Executed**
Prerequisite 1. Adequate resources are provided for identifying IT projects and systems and collecting relevant information into an inventory.	Not Executed	Not Executed
Activity 1. The organization's IT projects and systems are identified and specific information about these projects is collected in an inventory.	Not Executed	Not Executed
Activity 2. Changes to IT projects and systems are identified and changed information is collected in the inventory.	Not Executed	Not Executed
Activity 3. Information from the inventory is available on demand to decision-makers and other affected parties.	Not Executed	Not Executed
Activity 4. The IT project and system inventory and its information records are maintained to contribute to future investment selections and assessments.	Not Executed	Not Executed

Source: OIG analyses

a. The FBI has Executed Two of the Seven Key Practices Associated With Identifying IT Projects and Systems

Based on our analyses, we determined that the FBI has executed two of the seven key practices associated with this critical process. Specifically, the FBI has developed written policies and procedures for identifying its IT projects and systems in an inventory that includes information relevant to the investment management process (Organizational Commitment 1). Additionally, the FBI has designated an official responsible for managing the IT project and system identification process and ensuring that the inventory meets the needs of the investment management process (Organizational Commitment 2).

Regarding Organizational Commitment 1, we determined that the FBI has developed adequate written policies and procedures for: (a) identifying its IT projects and systems and (b) collecting information relevant to the investment management process on each project and system. Prior to December 2001, the FBI did not have written policies and procedures for identifying IT projects and systems. The FBI did, however, provide us with an electronic communication dated December 3, 2001 from the enterprise architecture staff that was distributed Bureau-wide requesting management from each division to provide information on its IT systems. The information obtained from the divisions is used by the enterprise architecture staff to develop the data repository of IT systems.

Regarding Organizational Commitment 2, the FBI has designated the Chief Architect of the enterprise architecture office with responsibility for managing the IT project and system identification process and ensuring that the inventory, when completed, meets the needs of the investment management process and ITIM managers and users. The Chief Architect currently reports to the Information Resource Management Section Chief, who reports to the Chief Information Officer.

b. The FBI Must Execute Five of the Seven Key Practices Associated with Identifying IT Projects and Systems

Although the FBI has made recent progress in identifying IT projects and systems, the FBI does not have a comprehensive IT project and system identification process because it still has not executed five out of the seven key practices associated with this critical process. Specifically, the FBI must ensure that:

- adequate resources are provided for identifying IT projects and systems and collecting relevant information into an inventory (Prerequisite 1);

- the organization's IT projects and systems are identified and specific information about these projects and systems is collected in an inventory (Activity 1);

- changes to IT projects and systems are identified and changed information is collected in the inventory (Activity 2);

- information from the inventory is available on demand to decision-makers and other affected parties (Activity 3); and

- the IT project and system inventory and its information records are maintained to contribute to future investment selections and assessments (Activity 4).

Regarding Prerequisite 1, FBI managers told us that the FBI has not allocated adequate resources to ensure timely and successful completion of the IT project and system identification critical process. FBI managers from the Information Resources Management Section told us that they do not have sufficient staffing to support the ITIM process, including the enterprise architecture function. The enterprise architecture office within the Information Resources Management Section plays a key role in the ITIM process as it assists the Technical Review Board and maintains the data repository information on IT systems and projects. Further, personnel who we interviewed from the enterprise architecture office told us that limited staffing was a factor in not having the data repository completed.[41]

Regarding the remaining four key practices, none of those practices can be executed until the FBI completes the creation of its IT asset inventory. More importantly, the IT asset inventory will have little value to the FBI if it is not used when making IT investment decisions. Prior attempts at compiling an inventory of IT projects were used to satisfy Congressional and DOJ requests, rather than to assist the IT investment management process. For example, the FBI

[41] Our judgments regarding staffing issues within the enterprise architecture office are discussed in more detail later in this report.

prepared a partial list of its information technology projects to comply with a Congressional request in August 2000.

FBI officials informed us that they anticipate the investment review boards will use the completed inventories to contribute to future investment selections and assessments. The Plan states that the FBI must establish a complete IT portfolio set as the ITIM process matures. Further, FBI personnel told us that the enterprise architecture data repository, when complete, will be available to decision-makers and other ITIM users via the FBI's Intranet. However, we have not been provided with a specific timeframe for when the FBI expects to have a completed inventory.

FBI personnel told us that the primary cause of not having a completed IT asset inventory and actively using it in the ITIM process is because of staffing shortages. While that may be a contributing factor, we concluded that the lack of centralized management over IT investments was also a limiting factor. As a result, certain divisions maintained some version of an IT inventory for the projects and systems under their jurisdiction, and there was no centralized office responsible for maintaining a uniform listing Bureau-wide.

Without a complete IT asset inventory in the ITIM process, FBI management and board members do not have adequate assurance that accurate, timely, and complete information on existing IT projects and systems is available to them. As a result, there is a risk that new IT proposals selected overlap with one of the 200 or so existing FBI applications. While the recently established review boards helped to mitigate this risk for the FY 2004 budget selection process, we believe that an IT asset inventory must be used by the boards to optimize the use of the FBI's resources.

c. Recommendations

We recommend that the Director of the FBI:

9. Establish a deadline for completing the creation of the FBI IT inventory and ensure progress toward completion is monitored (Activity 1).

10. Implement processes to ensure:

    a. subsequent changes to IT projects and systems are identified and documented in the inventory (Activity 2);

    b. information from the inventory is available on demand to decision-makers and other affected parties (Activity 3); and

    c. the IT project and system inventory and its information records are maintained to contribute to future investment selections and assessments (Activity 4).

(6) Critical Process #4: Business Needs Identification

This critical process establishes the mechanism for identifying the business needs and the associated users that drive each IT project. This critical process links the organization's business objectives with its IT strategy and creates the partnership between the users and the IT providers. According to the Framework, effective identification of business needs requires:

- defining the organization's business needs and goals;
- identifying users who will participate throughout the life-cycle of each project;
- defining business needs for each IT project; and
- training IT staff in business needs identification.

While the FBI has made progress in identifying business needs for IT projects, it has not yet executed all the key practices necessary to implement this critical process. Prior to pilot testing the select phase of its ITIM process in March 2002, the FBI had been identifying users for each IT project in the Exhibit 300.[42] Since pilot testing the select phase of the ITIM process beginning in March 2002, the FBI has used a concept paper along with the Exhibit 300 to identify and define business needs. In addition, the FBI has defined its general business needs and goals in its strategic plan, which is further discussed later in this report. However, as previously mentioned, the FBI has not

[42] An Exhibit 300 is a capital asset plan that must be prepared for major projects and is submitted to the DOJ and OMB.

identified all of its IT projects in an asset inventory; consequently, progress in implementing this critical process is contingent upon completing the FBI IT inventory. Also, we were not provided evidence indicating that identified users participate in project management throughout a project's life-cycle. The following table summarizes the key practice ratings for the business needs identification critical process.

FBI Progress Toward Identifying its Business Needs (Critical Process #4)

Key Practice	Key Practice Execution Status Prior to March 2002	Key Practice Execution Status as of June 2002
Organizational Commitment 1. The organization has written policies and procedures for identifying the business needs (and the associated users) of each IT project.	Not Executed	Not Executed
Prerequisite 1. Adequate resources are provided for identifying business needs and associated users.	Not Executed	Not Executed
Prerequisite 2. The organization has defined business needs or stated mission goals.	**Executed**	**Executed**
Prerequisite 3. IT staff are trained in business needs identification.	Not Executed	Not Executed
Prerequisite 4. All IT projects are identified in the IT asset inventory.	Not Executed	Not Executed
Activity 1. The business needs for each IT project are clearly identified and defined.	Not Executed	**Executed**
Activity 2. Specific users are identified for each IT project.	**Executed**	**Executed**
Activity 3. Identified users participate in project management throughout a project's life-cycle.	Not Executed	Not Executed

Source: OIG analyses

a. The FBI has Executed Three of the Eight Key Practices Required to Identify its Business Needs and Associated Users

We determined that the FBI has executed three of the eight key practices associated with this critical process. Specifically, the FBI has defined its business needs or stated mission goals (Prerequisite 2); the business needs for identified IT projects are clearly identified and

defined (Activity 1); and specific users are identified for each IT project (Activity 2).

Regarding Prerequisite 2, we determined that the FBI has defined business needs or stated mission goals. The FBI has stated mission goals in its strategic plan. The FBI's strategic plan has not been updated since 1998, but the Director has revised the priorities of the Bureau since the terrorist attacks on September 11, 2001. Further, the FBI is currently in the process of developing an enterprise architecture framework, which will link the FBI's strategic plan to its business needs.

Regarding Activity 1, we determined that the business needs for each IT project are clearly identified and defined in the Exhibit 300. Prior to the initiation of the ITIM pilot test in March 2002, the FBI did not have adequate management controls in place to ensure that the business needs for each project were accurately developed in the Exhibit 300. With the ITIM process, the board reviews of the concept papers and Exhibit 300s provided assurance that these business needs were clearly identified and defined. In instances where the business needs were vague, the boards, especially the Technical Review Board, returned the concept papers and Exhibit 300s to the project sponsor for re-work. This re-work demonstrates that board review of these IT proposals was an effective control over the business needs identification process. Our review of Exhibit 300s that were ultimately recommended to the Executive Review Board for inclusion in the FY 2004 budget cycle confirmed that business needs were clearly identified and defined.

Regarding Activity 2, the FBI identified specific users for each IT project. Based on our reviews of several Exhibit 300s both before and after the initiation of the ITIM process in March 2002, we determined that the users for the IT project were identified and documented.

b. The FBI Must Execute Five of the Eight Key Practices Required to Identify its business Needs and Associated Users

Although progress has been made in identifying its business needs and associated users, the FBI has yet to execute five of the eight key practices associated with this critical process. Specifically, the FBI must ensure that:

- it has formalized written policies and procedures for identifying the business needs (and the associated users) of each IT project (Organizational Commitment 1);

- adequate resources are provided for identifying business needs and associated users (Prerequisite 1);

- IT staff are trained in business needs identification (Prerequisite 3);

- all IT projects are identified in the IT asset inventory (Prerequisite 4); and

- identified users participate in project management throughout the project life-cycle (Activity 3).

Regarding Organizational Commitment 1, we determined that the FBI does not have written policies and procedures for identifying the business needs (and the associated users) of each IT project. The FBI has been defining business needs for IT projects in the Exhibits 300 and related concept papers. The Post-Implementation Review acknowledges that the FBI needs more formally developed policies and procedures to support the ITIM process. By formalizing these procedures in writing, the FBI reduces the risk that it will neglect to perform this practice in the future.

Regarding Prerequisites 1 and 3, FBI officials told us that adequate resources were not allocated to identifying business needs and associated users. Specifically, FBI officials from the Information Resources Management Section told us that there has not been sufficient resources dedicated to the ITIM process, including the training of ITIM users. The importance of training ITIM users in the many facets of the ITIM process cannot be underestimated. Part of the required ITIM training must include the business needs identification process. Examples of training in this critical process include organizational requirements for ongoing education, rotation of ITIM users through supported business units, and relevant conference attendance. As previously mentioned, many ITIM users have only received one training session on the FBI's ITIM process. Additionally, the FBI has not provided us with specific plans for future training sessions that include business needs identification. As a result, these key practices have not been executed.

The ITIM training that occurred in February 2002 provided only an overview of the ITIM process, rather than role-specific training that addressed the business needs identification. The Post-Implementation Review stated that re-work of Exhibit 300s and concept papers were required after these products were submitted to the ITIM program office. This re-work was necessary because there was not a clear alignment between the IT proposal and the FBI's strategic goals. Better training that included business needs identification may have reduced some of the re-work. Further, a more clearly defined enterprise architecture framework would have increased the IT staff's knowledge in business needs identification.

Regarding Prerequisite 4, as previously mentioned, the FBI has not completed its IT asset inventory. Identifying all projects in an IT asset inventory is a fundamental step in having a fully developed business needs identification process. The availability of this inventory assists board members in recommending IT projects that support one or more business needs or mission goals.

Regarding Activity 3, FBI officials have acknowledged that identified users do not consistently participate throughout the project's life-cycle. FBI officials informed us that not keeping IT system users actively involved in the creation and implementation of IT projects is a major factor in the development of multiple IT systems (including ACS) that do not effectively meet user needs. When we asked the former Chief Information Officer for other examples of systems that do not effectively meet user needs, his response was "pick one." Clearly, this is a significant need that must be addressed by the ITIM process. The DOJ's System Development Life-Cycle requires user participation throughout the life-cycle, but as we previously noted in this finding, the System Development Life-Cycle is not used by the FBI on a consistent basis. Board oversight of project teams should be required to ensure that users are engaged throughout the project's life-cycle.

FBI officials told us that there has not been ample time since the implementation of the Plan to adequately train its IT staff and board members in business needs identification. A complete explanation as to why the FBI did not have ample time for training was previously discussed in section A.3 of this finding.

Although FBI officials have told us that additional training for IT staff and board members is expected to occur sometime in the future, we were not provided evidence that shows there will be any training specifically related to business needs identification. Further, we have

not been provided with a timetable as to when this training will take place. In addition, an effective business needs identification process requires an organization to have a comprehensive IT portfolio and enterprise architecture, neither of which the FBI currently has. Our assessment of the FBI's efforts to implement a basic enterprise architecture is discussed later in this report.

Without a comprehensive business needs identification process, FBI management and board members do not have adequate assurance that they are selecting IT projects that align with mission needs and priorities. Additionally, projects under development are at risk of not meeting the needs of users, as has been the case with ACS and other FBI systems.

c. Recommendations

We recommend that the Director of the FBI ensures:

11. Written policies and procedures are developed for identifying the business needs (and the associated users) of each IT project (Organizational Commitment 1).

12. Adequate resources are allocated to train ITIM users in identifying business needs and associated users (Prerequisites 1 and 3).

13. Identified users participate in project management throughout a project's life-cycle (Activity 3).

(7) Critical Process #5: IT Proposal Selection

The proposal selection critical process establishes a structured methodology for selecting new IT proposals. The FBI should have this critical process fully implemented to ensure that it selects the most meritorious IT proposals to meet its mission critical needs. According to the Framework, this critical process requires:

- designating an official to manage the proposal selection process;
- using a structured process to develop new proposals;
- making funding decisions based on an established process; and
- analyzing and ranking new IT proposals against criteria that includes cost and schedule data.

The following table summarizes the key practice ratings for the proposal selection critical process.

FBI Progress Toward Establishing an IT Proposal Selection Process (Critical Process #5)

Key Practice	Key Practice Execution Status Prior to March 2002	Key Practice Execution Status as of June 2002
Organizational Commitment 1. Executives and managers are committed to follow an established selection process.	Not Executed	**Executed**
Organizational Commitment 2. An official is designated to manage the proposal selection process.	Not Executed	**Executed**
Prerequisite 1. Adequate resources are provided for proposal selection activities.	Not Executed	Not Executed
Activity 1. The organization uses a structured process to develop new IT proposals.	Not Executed	**Executed**
Activity 2. Executives analyze and prioritize new IT proposals according to established selection criteria.	Not Executed	**Executed**
Activity 3. Executives make funding decisions for new IT proposals according to an established process.	Not Executed	**Executed**

Source: OIG analyses

a. The FBI Has Executed Five of the Six Key Practices Associated With Establishing an IT Proposal Selection Process

As previously discussed, the FBI pilot tested its ITIM proposal process in March 2002. The Plan outlined a conceptual framework for selecting projects, while subsequent documents further defined the process. We determined that the FBI has executed five of the six key practices associated with this critical process. The five key practice are:

- FBI managers are committed to follow an established selection process (Organizational Commitment 1);

- an official is designated to manage the proposal selection process (Organizational Commitment 2);

- the FBI uses a structured process to develop new IT proposals (Activity 1);

- FBI managers analyze and prioritize new IT proposals according to established selection criteria (Activity 2); and

- executives make funding decisions for new IT proposals according to an established process (Activity 3).

Regarding Organizational Commitment 1 and Activity 1, we concluded that in pilot testing its proposal selection process in March 2002, FBI managers were committed to and followed an established selection process for the FY 2004 budget cycle.

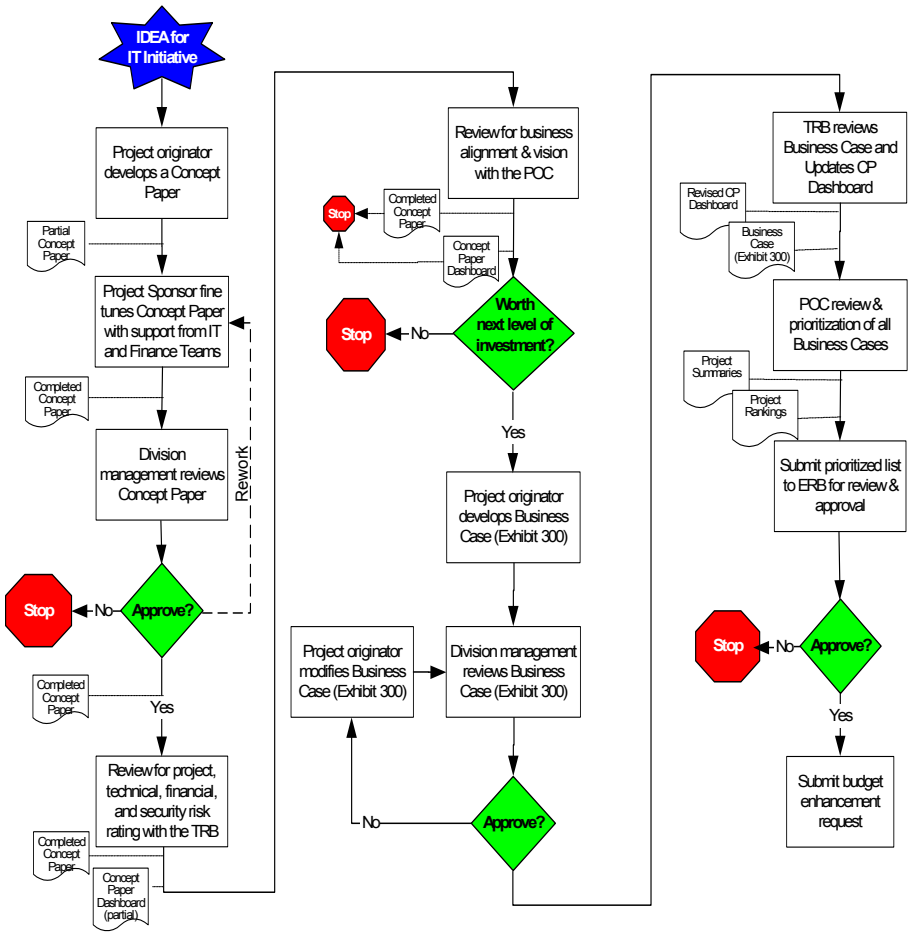
Prior to the initiation of the ITIM process in March 2002, the FBI did not have an established process for selecting IT proposals. Several FBI officials told us that individual divisions determined their IT needs in a "stovepipe," without knowledge of the business needs and priorities of the Bureau as a whole. Once each division decided on its IT request, the request was forwarded to the Information Resources Management Section for a "technical" review. This review, performed by the Information Resources Management Section Chief, was designed to ensure that the request was consistent with the FBI's existing IT infrastructure. However, without an established enterprise architecture, the review could not adequately provide assurance that the proposal aligned with the FBI's business needs and priorities.

Once approved by the Information Resources Management Section Chief, the request was then forwarded to the Finance Division to determine if similar requests for budget enhancements were previously denied by Congress. Requests approved by the Finance Division were forwarded to a committee comprised of executive managers for final evaluation and selection. However, personnel from the Finance Division told us that it was not uncommon for the IRD, Laboratory, and CJIS Divisions to submit requests for IT projects that were duplicative but were approved anyway. This indicates that the Information Resources Management Section did not adequately perform its role in overseeing IT proposals. Additionally, according to FBI officials, the committee of executive managers did not have a formalized charter, follow approved polices or procedures, or maintain

documentation detailing committee activities. Therefore, the process was not standardized or repeatable.

With the initiation of the ITIM process in March 2002, the FBI established a proposal selection process for the FY 2004 budget cycle. IT proposals were developed by the project sponsor with a preliminary feasibility analysis, referred to as a concept paper. The concept paper was submitted to the Enterprise Architecture Technical Committee for a preliminary technical review, and then forwarded to the Technical Review Board with a recommendation as to whether the project should be approved. Upon the Technical Review Board's approval, the project sponsor was asked to prepare a more comprehensive business case analysis, which was documented in the Exhibit 300. The project proposal package, which includes the concept paper and Exhibit 300, was then submitted to the Project Oversight Committee for a business review. The Project Oversight Committee assembled the multiple requests and recommended a list of projects for the Executive Review Board's review. The Executive Review Board selected projects for the FY 2004 budget cycle. Because this process was documented in the Plan, and enhanced with training materials, we concluded that the FBI effectively established a selection process. The following flowchart outlines the FBI's proposal selection process.

FLOWCHART OF FBI'S ITIM SELECT PHASE



Source: FBI's training materials for the ITIM process as of February 2002.

Regarding Organizational Commitment 2, prior to the initiation of the select phase of its ITIM process in March 2002, the FBI did not have a clearly designated official to manage the proposal selection process. According to Information Resources Management Section personnel, the Finance Division managed the IT selection process. However, according to Finance Division personnel, the Information Resources Management office was responsible for managing the proposal selection process. With the onset of the ITIM process in March 2002, the FBI's Chief Information Officer appointed the ITIM

Program Manager to manage the proposal selection process. This official reports to the Information Resources Management Section Chief, who reports to the Chief Information Officer.

Regarding Activity 2, we determined that FBI IT investment board members analyzed and prioritized new IT proposals according to established selection criteria for the FY 2004 budget cycle. Projects were prioritized according to three separate areas: (1) mission fit; (2) technical criteria (including risk management and architectural assessments); and (3) financial criteria (including performance measures, cost/benefit analyses, and acquisition strategy).

Regarding Activity 3, the three IT investment review boards made funding decisions for new IT proposals according to a process established for the FY 2004 budget cycle. The Executive Review Board, chaired by the Director, had the final authority for making IT funding requests to the DOJ. The Executive Review Board members based their decisions upon recommendations made by the Technical Review Board and the Project Oversight Committee. Based on the use of an established process, this key practice has been executed.

b. The FBI Must Execute One Key Practice Associated With Establishing an IT Proposal Selection Process

Although the FBI has made substantial progress in establishing an IT proposal selection process for the FY 2004 budget cycle, in our judgment it has yet to allocate adequate resources for comprehensive proposal selection activities. Our conclusion is based upon the following observations.

- The FBI pilot tested the selection process only for proposed budget enhancements for FY 2004 and not for projects already included in the base funding for IT.[43] As a result, the selection process was not comprehensive because it did not include all FY 2004 funding for IT.

- Project sponsors had insufficient time to adequately document proposals in the concept paper and Exhibit 300. According to the FBI's Post-Implementation Review of the pilot test, project sponsors had as little as three days to develop concept papers

[43] Funding for IT projects comes from both base funding and enhancements. Base funding is usually the prior fiscal year's budget allocation. Enhancements are additions to the prior fiscal year's base that are sought to fulfill certain priorities.

and Exhibit 300s used in the IT proposal selection process. FBI officials told us that it can take over a month to adequately prepare a comprehensive business case analysis (Exhibit 300). As a result of the time constraints, the Post-Implementation Review stated that concept papers, Exhibit 300s, and IT proposal summaries were submitted with gaps and omissions in areas such as: (1) aligning proposed activity with the FBI's strategic goals, (2) technical details, (3) acquisition and performance management approaches, (4) resource requirements and commitments, (5) expected levels of return-on-investment, and (6) security.

- According to the Post-Implementation Review of the pilot test, the boards and project sponsors did not maximize the use of subject matter experts to facilitate the proposal selection process. Additionally, according to the Post-Implementation Review, project owners did not adequately consult with internal staff in various divisions when preparing their IT proposals.

- Finally, the ITIM Program Manager, appointed in February 2002, was not provided any staff to assist her (other than contractor support). FBI officials stated to us in the self-assessment that the insufficient staffing is the number one challenge to implementing the ITIM process. Additionally, according to the Post-Implementation Review, the ITIM Program Office did not have sufficient staffing to sustain the ITIM process. Specifically, the Post-Implementation Review recommends two additional full-time employees to be added immediately, with an eventual goal of having at least six full-time employees in the ITIM Program Office. ITIM staffing is necessary to facilitate communications between the boards, project owners, and divisions. Clearly, adequate staffing for the ITIM Program Office is essential to successfully implement the ITIM process.

Without a comprehensive proposal selection process that includes adequate resources and training, the FBI cannot ensure that it is selecting the best IT projects that meet mission-critical needs.

c. Recommendations

We recommend that the Director of the FBI ensures:

14. The ITIM process applies to all IT project proposals, including proposals that are funded through the FBI's base funding.

15. Sufficient staffing is provided to the ITIM Program Office, as recommended in the Post-Implementation Review.

(8) Overriding Cause for the Lack of an FBI IT Investment Management Foundation

Although the GAO ITIM Framework was originally published in May 2000, the underlying key practices needed to implement each critical process are, in essence, tasks that are fundamental to any project management endeavor. Some of these tasks include the prerequisite conditions that must be in place in an organization to successfully implement critical processes. These tasks involve allocating resources, establishing organizational structures, and providing training. Another group of tasks include the organizational commitments that ensure critical processes will endure. These tasks involve establishing organizational policies and engaging senior management sponsorship. A third group of tasks include the activities necessary to implement the critical processes. These tasks involve establishing procedures, performing and tracking the work, and taking corrective actions as necessary.

Although these tasks are fundamental to effective project management, the majority of these tasks had not been executed by the FBI to select and manage its IT resources. Prior to the development of its ITIM process in early 2002, the FBI did not give sufficient attention to IT investment management. Organizational policies were not clearly established to ensure that critical IT investment policies endure. Additionally, there were no clearly defined, uniform procedures for project management, tracking project performance, and taking corrective actions as necessary.

Because the FBI did not fully implement any of the critical processes associated with Stage Two, the FBI continues to spend hundreds of millions of dollars on IT projects without having adequate selection and project management controls in place to ensure that IT projects will deliver their intended benefits. However, the FBI has made progress in improving its IT investment process since it initiated

a new ITIM process in early in 2002. Although further action is required, the launching of the ITIM process represents improvement in the FBI's ability to mitigate the risks that IT projects will not deliver their intended benefits. Whether the FBI can achieve further improvement depends on whether the Plan addresses the remaining key practices not being executed as well as the FBI's ability to completely implement the Plan and fully establish its ITIM process.

B. The FBI's Ability to Improve its IT Investment Practices

As previously noted, the FBI lacks a foundation necessary to build its IT investment capabilities, and therefore, is in Stage One maturity. However, in January 2002, the FBI developed an ITIM plan to build a foundation for selecting, controlling, and evaluating IT investments. Additionally, during the course of our audit fieldwork (from January 2002 to June 2002), the FBI initiated its ITIM process, as defined by the Plan. Consequently, the FBI made progress towards implementing the Plan, especially in the area of IT proposal selection.

Because the FBI was only in the beginning stages of implementing the Plan during our audit fieldwork, we assessed the FBI's ability to progress through the more advanced stages of the framework necessary to improve its IT investment maturity. Our assessment of the FBI's ability to improve its IT investment management consisted of the following four areas:

1. the Plan's coverage of Stage Two key practice activities that were not being executed during our fieldwork – necessary to determine adequacy of the Plan;

2. the amount of participation from ITIM users in developing the ITIM process – necessary to determine buy-in to the process;

3. the support from the project management function – necessary to execute the control and evaluate phases of the ITIM process; and

4. the support from the enterprise architecture function – necessary to advance through the maturity stages of the Framework.

Our evaluation of these four areas, documented in the following sections, includes both the FBI's strengths and weaknesses in each

area. In our judgment, the FBI's efforts in these areas are critical to its ability to maximize the effectiveness of its ITIM process, and ultimately improve mission performance.

(1) The Plan's Coverage of Stage Two Key Practice Activities That Were Not Being Executed During Our Fieldwork

The FBI's IT Investment Management Model and Transition Plan addresses the select, control, and evaluate key practice activities necessary to build an IT investment foundation. However, the Plan requires further development to ensure effective implementation. Because the Plan was intended to be a conceptual framework, it was not written to fully describe the specific policies and procedures of the select, control, and evaluate phases of the ITIM process. Without further development of the ITIM process, the FBI will have difficulty making additional progress in improving its IT investment management practices, especially in the control and evaluate phases.

a. Importance of the Plan's Coverage of Stage Two Key Practice Activities

Because the Plan stated that its purpose is to establish and define the FBI's Stage Two methodology necessary to build an IT investment foundation, we examined the Plan's coverage of Stage Two key practice activities. The FBI was pilot testing the select phase of the ITIM process during our audit fieldwork. As previously noted, we determined that the FBI executed 14 of 38 Stage Two key practices, mainly in the area of proposal selection. Of the 24 key practices that were not executed, 11 specifically related to activities associated with the control and evaluate phases of the ITIM process. Although the FBI had made little progress in executing activities from the control and evaluate phases of the Plan during our fieldwork, we examined the Plan to determine whether it adequately addressed the 11 Stage Two key practices activities associated with the control and evaluate phases that were not being executed. The ability of the FBI to achieve Stage Two maturity is dependent, in part, on the adequacy of the Plan.

In JMD's assessment of the Plan, JMD rated the Plan against elements it considered necessary to comply with GAO, OMB, and DOJ guidelines. JMD's assessment indicated that the Plan complied with the criteria used.[44] Additionally, JMD's assessment stated that although the Plan does not fully address a few items, such as the exact

[44] JMD's assessment of the Plan is contained in Appendix 4 of this report.

criteria that will be used to select and evaluate investments, it does provide a schedule for completing these items.

Our assessment of the Plan focused on whether it addressed the Stage Two maturity key practices in the GAO ITIM Framework and our conclusions are consistent with those from JMD.

b. Results of Our Assessment of the Plan's Coverage of Stage Two Key Practice Activities Associated with the Control and Evaluate Phases

In our judgment, the FBI's IT Investment Management Model and Transition Plan addresses the 11 Stage Two key practice activities, on a conceptual level, that were not being executed during our fieldwork. Because the key practice activities are addressed conceptually, further development is needed to clearly define these activities and to determine how these activities can be implemented.

Our analyses (previously documented in this report) indicated that the FBI was not executing one or more key practice activities in each of the following Stage Two critical processes: (1) IT investment board operation; (2) IT project oversight; (3) IT project and system identification; and (4) business needs identification. As previously discussed, 11 of the key practice activities necessary to implement these four critical processes relate to the control and evaluate phases of the Plan. The tables below describe how the Plan addresses the key practice activities that we determined were not being executed during our audit testing.

IT Investment Board Critical Process	
Key Practice Activity Not Executed	**How the Plan Addresses the Activity**
Activity 2: Each IT investment board operates according to written policies and procedures in the organization-specific IT investment process guide.	While the Plan does not provide the specific written policies and procedures that the investment boards must follow, it does indicate that further development of these policies and procedures are necessary. Additionally, the Post-Implementation Review of the select phase of the ITIM pilot test recommends that additional policies and procedures be developed in a document that is independent of the Plan. Once the FBI's ITIM policies are completely developed, this key practice can be executed when the FBI rolls-out the control and evaluate phases of the ITIM process.

Source: OIG analyses

IT Project Oversight Critical Process	
Key Practice Activity Not Executed	**How the Plan Addresses the Activity**
Activity 1: Each project's up-to-date cost and schedule data are provided to the appropriate IT investment board.	The Plan stipulates that the functioning project management office will review status reports on cost, schedule, and performance measures. The project management office will then forward selected reports to the boards for review.
Activity 2: Using established criteria, the IT investment board oversees each IT project's performance regularly by comparing actual cost and schedule data to expectations.	The Plan states that the Project Oversight Committee will ensure that selected projects are meeting performance measurement objectives, risks are being appropriately managed, budgets and schedules are on track, and resource levels are adequate.
Activity 3: The IT investment board performs special reviews of projects that have not met predetermined performance standards.	According to the Plan, the Project Oversight Committee will perform special reviews of projects whose status reports are not meeting predetermined performance standards.
Activity 4: Appropriate corrective actions for each under-performing project are defined, documented, and agreed to by the IT investment board and the project manager.	The Plan states that the Project Oversight Committee will review a portfolio status report to determine if quick corrective actions can be executed to get under-performing projects back on track. When this is not possible, appropriate recommendations will be made to the Executive Review Board.
Activity 5: Corrective actions are implemented and tracked until the desired outcome is achieved.	The Plan gives the Project Oversight Committee the responsibility to ensure that corrective actions are implemented.

Source: OIG analyses

IT Project and System Identification Critical Process	
Key Practice Activity Not Executed	**How the Plan Addresses the Activity**
Activity 1: The organization's IT projects and systems are identified and specific information about these projects and systems is collected in an inventory.	The Plan states that an IT investment portfolio will be built for development projects as the ITIM process is being pilot tested. An IT portfolio is expected to be completed for the full-blown ITIM roll-out during the FY 2005 budget cycle.
Activity 2: Changes to IT projects and systems are identified and change information is collected in the inventory.	FBI personnel told us that while there is not a written procedure to document changes to IT projects and systems, a policy will be developed when the IT asset inventory is complete. The IT asset inventory will then be updated as changes are made to IT projects and systems.
Activity 3: Information from the inventory is available on demand to decision-makers and other affected parties.	FBI personnel stated that the IT asset inventory, when complete, will be maintained on the FBI's Intranet, so that relevant information will be available on demand to decision-makers and other affected parties.
Activity 4: The IT project and system inventory and its information records are maintained to contribute to future investment selections and assessments.	FBI personnel stated that the IT asset inventory and IT portfolio, when complete, will be updated continually to become an archive of information to be used for future investment selections and evaluations.

Source: OIG analyses

Business Needs Identification Critical Process	
Key Practice Activity Not Executed	**How the Plan Addresses the Activity**
Activity 3: Identified users participate in project management throughout a project's life-cycle.	The Plan states that it is crucial for project team members (which must include identified users of the project) to work closely together throughout the project's life-cycle. These project teams support the functional project management office and Project Oversight Committee.

Source: OIG analyses

With the pilot testing of the select phase, the FBI further developed and refined the proposal selection process and provided training on proposal selection to ITIM users. The training materials supplemented and supported the documentation in the Plan to more clearly define the roles of ITIM users, such as IT investment review board members, project sponsors, and ITIM liaison representatives.

Even with these additional materials, the Post-Implementation Review of the select phase of the Plan (performed by the ITIM contractor) recommended that the FBI significantly expand its documentation of polices and procedures relating to the ITIM process by:

- explicitly defining the ITIM Program Office's roles and responsibilities so that resources can be concentrated on enabling and facilitating the process as well as supporting the development of process input;
- developing and documenting detailed policy, processes, and procedures in a stand-alone document independent of the Plan;
- developing a formal ITIM training program that includes focused training on the roles of various ITIM users, including board members and ITIM liaison representatives;
- developing a formal communications plan to ensure all ITIM users are provided with visibility and timely feedback from the ITIM process; and

- refining and expanding ITIM tools necessary to sustain the process, including an "IT investment proposal tracking management tool."[45]

The FBI recognized that the Plan was never intended to represent its final policies and procedures for its ITIM process. The Plan states that it provides a conceptual framework for achieving Stage Two maturity, and will evolve as the FBI's ITIM process advances to higher levels of maturity.

Without further development and refinement of the ITIM process, the FBI will have difficulty making additional progress in improving its IT investment management practices. Because the goal of Stage Two maturity is to build standardized methodologies for selecting and controlling IT investments, the FBI must have adequate documentation of these methodologies to make them repeatable and institutionalized. The Post-Implementation Review, prepared by the ITIM contractor, acknowledged the necessity for further developing and refining the Plan. In our judgment, the FBI must implement the recommendations set forth in the Post-Implementation Review prior to taking further action in pilot testing the control and evaluate phases of the ITIM process.

c. Recommendation

We recommend that the Director of the FBI ensure:

16. The recommendations set forth in the Post-Implementation Review relating to expanding the policies and procedures of the ITIM process are implemented.

(2) The Amount of Participation from ITIM Users in Developing the ITIM Process

In our judgment, the Plan was written with minimal input and coordination from relevant ITIM users. The main reason cited by

[45] According to the Post-Implementation Review, this tool would formally track and document the entire life-cycle of an IT investment proposal from the time the ITIM Program Office receives a concept paper to the time the final disposition is made.

IRD officials[46] for the limited participation from ITIM users was insufficient time allotted to develop the Plan. As a result, the institutionalization and buy-in[47] of the ITIM process may have been hampered.

a. Importance of ITIM User Participation in Developing the ITIM Process

Good management practices dictate that organizations involve relevant stakeholders when attempting to implement a new management process. This involvement aids in the institutionalization of the process. Institutionalization of the ITIM process is a key goal of the Plan, which states: "[The ITIM] process applies to ALL information technology projects, from ALL business units, from ALL funding sources, whether they be new, in development or operational."

Because of the broad applicability of the ITIM process, in our judgment the FBI should have involved representatives from throughout the Bureau when developing the Plan. In particular, individuals from the three divisions that manage major IT projects (the IRD, CJIS, and Laboratory Divisions) should have had substantial input into the creation of the Plan. Further, the Inspection Division's Major Project Management Oversight Unit (MPMOU) has a responsibility to oversee major projects in the Bureau, including IT projects, and thus should also have been involved in creating the Plan.

b. Results of Our Assessment of ITIM User Participation in Developing the ITIM Process

We found that relevant ITIM users from the IRD, CJIS Division, Laboratory Division, and Inspection Division were not given significant input into how the Plan was developed. Our interviews with IRD personnel indicated that the FBI gave the ITIM contractor the primary responsibility to write the Plan, without requiring significant participation from ITIM users in developing the initial draft of the Plan.

---

[46] The Information Resources Management Section, maintained within the IRD until February 2002, was directed to oversee the development of the FBI's ITIM process. In February 2002, the Information Resources Management Section was moved from the IRD to the Office of the Director. The ITIM Program Office was then formed within the Information Resources Management Section to oversee the ITIM process.

[47] According to the Framework, institutionalization and buy-in of the ITIM process is signified by ITIM users supporting and executing ITIM process activities.

Additionally, we determined that while the contractor interviewed numerous individuals from the IRD, it only interviewed two people from the Inspection Division, one person from the CJIS Division, and none from the Laboratory Division.[48] Further, as we discuss below, the enterprise architecture office (part of the IRD until February 2002) was not given adequate input into the development of the ITIM process. Also, the interviews that did occur outside of IRD mainly focused on the individuals' current responsibilities for managing IT investments, rather than their insights into how the new ITIM process could be shaped to best meet the needs of the Bureau. The following paragraphs provide the perspectives of ITIM users from the IRD, CJIS Division, Laboratory Division, and the Inspection Division.

Personnel from the enterprise architecture office told us that because the FBI's ITIM process had been developing concurrently with the enterprise architecture function, there should have been more coordination between the ITIM contractor and enterprise architecture office to increase effectiveness and reduce duplication of effort. For example, the enterprise architecture office drafted charters for a three-tiered IT investment review board structure, similar to what was ultimately written by the ITIM contractor. Additionally, the enterprise architecture office was preparing initiatives to improve the FBI's IT investment management practices. While the enterprise architecture office was drafting board charters and other processes designed to improve the FBI's IT investment management practices, the ITIM contractor, supervised by the ITIM Program Office, wrote the Plan without incorporating the work already accomplished by the enterprise architecture office.

Additionally, an individual from the enterprise architecture office told us that although he believed the ITIM process represents a positive step for the FBI, it must incorporate more involvement from the enterprise architecture function to ensure success of the process. He further stated that the IT investment review boards must rely more on the vast knowledge, expertise, and talents of FBI IT personnel prior to making decisions.

Further, according to a manager in the Information Resource Management Section, the Enterprise Architecture Technical Committee, which supports the Technical Review Board, has not been given the responsibility to ensure that IT proposals align with the

[48] The ITIM Program Office has the ultimate responsibility for directing the actions of the ITIM contractor.

mission of the FBI. The responsibilities of the Technical Review Board, as defined in the Plan, are focused on reviewing the technical risks of IT projects. These technical risks include compliance with the "technical architecture" or configuration management of the FBI, rather than the business architecture which shows how the business processes work together to satisfy the mission. The Plan and board charters assigned this responsibility to the Project Oversight Committee. In our judgment, because the responsibilities of the enterprise architecture office comprise both the technical and business architecture, the Enterprise Architecture Technical Committee should not only be responsible for assessing compliance with the technical architecture, but should also be responsible for assessing compliance with the business architecture. This added responsibility would provide greater assurance to FBI executives that IT proposals selected will enhance the Bureau's capability in achieving its mission.

An official from the CJIS Division told us that he was interviewed by representatives from the ITIM contractor on one occasion to determine what role the CJIS Division had in managing IT projects. However, he was not consulted on how the FBI's ITIM process should be created. He stated the only opportunity he had to comment on the Plan was after it was written in January 2002. His belief was that the ITIM Program Office was relying solely on the contractor to write the Plan, rather than building a Plan that has the input and buy-in from all FBI divisions.

While this official from the CJIS Division said to us that the Plan was an improvement over the FBI's current process for managing IT investments, he was not convinced that the process could be effectively implemented without addressing other pressing issues, such as the need for: (1) standardized methodologies in configuration management, quality assurance, and IT security; (2) improved support of contractors that work on IT systems; and (3) more representation of individuals with IT technical expertise on the IT investment review boards.

An official from the Laboratory Division's project management office told us that he first became aware of the Plan when training was announced for the new ITIM process in February 2002. Another official from the Laboratory Division told us that to his knowledge, no one from the Laboratory Division was consulted by the ITIM contractor prior to the preparation of the Plan. He told us that the Laboratory Division's current process was working fine and not in need of change.

Additionally, Inspection Division personnel, including individuals from the MPMOU, told us (as of June 2002) they were only consulted by the ITIM contractor as to how they acquired IT, not for their project oversight role.

An official from the Information Resources Management Section cited the insufficient amount of time allotted to prepare the Plan as the main cause for the limited involvement from ITIM users. As we previously mentioned, the FBI waited until December 2001 to engage the ITIM contractor to develop the Plan, despite learning of the DOJ's requirements to prepare a plan in January 2001. The ITIM Program Office Manager stated that the former Chief Financial Officer did not initially approve the use of an outside contractor to develop the Plan, causing a delay in hiring the contractor. The former Chief Financial Officer confirmed to us that there were initial concerns in using an outside contractor to develop a management process that affects how the IT budget is allocated and spent. Because the DOJ required initiation of the ITIM process during the FY 2004 budget cycle (which for the FBI begins in March), there was limited time between the development of the Plan (December 2001) and the initiation of the ITIM process (March 2002). In fact, the FBI only gave the contractor approximately two weeks to write the Plan because of the impending deadline to submit the Plan to JMD. As a result, FBI personnel told us that the ITIM contractor did not have ample time to include more ITIM users in the Plan's development.

While FBI officials from the Information Resources Management Section acknowledged the ITIM contractor's time constraints in developing the Plan, they also stated that the Plan is only a draft, and will be modified as the ITIM process is pilot tested. Additionally, because the three IT investment review boards established by the ITIM process include representatives from the major divisions that manage IT projects, officials from the Information Resources Management Section told us that there is significant opportunity for input into refining the ITIM process as it is being pilot tested.

Despite the Information Resource Management Section's position that the pilot test provides ample opportunity for input into refining the ITIM process, in our judgment, the ITIM Program Office, along with the ITIM contractor, continues to develop the ITIM process without incorporating sufficient input from relevant stakeholders. For example, a manager from the enterprise architecture office stated to us in July 2002 that the ITIM Program Office had not requested his participation during development of the control phase of the ITIM

process. This individual told us the enterprise architecture function should have a role in enhancing the control and evaluate phases of the ITIM process, but has not had the opportunity to demonstrate this role. Additionally, the process for the development of the control phase has not substantially changed from the select phase: the ITIM contractor, supervised by the ITIM Program Office, writes the policies and procedures which are then pilot tested by the ITIM users. In our judgment, this approach is not conducive to a process whose success depends on institutionalization and buy-in from ITIM users.

c. Summary

In our judgment, the lack of involvement by relevant ITIM users inhibits management buy-in to the ITIM process. If there had been more participation in the development of the Plan, some of the concerns stated above by key ITIM users might have been mitigated. The FBI must address these concerns to facilitate the institutionalization and buy-in the of the ITIM process, and ultimately improve its effectiveness.

d. Recommendations

We recommend that the Director of the FBI ensure:

17. The ITIM Program Office and the ITIM contractor incorporate the input from various ITIM users, including those from the enterprise architecture office, the CJIS Division, the Laboratory Division, and the Inspection Division as the control and evaluate phases of the ITIM process are being developed and refined. This input should be solicited through working group sessions scheduled on a periodic basis.

18. The ITIM process is modified so that the Technical Review Board and Enterprise Architecture Technical Committee perform a business architecture compliance review of IT project proposals to ensure these proposals support the mission of the FBI.

(3) The Project Management Function's Support of the ITIM Process

The FBI's project management function needs improvement to adequately support the ITIM process, especially in the control and evaluate phases of the process. The FBI recognizes the importance of upgrading the project management function. In particular, the Plan

states that the project management office must fulfill a critical role in supporting the Project Oversight Committee. In addition to the Plan, the FBI has taken other steps towards improving its project management function. Specifically, in June 2002, the FBI announced plans to create an Office of Programs Management. The Office of Programs Management will serve as a centralized project management office[49] that FBI officials from this office and the Information Resources Management section expect to play a key role in implementing the ITIM process. Despite the progress being made, the FBI still has critical areas to address, such as integrating a project management methodology with its ITIM process.

a. Relationship Between Project Management and ITIM

Numerous legislative mandates, including the Results Act and the Clinger-Cohen Act, require federal agencies to establish and maintain processes for managing systems throughout their life-cycle. These legislative mandates indicate that basic project management practices are essential if an organization is to ensure that its IT projects have established cost, schedule, and technical performance baselines that are monitored throughout the project's life-cycle. Additionally, project management is fundamental to supporting an ITIM process. In particular, the control phase of an ITIM process requires an organization to have a project management function. For example, IT project oversight, which encompasses basic project management practices, must be implemented for an organization to achieve Stage Two maturity. However, the Framework does not by itself provide a comprehensive model for how an organization should develop its project management function.

According to the Framework, an ITIM process is not a substitute for good project management. While an ITIM process takes an enterprise-wide focus, good project-level management forms the foundation for successful IT investments.

In our judgment, for the FBI's project management function to effectively support its ITIM process, the Bureau must have: (1) a fully operational centralized project management office whose responsibilities are directly integrated with the ITIM process, and (2) a standardized project management methodology that is

[49] In this context, a centralized project management office is independent of any division. As a result, the Project Management Executive, who heads the Office of Programs Management, reports to the Director.

integrated with the ITIM process. Because of the importance of these efforts, we assessed the FBI's progress in integrating these areas with its ITIM process.

b. Importance of a Centralized Project Management Office

The Plan recommends that project teams be staffed from a "pool" of managers and developers maintained in the project management office. These project teams would not be dedicated to solely one division, function, or application; instead, these teams would work on all types of IT projects across the Bureau. According to the Plan, this approach has many benefits, including:

- critical IT skills are available across all projects;
- personnel have more opportunities to work in multiple environments, which creates a richer, more interesting job environment;
- expertise across projects enhances and encourages the use of best practices; and
- managers are better able to assess IT personnel as they perform in multiple project environments.

We concur with the Plan's recommendations. Although the Plan does not specifically state that the project management office should be centralized (independent of any division), in our judgment, such a structure is most conducive to attaining the benefits listed above.

In addition to the above benefits, a centralized project management office can ensure that IT project teams are following a standardized project management methodology that is integrated with the ITIM process. In our judgment, this added control is especially important to the FBI since we previously concluded that the FBI's three main divisions that manage IT projects (the IRD, CJIS, and Laboratory Divisions) have not been consistently using a standardized project management methodology.

c. Importance of a Standardized Project Management Methodology

The DOJ recognized the importance of integrating project management with the ITIM process. In January 2001, it issued DOJ

Order 2880.3 to require components to manage IT investments in a way that demonstrates good stewardship, complies with applicable laws, and accomplishes the agency's diverse mission. Among its policies, the Order required each DOJ component to establish an ITIM process that is integrated with a structured system development life-cycle methodology. While the FBI is mandated to use the DOJ's System Development Life-Cycle methodology, we previously stated in this report that it has not been used consistently.

d. Results of Our Assessment of the FBI's Progress in Integrating its ITIM Process with the Responsibilities of a Centralized Project Management Office

As discussed below, we concluded that the FBI has recently made progress in integrating its ITIM process with the responsibilities of a centralized project management office. Not only does the FBI recognize the importance of this integration, but it has taken major steps towards incorporating the ITIM process with the responsibilities of a centralized project management office. This progress was evidenced by: (1) how the Plan defined the role of the project management function, and (2) the FBI's recent efforts to establish a centralized project management office.

The Plan recommends centralization of IT investment management through the use of IT investment review boards that have Bureau-wide oversight. Of the FBI's three IT investment review boards, the Project Oversight Committee has the primary responsibility for controlling IT projects. Additionally, the Plan calls for a project management office, a subcommittee of the Project Oversight Committee, to have discretion in managing IT projects Bureau-wide.

Specifically, the Plan defines how the primary responsibilities of the project management office must be integrated with the activities of the ITIM process, particularly during the control and evaluate phases. These responsibilities include:

- ensuring that resources, funding, and schedule timeframes are reasonable for each individual project;

- determining what staff and funding are needed for a project, and assigning staff and funding accordingly;

- providing advice and counsel to internal project teams in the execution of ITIM activities;

- providing a consistent set of project management tools and processes for ITIM projects;

- providing tools to project team members, such as Gantt charts, Pertt charts, and Microsoft Project;

- providing governing responsibility and oversight to day-to-day project managers; and

- determining whether project goals are achieved on time, on budget, and as designed.

We were told in June 2002 that the Director of the FBI approved the creation of a centralized project management office, whose chief executive would report to the Director.[50] This project management office, which would be independent of all other FBI divisions, would have the primary responsibility of managing projects in the Bureau. These projects would include, but not be limited to, information technology. The proposed mission for this new office is: "To assist the FBI in effectively managing, implementing, and deploying high-priority, complex and high risk development projects of high dollar value to successfully support the FBI's operational mission." To achieve this mission, this office will be:

- developing a repeatable process for the efforts described in the mission statement (defined above) and for training a skilled corps of FBI project management subject matter experts;

- advising on program management and acquisition-planning related organizational issues, proposals, and strategies;

- providing direct project management support in developing the crucial technology infrastructure for FBI investigation operations; and

- coordinating organizational resource allocation and management services and supporting the FBI's mission and priorities.

[50] The FBI is calling this office the "Office of Programs Management." As planned by the FBI, this office will be under the Director's office and independent of any division.

In addition, the Office of Programs Management has the following core functions for which it will ultimately be responsible: (1) system engineering, (2) schedule, (3) budget, (4) risks, (5) contract management, (6) certification and accreditation of IT systems, (7) configuration management, and (8) quality assurance.

In our judgment, the creation of the Office of Programs Management represents a critical first step towards centralizing the project management function and improving its effectiveness. Additionally, officials from the Information Resources Management Section and the Office of Programs Management have told us that they are working together to facilitate the integration of the responsibilities of the eight core functions listed above. The ITIM process needs the full support of the Office of Programs Management to implement the control and evaluate phases of the Plan. Therefore, in our judgment, the FBI should continue its efforts to integrate the responsibilities of the Office of Programs Management with the ITIM process. Specifically, a plan should be developed that outlines activities that must be performed to complete the integration, along with reasonable suspense dates. Additionally, this plan should provide the criteria and thresholds that the Office of Programs Management will use to select IT projects for review.

e. Results of Our Assessment of the FBI's Progress in Integrating its ITIM Process with a Standardized Project Management Methodology

We concluded that the FBI has not taken the necessary actions to integrate the ITIM process with a standardized project management methodology. While officials from the Information Resources Management Section have acknowledged to us that the ITIM process needs to be integrated with a standardized project management methodology, they have not taken sufficient action to ensure that these processes are integrated in a timely manner. This conclusion is evidenced by the Information Resources Management Section's lack of coordination with the Inspection Division's Major Project Management Oversight Unit (MPMOU), as previously reported in this section. Additionally, as discussed in the following paragraphs, the FBI risks duplicating efforts in managing IT projects if it implements the control and evaluate phases of the ITIM process without integrating these phases first with a standardized project management methodology.

To improve the FBI's ability to manage projects, including IT projects, the prior FBI Director requested that the MPMOU establish a standardized project management methodology for Bureau-wide use. In October 2001, the MPMOU completed the Project Management Process and submitted it to executive management for approval. The Project Management Process, which incorporates the DOJ's System Development Life-Cycle methodology, provides a framework that encompasses all phases of a project's life-cycle, including planning, developing, support, and disposal.

Personnel from the MPMOU stated to us that the Project Management Process provides a mechanism to fulfill certain requirements of the ITIM process. Specifically, personnel from the MPMOU told us that the project management process facilitates the ITIM process by:

- providing documentation to support investment decisions that span the life-cycle of the IT investment;

- providing a select, control, evaluate approach to managing validated IT needs;

- providing quantifiable measurements for monitoring cost, schedule, and performance baselines and processes for identifying baseline breaches;

- providing an executive oversight forum for monitoring the management of IT investments; and

- acknowledging the interdependencies between cross-cutting processes.

According to MPMOU personnel, given their knowledge of the FBI's requirement to develop an ITIM process, they made repeated attempts beginning in 2001 to work with individuals from the Information Resources Management Section to develop these processes concurrently.

In November 2001, personnel from the MPMOU prepared a presentation entitled "Project Management Process Compatibility with the ITIM Process" to show appropriate individuals from the IRD the similarities between the two processes. However, according to MPMOU personnel, individuals from the IRD who were managing the development of the ITIM process never gave MPMOU the opportunity

to make their presentation. In April 2002, after the development and initiation of the ITIM process, the MPMOU sent an electronic communication to the Director's office explaining the need to integrate these processes. The electronic communication stated that integration of these processes would improve efficiencies, streamline reporting and paperwork requirements, and improve the FBI's compliance with applicable regulations, including DOJ Order 2880.3. As of June 2002, no additional action had been taken by the Information Resources Management Section to integrate these processes.

Despite the efforts by the MPMOU to integrate the two processes, the Information Resources Management Section (with the support of the ITIM contractor) developed and began implementation of the FBI's IT Investment Model and Transition Plan without attempting to integrate it with the Project Management Process. Until the FBI integrates these two processes, the FBI will not be in compliance with DOJ Order 2880.3. Additionally, the FBI will be unable to effectively implement the control phase and evaluate phases of the ITIM process. Further, the FBI risks inefficient use of resources as a result of the duplication of efforts that could occur if the FBI fails to integrate these processes. FBI officials from the Information Resources Management Section have acknowledged to us that they must integrate the control and evaluate phases of the ITIM process with a standardized project management methodology. Despite their recognition of this need, as of June 2002 they did not have the details of how or when this will occur.

f. Summary

Although the FBI has taken a critical first step in (1) centralizing its project management structure, and (2) incorporating the responsibilities of the Office of Programs Management with the ITIM process, the FBI must take further action in integrating its ITIM process with a standardized project management methodology. Without this further action, the FBI's project management function will not adequately support the ITIM process. Consequently, the FBI risks ineffective execution of its control and evaluate phases as well as inefficient use of resources in managing its IT investments.

g. Recommendations

We recommend that the Director of the FBI ensure:

19. The FBI prepares a plan that specifically details how the project management office will support the ITIM process. This plan should include the project management office's criteria and thresholds for: (a) selecting IT projects to manage, and (b) identifying projects that the Project Oversight Committee will review.

20. The FBI develops and implements a specific plan detailing how and when it will integrate the ITIM process with a system development life-cycle methodology such as the Project Management Process.

(4) The Enterprise Architecture Function's Support of the ITIM Process

The FBI's enterprise architecture function needs improvement to adequately support the ITIM process. The FBI has taken a critical first step in establishing an enterprise architecture framework with a limited amount of time and resources dedicated to this effort. Despite the progress being made, the lack of a fully developed enterprise architecture framework will hamper the FBI's ability to advance through the ITIM maturity framework.

a. Importance of Having Support from the Enterprise Architecture Function

Enterprise architecture is the organization-wide blueprint that defines an entity's functions and systems, including IT systems. It provides a comprehensive view (through models, narratives, and diagrams) of the interrelationships of an organization's operations and structures and how these structures align with the organization's mission. The Clinger-Cohen Act of 1996 recognizes the interrelationship between enterprise architecture and IT investment management by requiring federal agencies to develop an enterprise architecture.

In a review of enterprise architecture use in the federal government, the GAO stated in its February 2002 report:[51]

> The architecture describes the enterprise's operations in both (1) logical terms, such as interrelated business processes and business rules, information needs and flows, and work locations and users, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. It provides these perspectives both for the enterprise's current or "as is" environment and for its target or "to be" environment, as well as a transition plan for moving from the "as is" to the "to be" environment. Enterprise architecture development, implementation, and maintenance is a basic tenet of effective IT management. Managed properly, these architectures can clarify and help optimize the interdependencies and interrelationships among an organization's business operations and the underlying IT infrastructure and applications that support these operations. Employed in concert with other important IT management controls, such as portfolio based capital planning and investment control practices, enterprise architecture frameworks can greatly increase the chances that organizations' operational and IT environments will be configured in such a way as to optimize mission performance. Our experience with federal agencies has shown that attempting to modernize information technology environments without an enterprise architecture to guide and constrain investments often results in systems that are duplicative, not well integrated, unnecessarily costly to maintain and interface, and ineffective in supporting mission goals.

[51] See "INFORMATION TECHNOLOGY: Enterprise Architecture Use Across the Federal Government Can Be Improved" (GAO-02-6).

According to the Framework, achieving IT investment maturity depends not only on implementing the ITIM critical processes, but also on other good management attributes such as the effective use of human capital, training, enterprise architecture, and software management. Specifically, an established enterprise architecture supports the ITIM process by facilitating an organization's advancement through the maturity stages of the Framework.

Achieving Stage Two maturity requires an organization to, among other things: (1) identify its IT projects and systems; (2) identify its business and user needs; and (3) select IT projects that align with those business and user needs. An organization's enterprise architecture would assist in the implementation of this critical processes by identifying the needs between the entity's current IT systems and processes and its target or future IT system environment.

Achieving Stage Three maturity[52] is dependent on a functioning enterprise architecture framework. The Plan states that to advance to Stage Three maturity, the FBI will a need a formal enterprise architecture committee to assess the IT portfolio for enterprise architecture compliance.

Achieving Stage Four maturity requires further integration of the enterprise architecture function with the ITIM process.[53] The Plan states that the FBI will have to completely integrate its enterprise architecture framework to enhance the management of its IT portfolio.

To respond to the importance of developing and overseeing enterprise architecture management in the Federal government, the GAO developed a maturity framework for enterprise architecture management that can be used in determining agencies' development, implementation, and maintenance of these architectures. The maturity framework, developed in 2001, is based on the core elements necessary for an organization to achieve effective enterprise architecture management. These core elements are arranged into a

[52] According to the Framework, Stage Three maturity is managing IT investments as a complete portfolio.

[53] According to the Framework, Stage Four maturity is improving the investment process through process evaluation techniques that focus on enhancing the performance and management of the organization's IT investment portfolio.

series of five hierarchical stages based on the implicit dependencies among these elements. This framework is consistent with other maturity frameworks, including the ITIM framework. The framework's five stages of enterprise architecture management maturity are described in Appendix 5 of this report.

To assess the status of federal agencies' efforts to develop, implement, and maintain enterprise architectures, the GAO surveyed 116 agencies (including the FBI) in 2001 using a questionnaire that was based on the core elements of the enterprise architecture maturity framework. The GAO published the results of this survey in its February 2002 report on enterprise architecture ("INFORMATION TECHNOLOGY: Enterprise Architecture Use Across the Federal Government Can Be Improved"). The GAO indicated in the report that of the 116 agencies surveyed, 98 reported meeting the minimum criteria necessary for Stages One or Two — creating enterprise architecture awareness or building an enterprise architecture management foundation. In contrast, only five agencies reported satisfying the practices that GAO stated are needed to effectively manage enterprise architecture activities (Stages Four or Five).

The results of the GAO survey, completed by the FBI in July 2001, indicated that the FBI is in Stage One of the enterprise architecture maturity framework.[54] According to the GAO, Stage One maturity is characterized by either no plans to develop and use an enterprise architecture, or plans and actions that do not yet demonstrate an awareness of the value of having and using one. While stage one agencies may have initiated some enterprise architecture core elements, these agencies' efforts are inconsistent and unstructured, and do not provide the management foundation necessary for successful enterprise architecture development.

Specifically, the GAO reported that the FBI needed to fully establish the management foundation that is necessary to begin developing, implementing, and maintaining an enterprise architecture. While the FBI implemented most of the core elements associated with establishing the management foundation, it had not yet established a steering committee or group that has responsibility for directing and overseeing the development of the architecture.

[54] The FBI's survey results are depicted in Appendix 6 of this report.

In addition, the GAO indicated that although establishing the management foundation is an essential first step, important further steps still need to be taken for the FBI to fully implement the set of practices associated with effective enterprise architecture management. These include having a written and approved policy for developing and maintaining the enterprise architecture and requiring that IT investments comply with the architecture.

We determined that the FBI's enterprise architecture function does not adequately support its ITIM process. Although the enterprise architecture office has provided support to the ITIM process during the pilot test of the select phase, this support needs to be enhanced. Our conclusion is based on the FBI not having a fully established enterprise architecture.

b. Results of Our Assessment of the FBI's Progress Towards Fully Establishing an Enterprise Architecture

We concluded that although the FBI has not fully established an enterprise architecture, it is taking important steps to establish one. Specifically, personnel from the enterprise architecture office told us that a baseline architecture is being developed in a data repository, which will ultimately be maintained on the FBI's Intranet. This data repository, when complete, will describe how all of the FBI's IT systems align with the business processes of the Bureau. Additionally, the enterprise architecture office is developing a technical reference model that will outline the technical architecture of the Bureau's IT systems. Also, this office is creating a commercial off-the-shelf roadmap of all commercially available hardware and software that will comply with the FBI's technical architecture.

Despite the limited staffing of the enterprise architecture office, this office has made progress towards building a foundation for an enterprise architecture function.[55] Given the importance of enterprise architecture to ensure successful IT investment management, coupled with the size and complexity of the FBI's IT infrastructure, we concluded that additional staffing and management attention to this area is warranted.

[55] As of July 2002, the FBI had two full-time employees solely focused on enterprise architecture. We were told by officials in the Information Resource Management Section that there were two vacant positions for the enterprise architecture office that were expected to be filled.

Despite the progress of the enterprise architecture office, not having a fully established enterprise architecture framework hampers the ITIM process. As we previously mentioned, the ITIM process depends on enterprise architecture functions to fulfill critical processes in the Framework. An organization's enterprise architecture would assist in the implementation of each of these critical processes, none of which the FBI has implemented as of June 2002. The following paragraph describes several causes for the FBI not having a fully developed enterprise architecture framework that adequately supports the ITIM process.

Personnel from the FBI's enterprise architecture office told us that the FBI has only recently paid significant attention to developing an enterprise architecture. According to the GAO, the FBI's lack of attention to enterprise architecture is not much different from other federal agencies. Historically, agency executives have not fully understood the value of enterprise architectures. Therefore, these tools have lacked the executive sponsorship necessary to become a funding priority. In addition, human capital expertise in this area has been scarce at federal agencies. As a result, the risk is heightened that federal agencies will proceed with investment decisions without the benefit of this architectural context and will end up with systems that limit mission performance, often after a significant and unwise use of funds. Specifically, the GAO stated in its June 2002 testimony: "The successful development and implementation of an enterprise architecture, an essential ingredient of an IT transformation effort for any organization and even more important for an organization as complex as the FBI, will require, among other things, sustained commitment by top management, adequate resources, and time."

c. Summary

Because the FBI does not have a fully developed enterprise architecture, the FBI will have difficulty in achieving more mature IT investment processes such as managing its IT investments as a complete portfolio and improving the investment process through post-implementation reviews.

d. Recommendation

We recommend that the Director of the FBI ensure:

21. The FBI continues its efforts to establish a comprehensive enterprise architecture. The FBI must also develop and

implement a specific plan to integrate the ITIM and enterprise architecture processes, even as these processes are being further refined and developed.

(5) Summary of the FBI's Ability to Improve its IT Investment Practices

We determined that the FBI must take additional actions to improve its IT investment practices. Not only will these actions facilitate the building of an IT investment foundation (Stage Two maturity), but these actions will also be essential for any advancement beyond Stage Two. In summary, the FBI must:

- fully develop and document the FBI's policy and procedures for IT investment management, especially in the control and evaluate phases;

- increase the participation of ITIM users in developing and refining the ITIM process as the pilot test continues;

- integrate a standardized project management methodology with the ITIM process; and

- continue to develop an enterprise architecture framework.

The FBI's efforts in these areas are crucial for it to successfully improve its IT investment maturity, and ultimately enhance mission performance.

C. Trilogy Case Study

To determine how the FBI's IT investment management practices affected a major IT project, we performed a case study of the FBI's Trilogy project. In section A of this finding, we concluded that the FBI was not fully implementing any of the critical processes necessary for successful IT investment management, including the most fundamental critical processes that are associated with the Framework's Stage Two maturity. Because our analysis in Section A of this finding was made on an organizational level, in our case study we assessed how the FBI's non-implementation of Stage Two critical processes affected an individual project. Next, we examined the FBI's internal assessments of Trilogy. Finally, we assessed the FBI's ongoing deployment of new computer hardware, software, and networks to its field offices.

We selected Trilogy for our case study because it is currently the FBI's largest ongoing IT project, with $458 million in total appropriations as of June 2002. Trilogy's purpose is to upgrade the FBI's: (1) hardware and software or Information Presentation Component (IPC), (2) communication networks or Transportation Network Component (TNC), and (3) five most important investigative applications or User Applications Component (UAC). The IPC and TNC upgrades will provide the physical infrastructure needed to run the applications from the UAC portion. The UAC portion is intended to upgrade and consolidate 5 of the FBI's 42 investigative applications. Because there are 37 other investigative applications and approximately 160 non-investigative applications that Trilogy will not include, Trilogy is only a starting point toward upgrading the FBI's entire IT infrastructure.

When discussing the state of the FBI's IT systems and the benefits Trilogy could bring, one Special Agent-In-Charge told us that "Trilogy must improve the FBI's IT systems. There is just no other way that agents can continue operating with such limited abilities." A senior FBI official stated to the Senate Judiciary Committee in July 2002 that agents must go through 12 screens just to upload one document in ACS. She further stated that the process is even more difficult because "there's no mouse, there's no icon, there's no year 2000 look to it, it's all very keyboard intensive." While FBI officials stated that Trilogy is not intended to provide the FBI with a state-of-the-art IT system, it lays the technological foundation so that an effective information system can be built. The implementation of Trilogy is vital to enhancing the FBI IT infrastructure, and consequently to the FBI's mission performance.

(1) Evolution of the Trilogy Project

During the 1990's, the FBI recognized that its IT infrastructure was aging and in need of modernization. Since 1997, the FBI has proposed to Congress several projects intended to improve its IT infrastructure and office automation.

First, the Information Sharing Initiative (ISI), a four-year project with an anticipated cost of about $400 million, was presented to Congress in 1997. The project's purpose was to upgrade the FBI's critical hardware, software, and communications capabilities and thus facilitate the development and deployment of modern computer

applications. It also would have provided secure information sharing within the FBI, and to law enforcement agencies outside of the FBI.

In November 1998, the ISI was funded by Congress with FY 1999 appropriations. However, expenditure of funds was contingent on the approval of the implementation plan and a review of it by the OMB's IT Technology Review Board. Following the OMB's review of the ISI plan, the FBI made minor modifications to the requirements document and acquisitions strategy. By January 2000, the FBI was ready to award the ISI contract. However, the Senate and House Appropriation Committees had not approved the implementation plan. FBI officials told us that by 1999, Congress had become increasingly concerned with the FBI's ability to manage major IT projects on time and within budget. We were told by FBI officials that this loss of credibility was caused by previous large-scale FBI IT projects that experienced significant cost and schedule overruns. Particularly, those officials said that the Integrated Automated Fingerprint Identification System and National Crime Information Center both were completed millions of dollars over budget and years behind schedule.

Because of the FBI's poor track record of managing major IT projects within cost and schedule, Congressional committees recommended that the FBI utilize a pilot implementation concept for ISI, which would modernize the IT infrastructure in phases. FBI officials said they resisted this concept because of concerns over having two sets of infrastructures, one old and one new. As a result, the FBI abandoned the ISI initiative.

In the Spring of 2000, the FBI prepared a project plan called eFBI, which was essentially a scaled back version of ISI. Because the project was less costly, FBI officials hoped that Congress would be more receptive to the project. The main difference between ISI and eFBI was that eFBI did not have the secure electronic information sharing capabilities included with ISI. However, press reports indicated that the FBI did not receive funding for the project when DOJ officials objected to certain proposed bidding procedures.

Because these plans to upgrade the FBI's IT infrastructure were never approved, the FBI's IT infrastructure had not received meaningful improvements since the early 1990's. As a result, there was an increasing need for a Bureau-wide IT upgrade. According to FBI documentation, by September 2000:

- more than 13,000 of the desktop computers utilized by the FBI were 4 to 8 years old and could not run modern software;

- the communications capability (networks) between and within FBI offices was up to 12 years old;

- most of the network components being used were no longer manufactured or supported;

- most Resident Agency offices were connected to the network at speeds equivalent to a 56k modem;

- Special Agents were unable to reliably e-mail each other on case specific information and often resorted to faxes; and

- Special Agents were unable to electronically communicate information to the U.S. Attorney Offices, other federal agencies, and state and local law enforcement agencies.

Recognizing its credibility problems with Congress, in July of 2000, the FBI hired a new chief information officer from the private sector to outline IT management. The new chief information officer was tasked with submitting another major technology upgrade plan to Congress. That plan, called the FBI Information Technology Upgrade Plan (FITUP), was drafted and delivered to Congress in September 2000. The FITUP was intended to achieve goals similar to the ISI and eFBI projects. FBI officials told us that Congress appeared more satisfied with the FBI's new IT management team, and consequently appropriated $379.8 million in November 2000 to fully fund the FITUP over a three-year period.

The objectives of the FITUP, as defined by the FBI, were to:

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

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

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

In November 2000, the FITUP was renamed Trilogy. A brief description of Trilogy's three components (IPC, TNC, and UAC) follows.

The IPC refers to how users see and interact with information. The IPC provides new desktop computers, servers, and commercial-off-the-shelf office automation software, including a web-browser and e-mail to enhance usability by the agents. The original Trilogy plan also included the use of thin-client desktop computers. Thin-client desktop computers, according to the FITUP, utilize application software that is run from the server computer, and consequently permits the desktop computer to function with fewer hardware resources such as processors and memory. Other benefits to the thin-client strategy included less maintenance of software in field offices and timely technology upgrades to meet user needs. The FITUP further stated that the FBI sized the departmental servers to handle the processing demands imposed by the thin-client strategy.

The TNC is the complete communications infrastructure and support to create, run, and maintain the FBI's networks. It is intended to be the means by which the FBI electronically communicates, captures, exchanges, and accesses investigative information. The TNC includes high capacity wide-area and local-area networks, authorization security, and encryption of data transmissions and storage.

The FBI combined the IPC and TNC portions for continuity when it requested contractor support, as both encompass physical IT infrastructure enhancements. The contractor for the IPC/TNC portions was signed in May of 2001. The originally scheduled completion date for these components was May 2004.

The UAC defines software-based capabilities and functions that Special Agents can use to access and analyze the information they need. The UAC is intended to provide the FBI with:

- improved capabilities to communicate inside and outside the FBI;

- access to information from internal and external databases that is properly authorized using primarily commercial products;

- the capability to evaluate cases and patterns of crimes through the use of commercial and FBI-enhanced analytical and case management tools; and

- the ability to find information in FBI databases without having to know where it is, and to search all FBI databases with a single query through the use of intelligent search engines.

The UAC is also referred to as the Virtual Case File. The Virtual Case File is intended to replace ACS as the FBI's primary investigative application. The goal of the Virtual Case File is to reduce agents' reliance on paperwork to improve efficiency. The Virtual Case File is supposed to have multi-media capability that will allow agents to scan documents, photos, and other electronic media into the case file. A separate contractor was hired in June 2001 to complete the UAC portion of Trilogy by June 2004.

(2) Accelerated Deployment of Trilogy

Even before the terrorist attacks on September 11, the FBI was looking for ways to accelerate the three-year Trilogy project, given the FBI's urgent need for improved IT infrastructure. In its Quarterly Congressional Status Report for the period between May 14, 2001 and July 6, 2001, FBI personnel stated that it had devised a plan to complete the IPC/TNC deployment in June 2003, nearly one year ahead of schedule, while the UAC deployment remained a three-year project. However, FBI officials stated they wanted to accelerate deployment of UAC.

After the terrorist attacks on September 11, 2001, the urgency of completing Trilogy increased. The FBI continued to explore options to accelerate the deployment of all three components of Trilogy. The FBI informed Congress in its February 2002 Quarterly Congressional Status Report that it devised a new plan with the contractor to complete the deployment of the IPC/TNC phases by December 31, 2002, which was nearly 18 months earlier than the originally planned completion date. Additionally, the FBI's February 2002 report stated that the contractor for the UAC phase developed a plan to make ACS web-enabled by July 2002. Web-enablement of ACS[56] was designed to put ACS in a multi-media format prior to the completion of the UAC phase in July 2004. According to its Congressional reports, the FBI could make these enhancements to Trilogy without any net increases to the project costs. The FBI would only need to have a portion of the funding earmarked for FY 2003 available by October 30, 2002.

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

The FBI also informed Congress in its February 2002 report, that with an additional $70 million funding for FY 2002, the FBI could further accelerate the deployment of Trilogy. This acceleration would include completion of the IPC/TNC phase by July 2002 and rapid deployment of the most critical analytical tools included as part of the UAC phase.

Congress supplemented Trilogy's FY 2002 budget with $78 million from the Emergency Supplemental Appropriations Act of January 2002 to expedite the deployment of all three components. The Emergency Supplemental Appropriations Act increased the total funding of Trilogy from $379.8 million[57] to $457.8 million. According to Trilogy documentation, the FBI obligated about $231 million as of June 2002. Trilogy's budget by component, as of June 2002, is described in the following table.

[57] Of this amount, $107.55 million was identified by FBI management as funding offsets, or cost savings, from other operations that would be replaced by Trilogy.

Trilogy's Budget by Component

Component Area	FY	Original Plan	Revised Plan Including the Emergency Supplemental Appropriation Plan
	2001	$68.0	$65.7
	2002	$87.8	$184.8
	2003	$82.8	$37.6
TNC/IPC	Total	$238.6	$288.1
	2001	$24.7	$28.1
	2002	$46.6	$63.8
	2003	$47.9	$47.8
UAC	Total	$119.2	$139.7
Contractor Computer Specialists	Total	-	$8.0
	2001	$8.0	$8.0
	2002	$8.0	$8.0
	2003	$6.0	$6.0
Project Management	Total	$22.0	$22.0
Total		**$379.8**	**$457.8**

Source: FBI budget documentation

Congress's willingness to provide the FBI with additional funding after September 11 was not limited to Trilogy. The FBI saw an increase in funding of approximately 102 percent for IT projects from $352.8 million FY 2001 to $714 million in FY 2002.

The IPC/TNC infrastructure enhancements are being deployed in three phases in the accelerated plan. The first phase, called Fast Track, is the installation of Trilogy hardware in all of the field offices and some of the Resident Agencies. The Fast Track deployment consists of new network printers, color scanners, local area network upgrades, desktop workstations, and office automation software. FBI officials reported that by the end of April 2002, all of the 56 field offices had Fast Track completed.

We were told by FBI officials that following the completion of Fast Track, the next phase of deployment, referred to as Extended Fast Track, was initiated, and was still continuing as of June 2002. Under Extended Fast Track, the FBI: (1) installed servers and other

network components at field office and resident agency sites, and (2) deployed the hardware included under Fast Track to additional resident agency sites that were not included in the first phase. Also, the FBI intended Extended Fast Track to correct any shortfalls in the distribution of hardware to the field offices that occurred in the original Fast Track deployment.

The final phase of the deployment, called Full Site Capability, represents the complete infrastructure upgrade. This phase will provide the wide area network connectivity together with new encryption devices, new operating systems and servers, and new and improved e-mail capability. According to June 2002 Congressional Testimony, Full Site Capability is expected to be completed in March 2003.

The UAC portion is also going to be deployed in two phases in the accelerated plan, release one and release two. The initial Virtual Case File release will migrate data from the current ACS and IntelPlus to the Virtual Case File. The Virtual Case File will replace ACS and serve as the backbone of the FBI's information systems, replacing the FBI's paper files with electronic case files that include multi-media capabilities. The first release of Virtual Case File has a targeted completion date of December 2003. This release is intended to allow different types of users, such as agents, analysts, and supervisors, to access information from their desktop computers that is specific to their individual needs. This Virtual Case File release is also intended to enhance the FBI's capability to set and track case leads, index case information, and move document drafts more quickly through the approval process with digital signatures.

The second release is intended to upgrade three other investigative applications into the Virtual Case File. The second Virtual Case File release has a targeted completion date of June 2004. It is intended to provide agents with Audio/Video Streaming capability and content management capability. According to FBI documentation, content management should help agents access information from the FBI's data warehouse, regardless of where in the system the information was entered, providing a single query for all of the FBI's systems.

(3) Results of Our Assessment of Trilogy Against the Stage Two Critical Processes

The Framework provides the organization level processes necessary for effective IT investment management. As a result, the Framework's critical processes, and in particular the Stage Two critical processes, do not necessarily ensure that individual IT projects will be effectively managed. However, it does ensure that, at a minimum, basic selection and management control processes are in place.

As discussed in Section A of this finding, Stage Two builds the foundation for successful IT investment management by establishing basic IT selection and control processes for IT projects. Stage Two is defined by the following five critical processes:

- IT Investment Board Operation - the process for creating and defining one or more IT investment boards within the organization;

- IT Project Oversight - the process whereby the organization monitors all projects relative to cost and schedule expectations;

- IT Project Identification - the process by which the IT inventory is created and maintained to provide asset tracking data to executive decision-makers;

- Business Needs Identification - the process of identifying the business needs and the associated users that drive each IT project; and

- Proposal Selection - the process establishing defined processes used by an organization to select new IT project proposals.

Our assessment of how Trilogy was managed in relation to each Stage Two process is described in the following paragraphs.

a. IT Investment Board Operation

According to the Framework, IT investment boards have executive decision-making authority throughout the organization. This organization-wide perspective is necessary to ensure that only the best

projects are selected for development, and projects under development are being monitored with consistent policies and controls.

In section A of this finding, it was noted that the FBI did not have IT investment boards operating prior to March 2002. Because Trilogy was initiated in September 2000, it was not selected through the operation of formal IT investment boards. Additionally, because the FBI's IT investment boards were not involved in overseeing IT projects as of June 2002, Trilogy has not been subjected to board oversight.

FBI officials have told us that most of Trilogy's development has been managed in a "stovepipe." One FBI official told us that the organization's focus on Trilogy has drained the FBI of a broader view of IT. As a result, FBI personnel not involved in the management of Trilogy had little knowledge of the project's status and progress. Although the Trilogy management structure has changed frequently, it was managed out of the IRD until March 2002. However, IRD personnel who were responsible for acquiring IT products and services through contractors on IRD IT projects were not involved in Trilogy's acquisitions. Only members of the Trilogy management team performed these activities. Further, FBI personnel told us there was little coordination taking place with Trilogy management and contract specialists from the Finance Division or the IRD's unit responsible for procurement of non-Trilogy IT needs. Because of the lack of coordination, there is a heightened risk that resources could be spent on potentially duplicative or non-compatible hardware, software, and systems. FBI officials have told us that the IRD is in the process of developing technical enterprise architecture that incorporates Trilogy requirements to mitigate this risk.

b. Project Oversight

The GAO Framework states that IT investment boards should monitor all projects relative to cost, schedule, and technical baselines to measure the progress of IT projects under development, and the performance of projects upon deployment. When an IT project is not performing according to expectation, the investment boards should seek corrective actions to be taken.

IT investment boards have not been involved in overseeing Trilogy. In our judgment, the lack of project oversight from IT investment review boards contributed to the FBI not having

established schedule, cost, and technical baselines for Trilogy, as of June 2002.[58]

In terms of a cost baseline, FBI officials told us that the rapid procurement and deployment of Trilogy has prevented the project managers from performing earned value management,[59] as promised in the FITUP. While FBI officials were confident they know how much money has been spent on Trilogy to date, and how much funding has been committed, they have less assurance as to whether Trilogy is on budget, over budget, or under budget.

A schedule baseline for Trilogy has never been well-established. First, FBI officials said they would complete IPC/TNC deployment in May 2004. Then, they said it could be finished in June 2003. Next, they said it would be finished by December 2002. After receiving $78 million of supplemental funding, they said it would be done by July 2002. Then, they said they could not make the July 2002 deadline and moved it to October 2002. As of June 2002, FBI officials have said deployment will probably not be complete until March 2003. Also as of June 2002, the FBI was still in the process of building a comprehensive schedule of Trilogy milestones.

In terms of a technical baseline, we previously stated that the FBI is still developing a technical architecture framework that includes Trilogy hardware and software. Personnel from the enterprise architecture office initially told us at the beginning of our audit that they were not significantly involved in ensuring that Trilogy acquisitions were compatible with non-Trilogy hardware and software. But, as of June 2002, the enterprise architecture office had developed a technical reference model, although it was not finalized.

According to the FITUP, the philosophy employed in implementing Trilogy was "to get 80% of what is needed into the field now rather than 97% later. Then we can proceed in an orderly fashion to move toward 100% in the future." Additionally, after the events of September 11, the urgency to deploy Trilogy as quickly as possible increased. FBI management told us that risks associated with this rapid deployment were accepted. Further, they stated that given the

[58] Cost baselines establish the specific cost of equipment or user-applications delivered. Schedule baselines establish when equipment or user-applications would be delivered. Technical baselines establish the enhancements made to systems.

[59] Earned value management is comparing the value of products and services received with funds that have been expended.

accelerated schedule, and additional funding needed, the cost and schedule baselines could not be static.

While the events of September 11, 2001 affected the FBI's ability to manage cost, schedule, and technical baselines, we believe the risks of not establishing such baselines puts the project at a high risk of failure. Although the overall success of Trilogy will not be determined for years to come, the FBI has already missed the July 2002 deadline to complete the IPC/TNC phase. In our judgment, this missed deadline is a further indication that increased oversight of the project is needed.

The new Trilogy project executive, hired in March 2002, has taken a different approach to managing Trilogy. She has emphasized the importance of having more structured oversight of the project. She has been developing a comprehensive schedule for all three components. Additionally, she has indicated that there are limitations to how fast Trilogy can be deployed, without risking the security of the system. In our judgment, while these actions since March 2002 represent positive changes to Trilogy's project management function, the project's completion time, final cost, and ultimate performance remain uncertain. Also, we concluded that for the Trilogy project management function to be effective, it must include oversight from IT investment review boards to provide much needed monitoring.

c. IT Project and System Identification

According to the Framework, IT project and system identification provides essential information to an organization as to how its IT assets (such as personnel, systems, applications, hardware, software licenses, etc.) are configured and relate to one another. Having a complete inventory of the organization's IT assets, including documentation of the configuration and technical architecture of IT systems, helps ensure that IT investment review boards will select projects that comply with the existing architecture in place. Additionally, this process can be equated with an organization having a blueprint of what systems it utilizes, how those systems were created, and what can be done to enhance those systems.

As noted in section A of this finding, we found that the FBI did not have a comprehensive inventory of all IT assets, including complete documentation of the technical architecture of its systems. Because the UAC portion of Trilogy is focused on making significant changes to, or possibly complete replacements of, five of the FBI's

investigative systems, having documentation of the exact configuration of these systems is critical to designing the requirements for UAC. According to a senior FBI official, the FBI must know what it has before it can define the right solution to fix the problem. Not having the documentation of the configuration of these five investigative systems has caused the FBI to engage in a process of reverse engineering, which is trying to determine the structure and components of the systems after deployment. Because the FBI has to perform reverse engineering on the FBI's five investigative systems that will be migrated to the Virtual Case File, there are limitations as to how rapidly UAC can be developed and deployed.

As of June 2002, the FBI was still defining the requirements for UAC because of the reverse engineering activities. Without knowing the exact requirements, the FBI will have difficulty establishing cost and schedule baselines for this component of Trilogy. As a result, some FBI officials told us that they believe the UAC portion of Trilogy is at significant risk of not being completed on schedule (in June 2004) or within budget.

d. Business Needs Identification for IT Projects

According to the Framework, an organization should have a systematic process for identifying, classifying, and organizing its business needs and the IT projects used to support these needs. This process should allow for the identification and definition of the business needs and specific users for all IT projects. This process can be equated with knowing where the organization wants to go, based on its mission, and the needs of its users to pursue that mission. While we concluded that the Trilogy project's users were identified, since all users of the FBI's systems will be affected by the IPC/TNC portion of the project, we found that the specific needs of the users, and of the FBI as a whole, were not adequately defined before Trilogy was selected and funded.

Specifically, we found that the requirements for the applications of the UAC portion were still being defined as of June 2002. Since January 2002, the FBI and the contractor were participating in a Joint Application Development planning process to define and prioritize the users' operational requirements. This process brings users, designers, and future systems operators together to develop the applications in order to better establish operable and maintainable systems.

The Joint Application Development sessions represent a thoughtful and productive approach to ensuring that the UAC portion of Trilogy will adequately support agents' investigative activities. However, in our judgment, this process should have been initiated from the beginning of the Trilogy project.

e. Proposal Selection

According to the Framework, proposal selection activities ensure that the right projects are selected to support the organization's mission. The proposal selection process relies on the project and system identification process, as well as the business needs identification process, so that information contained within project proposals include sufficient documentation of the technical requirements of the projects.

While no investment boards existed at the time of Trilogy selection, it has been widely recognized by the Attorney General, FBI Director, and Congress that an investment in the upgrade of the FBI's information technology was essential to the FBI meeting its mission goals. The FBI's technology was outdated in terms of hardware, software, user-applications, connectivity, and data sharing abilities. There is little question of the FBI's need to select this project. However, successful execution and deployment of the project depends on having the other control processes in place. Specifically, proposals should have adequate documentation of technical requirements and project risks.

We were told that some aspects of Trilogy that were submitted to Congress did not turn out to be technically feasible. For example, FBI officials told us that the thin-client strategy was not pursued because it was found that this type of network could not be achieved given the technical requirements of the FBI. Another example is web-enablement of the ACS, which was also discontinued when it was realized that it would require more resources than anticipated. Had a more rigorous proposal selection process been in place that required sufficient documentation of the technical requirements and risks of the project, the expending of time and resources on thin-client technology and web-enablement of ACS may have been minimized.

f. Summary

We have found that not implementing the critical processes associated with Stage Two maturity has contributed to missed

milestones and uncertainties associated with the remaining portions of Trilogy. However, the FBI's new Trilogy project executive has taken positive steps in establishing management controls and oversight to the project.

g. Recommendations

We recommend that the Director of the FBI ensure:

22. The IT Investment Review Boards initiate oversight of Trilogy, including:

    a. the establishment of cost, schedule, technical, and performance baselines; and

    b. tracking significant deviations from these baselines and taking corrective actions as necessary.

23. The technical requirements for Trilogy are adequately defined, documented, and shared with other IT users.

(4) The FBI's Internal Assessments of Trilogy

The FBI had three internal assessments performed concerning the management of the Trilogy project. These assessments were done by the FBI's Inspection Division, CJIS Division, and a contractor performing independent verification and validation work. The assessments found that the lack of baselines and general program oversight pose potential risks for the Trilogy program meeting its budget, schedule, technical, and performance goals. These assessments recommended that the FBI designate a program manager specifically for Trilogy, and that the program manager immediately take steps to establish baselines and requirements for the project.

The objective of our case study was to determine how Trilogy was being managed within Stage Two of the Framework. These assessments go beyond that objective and address additional areas of potential risk within Trilogy, such as security and configuration management. An overview of the three independent assessments (FBI Inspection Division Trilogy Risk Assessment, November 2001; Trilogy Independent Validation and Verification, December 2001; and CJIS Division Trilogy Assessment, January 2002) are presented in the following paragraphs.

a. Inspection Division Trilogy Risk Assessment

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

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

The MPMOU issued two follow-up letters to the Director in December 2001 and February 2002 to assess the FBI's progress in mitigating these risks and taking action on their recommendations.

In December 2001, the Inspection Division indicated that while Trilogy management acknowledged certain project risks, Trilogy managers were willing to accept aspects of those risks and move forward. However, personnel from the Inspection Division noted that FBI senior management did hire a program manager for Trilogy in March 2002.

In February 2002, Inspection Division personnel indicated that there was then disagreement between them and Trilogy management on the level of project risk for Trilogy. The Inspection Division pointed to a CJIS review and an outside independent validation and verification report on Trilogy establishing that significant risks to the project exist, in the areas originally identified by the Inspection Division. The Inspection Division then reiterated its previous recommendation that calls for the development of a short and long-term strategy for Trilogy. Inspection Division personnel told us that Trilogy management did not sufficiently develop a short and long-term strategy for the project as was recommended.

b. Trilogy Independent Validation and Verification

The IRD hired an outside contractor to obtain an independent perspective on Trilogy. The objective of the assessment was to determine the labor requirements, level of effort, and verification and validation tasks necessary to ensure that the Trilogy acquisition meets the requirements of FBI users into the future within the established schedule and budget.[60] The independent validation and verification report, issued in December 2001, disclosed risks in the Program Management of Trilogy, IPC/TNC portion, and the UAC portion of Trilogy, including a lack of program management structure and focus, a lack of formal requirements, schedules, and baselines, and changes in the UAC/IPC/TNC portions without formal changes to contracts. While we concluded that the FBI improved the Trilogy management structure through the hiring of a new project manager in March 2002, we believe that risks associated with lack of formal requirements, schedules, and baselines still remained as of June 2002.

c. CJIS Division Trilogy Assessment

Upon reviewing the Inspection Division risk-assessment, the Director requested the CJIS Division to perform an independent review of Trilogy to get another perspective on the project. The CJIS Division performed their assessment between January 3 and January 16, 2002. This assessment covered management, quality assurance, configuration management, IT security, administrative and technical requirements, and technical management. It found weaknesses similar to those identified by the Inspection Division, including a lack of clear lines of authority, no clearly designated Program Manager, a lack of authority and support in the areas of quality assurance, security, configuration management, and technical requirements, and insufficient technical reviews of Trilogy documentation. While we concluded that the FBI improved the Trilogy management structure through the hiring of a new project manager in March 2002, we believe there are still weaknesses in Trilogy's documentation of technical requirements as of June 2002.

d. Summary

The three internal risk-assessments on Trilogy found significant risks associated with the management of the project. In our

[60] Initial Independent Verification and Validation Analyses Technical Report was issued on December 7, 2001 by an outside contractor.

judgment, effective IT investment management practices, including active oversight from IT investment review boards would have mitigated these risks.

e. Recommendation

We recommend that the Director of the FBI ensure:

24. The Trilogy project managers prepare an action plan to address the risks identified by the three internal reports on Trilogy. This plan should include (a) actions already taken to mitigate these risks, (b) planned actions, including suspense dates, and (c) an explanation for why some risks cannot be mitigated, if applicable. The IT investment review boards should then approve this plan and monitor it for implementation.

(5) Deployment of Trilogy to Field Offices

In addition to assessing the Trilogy management at FBI headquarters, we assessed the Fast Track deployment of Trilogy to five of the largest FBI field offices: (1) New York, (2) Washington, D.C., (3) Los Angeles, (4) Miami, and (5) Chicago. Our objectives were to assess the Fast Track deployment in terms of timeliness, support, and completion. Our goal was to identify current problems and recommend corrective actions, and discuss "lessons learned" for future system deployments.

In her July 16, 2002 Congressional testimony before the Senate Judiciary Committee, the FBI Project Management Executive stated that the Fast Track deployment involved the installation of Trilogy architecture at the FBI's 56 field office locations. The installation also included as many Resident Agencies as could be completed before the second phase of the deployment ("Full Site Capability") begins. This architecture consists of new network printers, color scanners, local area network upgrades, desktop workstations, and Microsoft office applications. She also stated that by the end of April 2002, deployment at all 56 FBI field offices was completed, and that Fast Track is continuing to deploy this architecture to the FBI's Resident Agencies.

a. Timeliness of the Fast Track Deployment

The Fast Track deployment to the five field offices in our survey began as early as December 2001. The FBI Project Management

Executive stated in her testimony that "By the end of April 2002, deployment at all 56 FBI field offices and two Information Technology Centers was completed. Fast Track is continuing to deploy this infrastructure to our resident agencies." During our testing at five FBI field offices in June 2000, we found that implementation activities were still ongoing to correct deficiencies that occurred during the original Fast Track deployment. The FBI Project Management Executive told us that her testimony was limited to "Fast Track" and did not include ongoing activities related to "Extended Fast Track."

Regarding the Resident Agencies, FBI employees informed us that as of June 2002, deployment to the Chicago, Los Angeles, and District of Columbia Resident Agencies was underway or completed. Deployment to the Miami Resident Agencies was scheduled for August 2002, and deployment to the New York Resident Agencies was still in planning.

Regarding installation of the basic Trilogy architecture by the contractor, employees from all five field offices said the timing of the architecture installation phase of the deployment occurred either on schedule or ahead of schedule.[61] Most employees interviewed (ten of eleven) said they were provided ample notice for the timing of the installation. A Telecommunications Manager in the Chicago Field Office said it was one of the FBI's smoothest "rollouts." Personnel from the Los Angeles Field Office indicated that through careful preparation they cut the installation phase from the three weeks scheduled to just seven days. Apparently, only the New York Filed Office experienced significant problems with the installation phase of the deployment. Specifically, the financial management system was left inoperable and they had to resort to pre-Trilogy processing to pay employees. Also, the FBI Intranet traffic was not reaching the FBI mainframe computer because of information being routed through too many pathways.

b. Adequacy of FBI Headquarters Support for the Fast Track Deployment

Regarding FBI Headquarters support, most employees we interviewed said they were provided with adequate planning and preparation instructions for the deployment. Employees from the

[61] Although the timing of the installation phase occurred as scheduled, the Extended Fast Track deployment to all five Field Offices was still ongoing as of June 2002. As discussed later, for two of the Field Offices additional installation work remained to be completed, and for four of the Field offices hundreds of desktops still remained to be delivered.

New York Field Office said FBI Headquarters did not provide instructions but instead informed them to send a team to Miami to learn about the deployment, and then return to New York to plan and prepare for it. As to whether there was sufficient communication between FBI Headquarters and the field offices, four of nine employees who responded indicated that communication could have been better to adequately prepare the field offices for deployment.

Six of eleven employees who responded did not believe the FBI's deployment strategy appropriately considered the individual needs of the field offices. Personnel from the Chicago Field Office indicated that since they had little opportunity to provide input, they had to work around the information and changing timelines received from FBI Headquarters. A supervisory computer specialist from the Los Angeles Field Office indicated the deployment was successful, in part, because they did not use the timeline provided by FBI Headquarters. Personnel from the Miami Field Office said they provided considerable information to the contractor during the survey phase that was subsequently lost. A supervisory computer specialist from the District of Columbia Field Office indicated concern that because offsite locations were not considered, there were an insufficient number of computers to deploy.

c. Adequacy of Contractor Support for the Fast Track Deployment

Eleven of the twelve employees we interviewed told us that the subcontractor for the actual installation work at the field offices was very helpful. Employees generally indicated that the subcontractor was technically competent and professional.

Regarding support from the contractor's service support center, of ten employees who responded, three employees said they did not use the service, five employees said the support provided was inadequate, and only two said the support was helpful.

- The three employees who did not use the support center were all from the Los Angeles Field Office. They indicated that personnel in their field office were aware of the service, but so far had no need to use it.

- The five employees who said the service was inadequate said that employees who worked at the center had little technical background and had to assign callers "ticket numbers" and refer

the calls to technicians. Often, the calls were not returned. When the calls were returned, it was usually several days later and often for the wrong ticket number. New York Field Office personnel became so frustrated with the service that FBI Headquarters eventually granted approval for them to call the computer manufacturer directly.

Part of the Fast Track deployment planning included the contractor conducting surveys at the field offices and resident agencies to identify existing equipment and installation requirements. The surveys were conducted in the third and fourth quarters of 2001. Regarding the accuracy of the survey work performed by the contractor, five of the nine employees who responded to our question said the surveys did not accurately identify the computer needs of personnel at the field offices.

- The Chicago Field Office personnel answered the contractor survey based on their understanding that the deployment would be a one-for-one exchange, or one new computer to replace each existing computer. Field office personnel said that FBI Headquarters later decided every employee would receive a computer, which resulted in revising the deployment plans.

- New York Field Office personnel also answered the survey based on their understanding that the deployment would be a one-for-one exchange. As a result, they indicated that the only squad where everyone had a computer was the one working on the investigation of the September 11, 2001 terrorist attacks.

- Los Angeles Field Office personnel indicated that the contractor only considered replacement of old equipment and did not obtain an adequate understanding of the full scope of the deployment. They indicated that as a result, the deployment was not fully completed because of a shortage of 12,000 feet of fiber-optic cable.

Of nine employees who responded to our question regarding accessibility of the contractor for equipment maintenance support, six indicated that the contractor was not easily accessible.

- Chicago employees said they had to wait as long as three weeks to receive replacement parts. To report a problem, they first had to call FBI Headquarters, who then relayed the problem to the contractor.

- The Miami Field Office indicated it could take weeks to get a question answered by the contractor.

- New York Field Office personnel also indicated that maintenance support was inefficient. Maintenance calls were often not returned. On one occasion, a contractor employee told them "everything was on hold because they had too many problems." Additionally, if a part needed replacing, the entire computer had to be shipped to the contractor, even if the problem involved a faulty floppy drive. Although FBI Headquarters allowed the New York Office to contact the manufacturer directly to resolve problems, they still had to call FBI Headquarters first so that calls could be logged.

- District of Columbia Field Office personnel stated that having maintenance performed off-site was unworkable. They also indicated that they had to ship computers to the contractor for maintenance, even if the problem involved a faulty floppy drive. This generally resulted in agents being without computers for about three weeks.

d. Adequacy of Training Support Provided to Field Office Personnel

All employees interviewed stated that training in MS Office 2000 applications and MS Outlook was generally available before, during, and after the Fast Track deployment. All interviewees said time was made available for agents to attend this training as well as additional computer-based training available on the FBI Intranet.

However, six of ten interviewees indicated that problems existed with the Learning Management System[62] available via the FBI Intranet. These six employees generally indicated that the system has not worked well from the beginning, that the system was down more than it was up, and that application problems existed.

- A telecommunications manager from the Chicago Field Office said that employees were unable to determine when classes were being held and that the system "was an embarrassment."

[62] The Learning Management System is a centrally-hosted, web-based training application available via the FBI Intranet and is designed to allow all employees to: (1) enroll in instructor-led classes, (2) access computer based training, (3) review training transcripts, and (4) access documentation libraries.

- Employees from the New York Field Office said the system was not used because of problems with the Trilogy training point-of-contact.

- A supervisory computer specialist from the District of Columbia Field Office said that although there were "major bugs" with the system, she was able to manually sort out the training timetable to ensure that all employees who desired training received it.

e. Completion of Fast Track Deployment

Based on the interview results, we concluded that the Fast Track deployment for all five field offices in our sample did not provide the quantities of the desktop computers that were expected. As a result, the FBI initiated Extended Fast Track to provide the desktop computers that were not originally provided with the Fast Track deployment. According to the FBI Project Management Executive, miscommunications between FBI Headquarters and the field offices resulted in differences between the number of desktop computers delivered by FBI Headquarters and the number of desktop computers expected to be received. Additionally, the FBI Project Management Executive said shortages of fiber optic cable resulted from these miscommunications, as some field offices budgeted for the wrong amount of cable. We found that as of June 2002 (the month our interviews were conducted), some field offices did not have sufficient quantities of fiber optic cable to complete the deployment and hundreds of desktop computers still remained to be delivered.

We did determine, however, that each desktop computer delivered included the complete baseline hardware and software package specified by the fast track deployment. Additionally, we randomly selected 30 Trilogy desktop computers received by each field office and verified that the desktop computers were received, installed, and operational.

For two of the five field offices we reviewed, additional installation work remained to complete the Fast Track deployment. At the Los Angeles Field Office, we were informed that about 40 percent of the Trilogy desktop computers were not connected to servers and networked because of the shortage of fiber optic cable. Additionally, although Los Angeles received the requisite number of Trilogy printers, none of these printers were operational because of the shortage of fiber optic cable. At the District of Columbia Field Office, we were

informed that only 3 percent of the Trilogy printers received were operational because the required fiber optic cables had not yet been installed.

Additionally, there appeared to be some confusion between FBI Headquarters and some of the field offices as to the actual number of Trilogy desktop computers to be deployed under Fast Track. As a result, four of the field offices had not yet received their full compliment of desktop computers as intended under the Fast Track deployment.

- Chicago Field Office personnel explained that FBI Headquarters initially informed them Fast Track would be a one-for-one exchange of old desktop computers for new desktop computers. Accordingly, they planned for a one-for-one exchange involving approximately 390 Trilogy desktop computers. However, the March 14, 2002 Electronic Communication (EC) indicated that the contractor was shipping 735 Trilogy desktop computers, one for each employee. Chicago Field Office personnel told FBI Headquarters that all they could accommodate at that time was 427 desktop computers, enough to accommodate a one-for-one exchange plus an additional ten percent.

- Miami Field Office personnel told us they received 556 desktop computers in January 2002. However, according to the March 14, 2002 Electronic Communication (EC) received 3 months later, the Miami Field Office was scheduled to receive 739 Trilogy desktop computers in January 2002.

- The March 14, 2002 EC indicated that the District of Columbia Field Office would receive 1,365 Trilogy desktop computers. However, the District of Columbia Field Office actually received 950. They indicated that 100 desktop computers would be deployed during the full implementation.

- The March 14, 2002 EC indicated that the New York Field Office would receive 2,101 Trilogy desktop computers, one for each person. New York Field Office personnel told us they received 1,245 desktop computers based on a one-for-one computer exchange and that the remaining desktop computers would be deployed during the full implementation.

f. Most Significant Obstacles to Fast Track Deployment

When asked to provide what they perceived to be the most significant obstacles to the Fast Track Deployment, personnel from the five field offices provided the following responses:

- Personnel from the Chicago Field Office stated that FBI Headquarters did not provide sufficient information prior to the deployment and did not inform them of changes in deployment planning. They also indicated that frequent turnover of personnel at FBI Headquarters made planning more challenging. They indicated that because of changing plans, FBI Headquarters required them to submit four separate surveys, three of which were subsequently lost by FBI Headquarters.

- Personnel from the Los Angeles Field Office indicated the contractor did not obtain sufficient input during survey work to understand the full extent of the deployment. Also, the contractor was rushed in completing the deployment. To complete the deployment, Los Angeles personnel had to perform some of the work themselves.

- Personnel from the Miami Field Office indicated that the on-site time to complete the installation phase of the deployment was too narrow.

- Personnel from the New York Field Office indicated that on-site technical personnel were not available to answer questions during survey work. Also, the contractor did not have sufficient time to complete the on-site deployment work.

- Personnel from the District of Columbia Field Office stated the contractor was rushed, and they had to do some of the contractor's work to expedite the deployment.

g. Limitations to Field Offices Fully Utilizing Trilogy Fast Track Capabilities

When asked what are the current limitations to utilizing Trilogy Fast Track capabilities, personnel from the five field offices provided the following responses.

- Chicago Field Office personnel stated that a shortage of fiber optic cable prevented them from making connections between

computers and building up the network infrastructure. Without the network infrastructure, they are unable to operate the system at full utilization.

- The Los Angeles Field Office indicated that funds were not available to buy required quantities of fiber optic cable to complete the deployment. Also, FBI Headquarters had not yet developed the macros for Microsoft Word. Further, although Los Angeles has trouble-shooting equipment for its existing application systems, no such equipment has been provided so far for Trilogy.

- The New York Field Office indicated that FBI Headquarters had not yet developed the macros for Microsoft Word.

- The District of Columbia Field Office indicated that it had yet to install the Trilogy printers. Also, FBI Headquarters had not yet developed the macros for Microsoft Word. As a result, agents were still using WordPerfect because of its nearly 1,000 FBI unique macros.

h. Summary

Based on the results of our work at the five field offices, the Extended Fast Track deployment was still ongoing as of June 2002. For two of the field offices, additional installation work remained to be completed, and for four of the field offices hundreds of desktop computers still remained to be delivered. A lack of clear communication between FBI Headquarters and the field offices contributed to the confusion over the number of desktop computers to be delivered and shortages of fiber optic cable. Additionally contractor maintenance support for the Trilogy architecture was inefficient, resulting in agents being without computers for weeks at a time. Improvements in agent and support personnel training, procurement of trouble-shooting equipment for the Trilogy architecture, and timely customization of word processing software will enhance user utilization of the Trilogy architecture.

(6) Recommendations

We recommend the Director of the FBI:

25. For future IT deployments, ensure that processes are established for field offices to submit input and receive feedback from FBI Headquarters prior to installing equipment.

26. Initiate action to remedy contractor deficiencies associated with inefficient: (a) operation of the service support center, and (b) maintenance support for Trilogy architecture.

27. Initiate action to enhance employee IT training by: (a) remedying problems associated with the FBI's on-line training system, and (b) developing a training plan specifically tailored to information technology specialists and electronic technicians.

28. Initiate action to complete the Extended Fast Track deployment timely by: (a) delivering the remaining quantities of Extended Fast Track desktop computers, and (b) procuring sufficient quantities of fiber optic cables.

29. Initiate action to: (a) procure adequate trouble-shooting equipment for Trilogy architecture, and (b) complete timely development of FBI unique macros for Microsoft Word.

2. The FBI's IT Strategic Planning and Performance Measurement

The FBI's IT strategic planning and performance measurement is inadequate because: (1) the FBI's strategic plan does not incorporate the ITIM process, and (2) the FBI's strategic plan and performance plan are not consistent with the DOJ's annual performance plan. These conditions occurred because the FBI has not updated its strategic plan since 1998, and its performance plan does not include strategic objectives, goals, and strategies relating to IT that are consistent with the DOJ's annual performance plan. As a result, the FBI will have difficulty advancing its ITIM process through the Framework's maturity stages. Additionally, there is a heightened risk that the FBI may not be appropriately allocating resources to meet the DOJ's strategic priorities.

A. Background on Strategic Planning

Strategic planning is used to determine and reach agreement on the fundamental results the organization seeks to achieve the goals and measures it will set to assess programs, and the resources and strategies needed to achieve its goals. Additionally, according to the GAO's June 2002 testimony to the House Appropriations Committee:[63]

> Strategic planning helps organizations to be proactive, anticipate and address emerging threats, and take advantage of opportunities to be reactive to events and crises. Leading organizations, therefore, understand that planning is not a static or occasional event, but a continuous, dynamic, and inclusive process. Moreover, it can guide decision-making and day-to-day activities.

The Government Performance and Results Act of 1993 (Results Act) provides for the establishment of strategic planning and performance measurement in the federal government. It seeks to improve the effectiveness, efficiency, and accountability of federal programs by establishing a system for agencies to set goals for program performance and to measure results. The Results Act requires agencies to prepare a strategic plan, annual performance

[63] This testimony, "FBI REORGINAZATION: Initial Steps Encouraging but Broad Transformation Needed" (GAO-02-865T), was made by the Comptroller General of the United States on June 21, 2002.

plans, and annual performance reports. The strategic plan, which is the key requirement of the Results Act, identifies agencies' long-term goals. Federal agencies are required to update their strategic plan at least every three years.

While the Results Act applies to the DOJ, it does not specifically apply to components such as the FBI. However, in our judgment, for the DOJ to comply with the Results Act, the components must have strategic and performance plans that are consistent with, and support, the DOJ's strategic and performance plans.

Annual performance plans include measurable goals that define what an agency will accomplish during a fiscal year. These plans should: (1) establish performance goals to define levels of performance to be achieved; (2) express those goals in an objective, quantifiable, and measurable form; (3) briefly describe the operational processes, skills, technology, human capital, information, or other resources required to meet the goals; (4) establish performance measures for assessing the progress toward, or achievement of, the goals; (5) provide a basis for comparing the actual program results with established goals; and (6) describe the means to be used to verify and validate measured values. There are at least two iterations of the annual performance plan. The initial annual performance plan is submitted to the OMB and is used during its review of the agency's budget request. The final annual performance plan is submitted to Congress soon after the transmittal of the President's budget.

The DOJ's annual performance plan is comprised of two parts. The first part is a summary performance plan that provides a departmental overview and synthesis and is submitted as a stand-alone document. The second part consists of the individual performance plans of the departmental components. These component plans are prepared pursuant to guidance provided by the DOJ and are incorporated within the components' budget submissions. Component plans should support the objectives, goals, and strategies of the DOJ's annual performance plan so that the DOJ can rely on the data provided through the component reports. In our judgment, components that do not incorporate the DOJ's objectives, goals, and strategies in their strategic and performance plans are at a heightened risk of not allocating resources in accordance with the DOJ's strategic priorities.

B. Strategic Planning's Relationship to the ITIM Process

According to the Framework, the purpose of ITIM is to describe and improve the IT investment management processes so that the strategic plans and decisions that are made can and will be supported by highly effective IT investments. Similarly, performance measures created and used to guide the organization and its activities are a factor in some ITIM critical processes. However, in general, activities related to the ongoing development and implementation of performance measures are largely outside the scope of the GAO ITIM Framework.

Although strategic planning is a function that is largely independent of the ITIM process, strategic planning activities relate to the Framework's activities at different stages of investment maturity. Specifically, the business needs identification critical process in Stage Two has a key practice that requires the organization to have defined business needs or stated mission goals. Additionally, Stage Five maturity, leveraging IT for strategic outcomes, is highly dependent on the comprehensiveness of the organization's strategic plan. Stage Five maturity also focuses on the organization's ability to improve strategic outcomes, change business processes to take advantage of technology changes, and learn from others by benchmarking processes. Based on the interdependencies between the ITIM and strategic planning processes, in our judgment the organization's strategic plan should address IT investment management.

In July 2002, the DOJ released its IT Strategic Plan that included the following four goals:

1. share information quickly, easily and appropriately - inside and outside the DOJ;

2. secure and protect information;

3. provide reliable, trusted, and cost-effective IT services; and

4. use IT to improve program effectiveness and performance.

To meet these goals, the DOJ is focused on four key areas that it considers to be the building blocks of the IT program: (1) IT infrastructure, (2) information security, (3) common solutions, and (4) management roles and processes. One of the strategic initiatives that comprise management roles and processes is: "Establish and

implement improved investment management processes and practices."[64] Based on this focus, in our judgment the DOJ has recognized the importance of integrating strategic planning with IT management.

C. Results of our Assessment of the FBI's IT Strategic Planning and Performance Measurement

We found that the FBI's IT strategic planning and performance measurement is inadequate because: (1) the FBI's strategic plan does not incorporate the ITIM process, and (2) the FBI's strategic plan and performance plan are not consistent with the DOJ's annual performance plan.

The FBI's ITIM Model and Transition Plan states that the Bureau's IT strategic plan must incorporate the ITIM process in order for it to achieve advanced IT investment maturity. However, as of the end of June 2002, the FBI did not have a current strategic plan dedicated to IT. Instead, individual divisions had program plans that included the use of IT within the particular program.

Additionally, the Bureau-wide strategic plan has not been updated since 1998. Not only does this time period pre-date the FBI's ITIM process, but it also pre-dates the development of the Framework in 2000. Officials in the Office of Strategic Planning told us that the Office of Strategic Planning's recent efforts have not been focused on IT.

The FBI acknowledged to us that it must incorporate strategic planning with its ITIM process, including updating its strategic plan. In our judgment, without a new strategic plan, the FBI will limit the effectiveness of its ITIM and strategic planning processes.

Further, we found that the FBI's strategic plan (from 1998) and its FY 2003 performance plan did not support the DOJ's annual performance plan relating to IT. This lack of support occurred because the FBI's strategic and performance plans are not consistent with the strategic objectives, goals, and strategies relating to IT as the DOJ's annual performance plan. The DOJ's FY 2003 annual performance plan

[64] Because the DOJ's IT Strategic Plan was first published in July 2002, we did not assess the FBI's compliance with it during our audit fieldwork. However, because of the recognized relationship between IT investment management and strategic planning, we did examine the FBI's strategic plan to determine if it incorporated the ITIM process.

includes the strategic objective to "make effective use of IT." Additionally, this strategic objective is supported by the annual goal to "expand electronic access and dissemination of information while ensuring IT security and cost effective IT investments meet programmatic and customer needs." However, both the strategic objective and the annual goal are not included within the FBI strategic plan and FY 2003 performance plan. As a result, there is a heightened risk the FBI may not be appropriately allocating resources to meet the DOJ's strategic priorities.

D. Summary

The FBI must have a Bureau-wide IT strategic plan to maximize the use of its IT investments, rather than having the division-specific IT focus that is currently in place. In fact, the purpose of the FBI's ITIM process is to move away from managing IT in division "stovepipes" to a centralized, Bureau-wide management focus. The FBI's strategic planning process must evolve with the ITIM process to ensure the success of both functions.

E. Recommendation

We recommend that the Director of the FBI ensures:

30. The IT strategic plan and performance plans are updated to: (a) fully integrate these plans with the FBI's ITIM process; and (b) include those performance goals and indicators included in the DOJ's IT Strategic Plan.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the FBI's management of IT investments. In connection with the audit, as required by the standards, we reviewed management processes and records to obtain reasonable assurance about the FBI's compliance with laws and regulations that, if not complied with, in our judgment, could have a material effect on FBI operations. Compliance with laws and regulations applicable to the FBI's management of IT investments is the responsibility of the FBI's management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations against which we conducted our tests are contained in the relevant portions of:

- the Government Performance and Results Act of 1993; and
- the Clinger-Cohen Act of 1996.

Our audit identified areas where the FBI was not in compliance with the laws and regulations referred to above. With respect to transactions that were not tested, nothing came to our attention that caused us to believe that FBI management was not in compliance with the laws and regulations cited above.

STATEMENT ON MANAGEMENT CONTROLS

In planning and performing our audit of the FBI's management of IT investments, we considered the FBI's management controls for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the management control structure as a whole; however, we noted certain matters that we consider to be reportable conditions under Government Auditing Standards.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the management control structure that, in our judgment, could adversely affect the FBI's ability to manage its IT investments. During our audit, we found the following management control deficiencies.

- The FBI lacked the basic selection and control processes necessary to build its IT investment capability.

- The FBI's IT strategic planning and performance measurement activities did not include its IT investment management process.

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

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The primary objectives of the audit were to: (1) determine whether the FBI was effectively managing its IT investments; and (2) assess the FBI's IT strategic planning and performance measurement activities.[65] In determining whether the FBI was effectively managing its IT investments, we also examined the FBI's efforts in developing enterprise architecture and project management functions. These two functions both complement and facilitate IT investment management. Additionally, we performed a case study of Trilogy, a significant IT project, to determine how the FBI's IT investment management practices affected the project's progress.

Scope and Methodology

The audit was performed in accordance with Government Auditing Standards, and included tests and procedures necessary to accomplish the audit objectives. We conducted work at: (1) FBI Headquarters in Washington, D.C. (2) FBI Laboratory facilities in Quantico, Virginia, and (3) FBI field offices in New York City, New York; Los Angeles, California; Chicago, Illinois; Miami, Florida; and Washington, D.C.

To perform our audit, we conducted approximately 85 interviews with 70 officials from the FBI (including field offices), DOJ, OMB, and GAO. The FBI officials interviewed were from the Director's office, Information Resources Division, Criminal Justice Information Services Division, Laboratory Division, Inspection Division, and Finance Division. Additionally, we reviewed over 200 documents related to IT management policies and procedures, project management guidance, strategic and program plans, IT project proposals and management plans, budget documentation, organizational structures, Congressional testimony, and prior GAO and OIG reports.

To determine whether the FBI is effectively managing its IT investments, we applied the GAO's ITIM framework and the associated assessment method. As part of the Framework's assessment method,

[65] During our audit fieldwork, we initiated work relating to a third objective: to determine if the FBI has implemented prior information technology related recommendations and improved its information technology. We will issue a separate report on this objective.

the FBI conducted a self-assessment of its IT investment management activities using the Framework. The self-assessment included those processes that the FBI had in place as of the beginning of our audit. Additionally, the self-assessment covered those processes that the FBI was planning to implement based on its IT Investment Management Model and Transition Plan.[66] In the self-assessment, the FBI indicated whether it executed each of the key practices in Stages Two through Five. The FBI asserted that it executed 27 of the 38 key practices from Stage Two, 3 of the 53 key practices from Stage Three, and none of the key practices from Stages Four and Five. Additionally, it stated in the self-assessment that the IT Investment Management Model and Transition Plan would be supplemented so that the FBI would eventually implement the critical processes necessary to achieve Stage Four maturity, as well as many of the key practices from Stage Five.

Because FBI officials stated in the IT Investment Management Model and Transition Plan that its initial goal was to advance to Stage Two, by default, the FBI indicated that it was in Stage One maturity. As a result, we validated the FBI's execution of the 38 key practices from Stage Two, and assessed the FBI's ability to improve its IT investment management practices through implementation of the ITIM process defined in the IT Investment Management Model and Transition Plan.

The Stage Two critical processes and key practices we examined focus primarily on the FBI's ability to effectively select and control its IT investments. To determine whether the FBI had implemented the critical processes and key practices in Stage Two, we evaluated policies, procedures, and guidance related to the FBI's IT investment management activities.

We compared the evidence collected from our document reviews and interviews to the key practices and critical processes defined in the Framework. Because the Framework is a hierarchical model, the rating of each critical process is dependent on the key practices below it. Therefore, we first rated the key practices. In accordance with the Framework's assessment method, we rated a key practice as "executed" when we determined that the FBI was executing the key aspects of the practice. A key practice was rated as "not executed" when we determined that there were significant weaknesses in the

[66] Although the FBI's IT Investment Management Model and Transition Plan, issued in January 2002, states that its primary goal is to provide the conceptual framework for Stage Two maturity, it also outlines the steps the FBI must take to advance to Stage Four maturity in preparation to achieving Stage Five maturity.

FBI's execution of the key practice and the FBI offered no adequate alternative, or when we found no evidence of a practice during the review.

Once the key practices were rated, we rated each of the Stage Two critical processes we reviewed. A critical process was rated "implemented" if all of the underlying key practices were rated as being executed. A critical process was rated as "not yet implemented, but substantial progress made" if over half, but not all, of its underlying key practices were rated as being executed. A critical process was rated as "not implemented" when there were significant weaknesses (i.e., fewer than 50 percent of the key practices had not been implemented) in the FBI's implementation of the underlying key practices and no adequate alternative was in place.

Beginning in March 2002, the FBI pilot tested the select phase of its new ITIM process. To measure the FBI's progress in improving the execution of Stage Two key practices during the course of our audit, we documented the key practices executed: (1) before the implementation start of the test pilot in March 2002, and (2) as of the end of our fieldwork in June 2002.

Our assessment of the FBI's ability to improve its IT investment management consisted of the following four areas:

1. the Plan's coverage of Stage Two key practice activities that were not being executed during our fieldwork;

2. the amount of participation from ITIM users in developing the ITIM process;

3. the support from the project management function; and

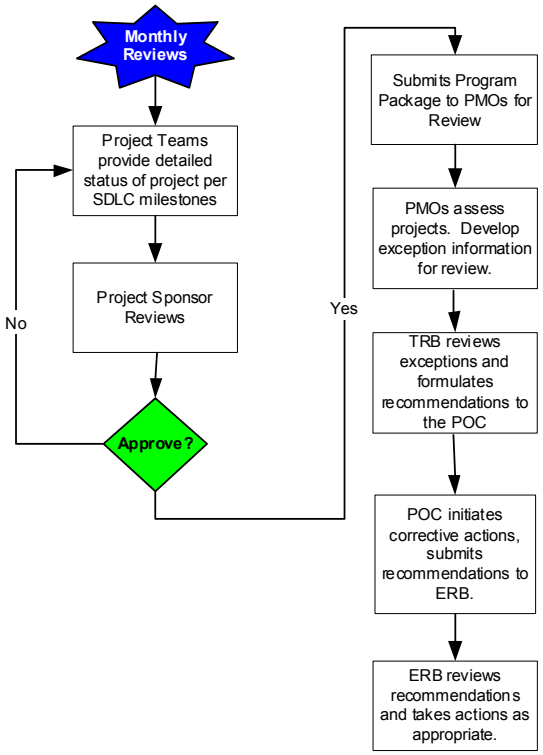
4. the support from the enterprise architecture function.

In addition, we performed a case-study of the Trilogy project to determine how the FBI's IT investment management practices have affected its progress. Trilogy was selected for a case-study because it is currently the FBI's most expensive IT project and its implementation is critical to the FBI's ability to achieve its mission. Trilogy is intended to provide the right hardware and software tools to the FBI's agents and analysts, enable the FBI's investigative personnel to easily and rapidly find, present, and manipulate required information, and transport and share information quickly and efficiently across the

Bureau. We performed the case-study both at FBI Headquarters where we interviewed individuals responsible for the project, as well as at five FBI field offices (New York, District of Columbia, Los Angeles, Miami, and Chicago) where we interviewed individuals responsible for assisting in the deployment of the new system, as well as agents utilizing the system.

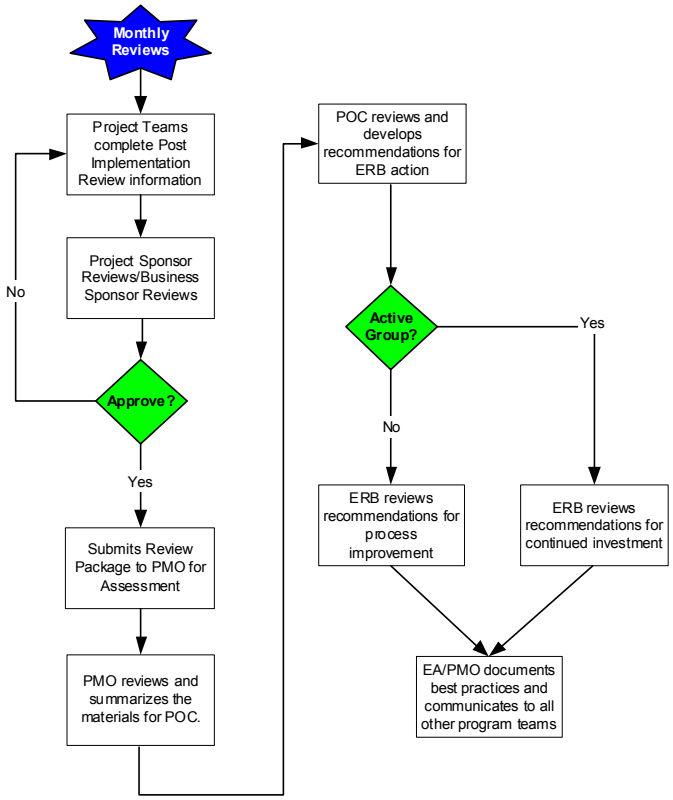
To assess the FBI's IT strategic planning and performance measurement activities, we reviewed strategic and performance planning documentation from the FBI, the DOJ's Strategic Plan for FYs 2001 to 2006, the DOJ's FY 2001 Performance Report, the DOJ's FY 2002 Revised Final Performance Plan for FY 2003, and the DOJ's IT Strategic Plan. To supplement our document review, we also interviewed officials responsible for creating FBI strategic and performance plans.

FLOWCHART OF FBI'S ITIM CONTROL PHASE



Source: FBI's training materials for the ITIM process as of February 2002.

FLOWCHART OF FBI'S ITIM EVALUATE PHASE



Source: FBI's training materials for the ITIM process as of February 2002.

JMD'S ASSESSMENT OF THE FBI'S ITIM PROCESS

Category	Element	Rating Values: Compliant, Partially Compliant, Non-Compliant
Policy/General	calls for the creation of an enterprise-wide IT investment review board tasked with oversight and decision-making responsibility over all investments in the organization's investment portfolio	Compliant
	establishes and maintains a comprehensive investment portfolio that includes all IT investments regardless of size, type, status, or source of funding	Compliant
	establishes a clear policy of endorsing IT investments based on their ability to meet the organization's mission and strategic goals and priorities	Compliant
	follows the select/control/evaluate ITIM model recommended by OMB, GAO, and DOJ	Compliant
	requires that the ITIM process be tied to and executed concurrently with the IT software development life cycle	Compliant
	provides mechanisms for expeditious reporting of current or historical investment information	Compliant
	for organizations that plan to create multiple IT investment boards along business or functional lines, establishes rules and procedures for: - properly aligning IT investments with functional level investment review boards and their portfolios - subjecting all portfolio decisions made by lower-level investment boards to final approval by an enterprise level investment review board - assigning the enterprise level investment review board with the responsibility of identifying and controlling IT investments having enterprise scope due to their importance, size, cost, risk, or crosscutting nature	N/A
	endorses the acquisition and use of tools to facilitate the ITIM process	Compliant

	defines major, crosscutting, and significant IT investments subject to DOJ CIO review that is consistent with DOJ policy	Compliant Not expressly stated in the process plan but acknowledged by submission of recent Exhibit 300/53s
Select Phase	establishes a structured, managed, and documented process for rating, ranking, and selecting IT projects for investment	Compliant
	establishes a structured and managed process for developing new IT proposals	Compliant
	establishes requirements and procedures for documenting new investment proposals including: - a concept of design and operation - impact on the organization's business functions and external entities - measured impact on mission, strategic goals, and priorities - comprehensive and detailed life-cycle costs - a realistic and defensible benefit/cost analysis consistent with OMB and GAO guidelines - a risk management plan - an acquisition plan - documentation that confirms consistency with mandated security and architectural requirements - a detailed consideration of alternatives that emphasizes return on investment	Compliant
	establishes a minimum return on investment "hurdle" that must be met by any new project in order to be eligible for consideration	Partially Compliant The document is ambiguous on this
	requires the consideration of COTS products and the products or services of other government or commercial entities as alternatives to in-house development of a new investment proposal	Compliant

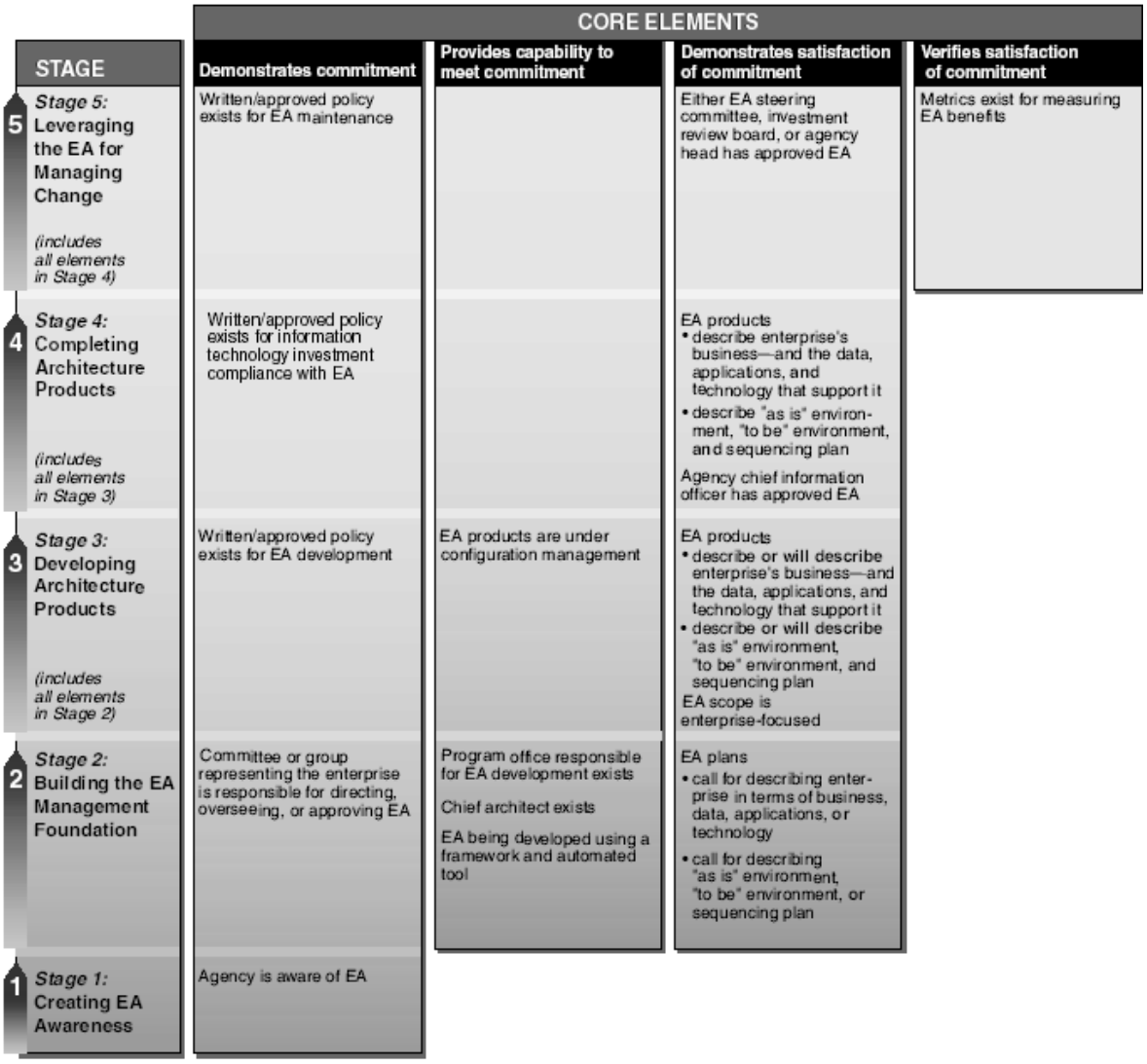
	establishes standardized, quantitative criteria for rating, ranking, and selecting investments in a consistent and uniform manner	Partially Compliant FBI is currently working on its rating criteria. Est. Completion date: 03-31-2002
	includes and gives considerable weight to selection factors that are linked directly to the organization's mission and strategic goals	Partially Compliant Acknowledged in principle; FBI is currently working on its selection criteria. Est. Completion date: 03-31-2002
	includes as a selection factor overall cost vs. budget availability	Partially Compliant FBI is currently working on its selection criteria. Est. Completion date: 03-31-2002
	includes as a selection factor the technical scope and complexity of the proposal and the organization's demonstrated ability to develop, implement, and manage projects similar in scope and complexity	Partially Compliant FBI is currently working on its selection criteria. Est. Completion date: 03-31-2002
	includes as a selection factor a project's adherence to the mandated enterprise architecture requirements	Compliant Acknowledged in principle throughout document
	includes as a selection factor a project's adherence to mandated security requirements	Compliant Acknowledged in principle in the document
	provides for the creation and maintenance of documentary evidence that supports the rating, ranking, and selection of each investment in the portfolio	Compliant

	requires that the cost, benefits, schedule, and risks of each investment are defined in a detailed and consistent manner and are supported by ample documentation	Compliant
	for projects that are selected for investment, establishes procedures and requirements for creating cost, schedule, and performance baselines that will be compared later to actual cost, schedule, performance, and mitigation of risks	Compliant
	for projects that are selected for investment, establishes requirements and procedures for: - creating a project management team to manage the investment throughout its life cycle whose membership includes representatives from all groups in the organization having a stake in the project's success or failure - preparing a project management plan to be followed by the project management team throughout the life cycle of the project - coordinating project acquisitions with the organization's acquisition staff - coordinating project funding and reporting with the organization's budget staff	Compliant
	requires the creation of an independent verification and validation plan for all approved projects	Compliant QA/testing project teams that are independent of development teams will define and execute these plans
Control Phase	establishes procedures for executing the project management plan	Compliant Part of existing FBI SDLC
	establishes requirements and procedures for calculating and documenting accurate and up-to-date project costs at prescribed intervals	Compliant
	establishes requirements and procedures for documenting project progress using key milestones and work breakdown schedules	Compliant

	establishes a requirement and procedures for employing standard earned value management techniques for managing and assessing contracted services	Compliant Not explicitly stated but part of current SDLC requirements
	establishes requirements and procedures for regular project reviews that compare current project costs, benefits, risk management, adherence to schedule, and performance measures to the baselines developed in the select phase, and that communicate the results of the reviews to the project stakeholders, the investment review board, and other entities having investment oversight responsibility	Compliant
	establishes reasonable baseline deviation tolerances that will be used to identify projects that are performing satisfactorily, marginally, or unsatisfactorily	Partially Compliant Deviation tolerances based on evaluation criteria still under development. Est. Completion date: 03-31-2002
	establishes procedures for taking corrective action or terminating projects that deviate from baselines	Compliant
	establishes requirements and procedures for subjecting all projects in the control phase to the rating, ranking, and selection processes of the select phase at prescribed intervals	Compliant
	establishes requirements, procedures, and mechanisms for producing required reports and communicating them to entities having project or portfolio oversight responsibility	Compliant
	establishes a requirement that projects in the portfolio be approved for deployment by the project management group and the investment review board	Compliant Part of SDLC process
	requires periodic deployment progress reports be prepared and communicated to the project management group, the investment review board, and other entities having oversight responsibility	Compliant Falls under FBI's generic definition of PIR
Evaluate Phase	establishes a requirement that a post implementation review be conducted of each investment after it is fully deployed and in use	Compliant

	establishes requirements and procedures for creating and communicating to oversight entities post implementation review reports that assess actual costs, benefits, and performance and compare them to corresponding baseline measures	Compliant
	establishes a requirement for producing user surveys when applicable in order to determine if and to what degree the project is meeting the needs of the users	Compliant
	establishes procedures for taking corrective action or terminating projects that deviate from baselines or that are not meeting the strategic needs of the organization	Compliant
	establishes a means of applying lessons learned in the selection, planning, development, deployment, and evaluation of the project in order to improve the ITIM and SDLC processes	Compliant
	establishes a requirement for conducting periodic operational reviews to assess the effectiveness of the investment in terms of cost, benefits, and performance, its adherence to enterprise architecture models and security requirements, and its ability to meet the organization's evolving mission goals and priorities	Compliant Falls under the umbrella of FBI's generic definition of PIR
	establishes a requirement that each project in the Evaluate phase be subjected again to the rating, ranking, and selection processes of the ITIM select phase at prescribed intervals so that a decision can be made on continued funding	Compliant
	establishes requirements, procedures, and mechanisms for producing required reports about the investments in the evaluation phase and communicating this information to entities having project or portfolio oversight responsibility	Compliant
	establishes a requirement that a plan be developed for disposing or replacing an IT asset when it no longer meets the needs of the organization	Partially Compliant Decision on disposal mentioned but not a plan.

GAO'S FIVE STAGES OF ENTERPRISE ARCHITECTURE MATURITY



	CORE ELEMENTS			
STAGE	**Demonstrates commitment**	**Provides capability to meet commitment**	**Demonstrates satisfaction of commitment**	**Verifies satisfaction of commitment**
5 *Stage 5:* Leveraging the EA for Managing Change *(includes all elements in Stage 4)*	Written/approved policy exists for EA maintenance		Either EA steering committee, investment review board, or agency head has approved EA	Metrics exist for measuring EA benefits
4 *Stage 4:* Completing Architecture Products *(includes all elements in Stage 3)*	Written/approved policy exists for information technology investment compliance with EA		EA products • describe enterprise's business—and the data, applications, and technology that support it • describe "as is" environment, "to be" environment, and sequencing plan Agency chief information officer has approved EA	
3 *Stage 3:* Developing Architecture Products *(includes all elements in Stage 2)*	Written/approved policy exists for EA development	EA products are under configuration management	EA products • describe or will describe enterprise's business—and the data, applications, and technology that support it • describe or will describe "as is" environment, "to be" environment, and sequencing plan EA scope is enterprise-focused	
2 *Stage 2:* Building the EA Management Foundation	Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA	Program office responsible for EA development exists Chief architect exists EA being developed using a framework and automated tool	EA plans • call for describing enterprise in terms of business, data, applications, or technology • call for describing "as is" environment, "to be" environment, or sequencing plan	
1 *Stage 1:* Creating EA Awareness	Agency is aware of EA			

Stage One: Creating Enterprise Architecture Awareness is characterized by either no plans to develop and use an enterprise architecture (EA), or plans and actions that do not yet demonstrate an awareness of the value of having and using one. While Stage One agencies may have initiated some EA core elements, these agencies' efforts are ad hoc and unstructured, and do not provide the management foundation necessary for successful EA development.

Stage Two: Building the EA Management Foundation focuses on assignment of roles and responsibilities and establishment of plans for developing EA products. Specifically, a Stage Two agency has

designated a chief architect and established and staffed a program office responsible for EA development. Further, a steering committee or group that has responsibility for directing and overseeing the development has been established and the membership of the steering committee is comprised of business and IT representatives. At Stage Two, the agency either has plans for developing or has begun development of at least some of the necessary EA products. This stage also requires the agency to have selected both a framework that will be the basis for the nature and content of the specific products it plans to develop, and an automated tool to help in the development.

Stage Three: Developing Architecture Products focuses on actual development of EA products. At Stage Three, the agency has defined the scope of its EA as encompassing the entire enterprise, whether organization based or function-based, and it has a written and approved policy demonstrating institutional commitment. Although the products may not yet be complete, these products are intended to describe the agency in business, data, applications, and technology terms. Further, the products are to describe the current (i.e., "as is") and future (i.e., "to be") states and the plan for transitioning from current to future state (i.e., sequencing plan). Also, as the architecture products are being developed, these products are to be subject to configuration control.

Stage Four: Completing EA Products is characterized by complete and approved EA products that the agency can use to help select and control its portfolio of IT investments. The complete products describe the agency in business, data, applications, and technology terms. Also, the products are complete in that the products describe the agency's current and future states and the transition plan for sequencing from the current state to the future state. Further, the agency's Chief Information Officer has approved the EA and the agency has a written policy requiring that IT investments comply with the EA.

Stage Five: Leveraging the EA for Managing Change entails evolving the products according to a written and approved policy for EA maintenance. Also at this stage, either the steering committee, investment review board, or agency head approves the EA. Finally, the agency has incorporated the EA into its corporate decision-making and has established and is using metrics to measure the effectiveness of its EA.

Source: GAO Report, "INFORMATION TECHNOLOGY: Enterprise Architecture Use across the Federal Government Can Be Improved" (GAO-02-6).

APPENDIX 6

FBI'S ENTERPRISE ARCHITECTURE MATURITY SURVEY

Department of Justice

Federal Bureau of Investigation: Stage 1[a]

Stage	Description	Satisfied?
Stage 5: **Leveraging the EA for Managing Change** (includes all elements from stage 4)	• Written/approved policy exists for EA maintenance. • Either EA steering committee, investment review board, or agency head has approved EA. • Metrics exist for measuring EA benefits.	No No Yes
Stage 4: **Completing Architecture Products** (includes all elements from stage 3)	• Written/approved policy exists for information technology investment compliance with EA. • EA products describe enterprise's business—and the data, applications, **and** technology that support it. • EA products describe "as is" environment, "to be" environment, **and** sequencing plan. • Agency chief information officer has approved EA.	Yes No No No
Stage 3: **Developing Architecture Products** (includes all elements from stage 2)	• Written/approved policy exists for EA development. • EA products are under configuration management. • EA products describe **or will describe** enterprise's business—and the data, applications, **and** technology that support it. • EA products describe **or will describe** "as is" environment, "to be" environment, **and** sequencing plan. • EA scope is enterprise-focused.	No Yes Yes Yes No
Stage 2: **Building the EA Management Foundation**	• Committee or group representing the enterprise is responsible for directing, overseeing, and/or approving EA. • Program office responsible for EA development exists. • Chief architect exists. • EA being developed using a framework and automated tool. • EA plans call for describing enterprise in terms of business, data, applications, **or** technology. • EA plans call for describing "as is" environment, "to be" environment, **or** sequencing plan.	No Yes Yes Yes Yes Yes
Stage 1: **Creating EA Awareness**	• Agency is aware of EA.	Yes

[a] The Federal Bureau of Investigation provided its survey response on July 18, 2001.

Source: GAO Report, "INFORMATION TECHNOLOGY: Enterprise Architecture Use across the Federal Government Can Be Improved" (GAO-02-6).

APPENDIX 7

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

November 8, 2002

Mr. Guy K. Zimmerman
U.S. Department of Justice
Room 4706, 950 Pennsylvania Avenue N. W.
Washington, D.C. 20530

Dear Mr. Zimmerman:

Reference is made to your memorandum dated October 10, 2002, concerning the FBI response to recommendations set forth in the Department of Justice (DOJ), Office of the Inspector General (OIG), draft audit report entitled "Federal Bureau of Investigation's Management of Information Technology Investments." This memorandum requested the FBI review and provide written comments regarding report recommendations. Specifically, you requested the FBI comment as to its agreement or disagreement with each of the recommendations. You also requested the FBI identify steps taken or planned to achieve corrective action and to include dates of implementation.

Attached is the FBI's written response which is based on the ITIM process as it exists today. However, with my recent appointment as Chief Information Officer and the hiring of a Chief Financial Officer, an assessment of the current process was initiated to identify areas to streamline and improve efficiencies within the ITIM process and between the ITIM process and other related business processes. The current ITIM process, as audited, may change as a result of this assessment. We anticipate the assessment and implementation of changes to be completed by February 2003.

Please note, the format of the enclosed document identifies the DOJ OIG draft audit report recommendation followed by the response of FBI Executive Management. Additionally, a sensitivity review was conducted per your request and the results are included in the written response.

The recommendation responses set forth in the attached were coordinated through the FBI's Inspection Division. Please contact me on 202-324-6165 or Lynne Hunt of the Inspection Division on 202-324-2901 should you have any questions.

Sincerely yours,

Darwin A. John
Chief Information Officer

FBI Response
to
DOJ OIG Draft Audit Report
Federal Bureau of Investigation's
Management of Information Technology Investments

Recommendation Number 1, Page 33: We recommend that the Director of the FBI: Require the ITIM Program Office to plan for and take more timely action to allow board members and other ITIM users to execute assigned responsibilities competently (Prerequisite 1).

Response: The FBI agrees with this recommendation. As a part of the ITIM governance structure established in April 2002, (1) the ITIM Program Office has established regularly scheduled meetings for each of the investment boards. These meetings are part of the ITIM process and have standing agenda's of items to be discussed. (2) The ITIM Program Office maintains an up-to-date list of items requiring board member action and the status of those items. (3) The ITIM Program Office supports a variety of requests from board members for information relating to their required duties.

The ITIM Program Office's ability to carry out these tasks on a regular and consistent basis is dependent on adequate permanent staffing of the ITIM Program Office (see Recommendation Number 15).

Recommendation Number 2, Page 33: We recommend that the Director of the FBI: Ensure that all members of the IT investment boards receive sufficient education and training to execute assigned responsibilities effectively. We suggest that for each of the investment boards the FBI: (1) identify the core competencies required of members in using the IT investment approach, and (2) develop appropriate education and training development plans to ensure members acquire the required core competencies (Prerequisite 2).

Response: The FBI agrees with this recommendation and has made significant progress towards implementation. Specifically, in March 2002 the ITIM Program Office provided training for each investment board member on the overall IT Investment Management Framework and detailed training on the SELECT process. The SELECT process training provided critical information to IT investment stakeholders as the Bureau implemented the "SELECT" pilot to support the selection of investments to be included in the FY 2004 Enhancement Request to DOJ.

Additional training for the CONTROL and EVALUATE process is a requirement of the ITIM office as part of their

respective pilot phases scheduled later this fiscal year, i.e., second and third quarters of FY 2003 respectively. Also, the Director has ratified the ITIM Program Office developed Program Charters and Roles and Responsibilities documents dated June 2002 that specifically identify the core competencies required for each investment board members, specifically for the Executive Review Board (ERB), Project Oversight Committee (POC), and Technical Review Board (TRB).

Recommendation Number 3, Page 41: We recommend that the Director of the FBI ensures: Official project management guidance is consistently followed by all FBI IT project managers.

Response: The FBI agrees with this recommendation. With the reorganization resulting from the establishment of the expanded Chief Information Officer (CIO) organization and the formalization of the Projects Management Office (PMO) headed by the FBI's Program Management Executive, that organization will have responsibility for establishing IT program management guidance within the Bureau. Policy, standards, and guidance will be established and mandated for all FBI IT projects. Selected projects, based on cost, size, complexity, risk, and/or importance to mission will be closely monitored by the PMO to ensure adherence to that guidance. The remainder of the projects will be monitored by their appropriate Division Assistant Director. As a part of the ITIM process, all projects will be required to present selected information to the POC and boards at specified decision points as part of the oversight process.

Recommendation Number 4, Page 41: We recommend that the Director of the FBI ensure: Written policies and procedures are developed for management oversight of IT projects for use by the investment review boards (Organizational Commitment 2).

Response: The FBI agrees with this recommendation. High-level written policy and procedure documents have been developed for the SELECT phase of the ITIM program piloted in March 2002 and are currently used by the investment review boards. High-level written policy and procedure documents are currently under development for the CONTROL and EVALUATE phases. As part of the planned continued maturity plans for the next phase, detailed written policy and procedure documents are included in the scope (third quarter FY 2003). Thereafter, as each element of ITIM (CONTROL/SELECT/EVALUATE) is matured, the respective policy and procedure documentation will be updated as part of the maturation process.

Recommendation Number 5, Page 41: We recommend that the Director of the FBI ensure: IT Investment Review Boards are supported by a centralized project management office that operates in accordance with ITIM policies and procedures (Prerequisite 1).

Response: The FBI agrees with this recommendation. A centralized PMO has been established by the Director and under the auspices of the CIO. The CONTROL design currently underway establishes that the centralized PMO will operate in accordance with the ITIM policies and procedures. The CONTROL design and pilot will involve the communication of essential project data between the PMO and ITIM Program Office. In addition, PMO will utilize the existing ITIM governance structure.

Recommendation Number 6, Page 41: We recommend that the Director of the FBI ensures: Each IT project has a project management plan, approved by the Project Oversight Committee, that includes cost and schedule controls (Prerequisite 2).

Response: The FBI agrees with this recommendation. As part of the ITIM process, each project, in accordance with standards established by the PMO, will develop a project management plan to include cost and schedule controls appropriate to its size, complexity, risk, and importance to the Bureau's mission. Once approved, that project will be tracked against that plan with reporting at the appropriate points in the plan to the review board designated at time of plan approval.

Recommendation Number 7, Page 41: We recommend that the Director of the FBI ensure: Information being developed in the IT asset inventory is made available to, and used by, the boards.

Response: The FBI agrees with this recommendation. As part of the enterprise architecture basic plan a comprehensive inventory of IT assets is being compiled. As part of the next phase of the ITIM framework maturity, the IT inventory will be assessed and analyzed for alignment to the Bureau's mission as well as functional and technical quality. The results will be made available as an investment decision making tool to the IT Governance Boards and other key stakeholders. Planned completion for the first phase of the inventory performance assessment is targeted for the third quarter FY 2003.

Recommendation Number 8, Page 41: We recommend that the Director of the FBI ensure: Execution of the five key

practices consisting of the activities necessary for the investment review boards to maintain effective oversight of IT projects during the critical control phase. These five key practices consist of:

Providing each projects up-to-date cost and schedule data to the appropriate IT investment board (Activity 1).

Response: The FBI agrees with this recommendation. As part of the CONTROL design, and as described in the response to Recommendation Number 19, it is at eight key decision points during the development life-cycle of an IT project that the FBI's POC would review scope, cost, and schedule of top-level projects that the FBI is managing. The first pilot of CONTROL is expected to begin in December 2002 and the roll-out of CONTROL is expected to be completed by fourth quarter FY 2003.

Establishing criteria for the boards to review each IT project's performance by comparing actual cost and schedule data to expectations (Activity 2).

Response: The FBI agrees with this recommendation. As part of the CONTROL design, the Office of the CIO is developing the required criteria and process for the investment review boards to review each IT project's performance by comparing actual cost and schedule data to expectations. The first pilot of CONTROL is expected to begin in December 2002 and the roll-out of CONTROL is expected to be completed by fourth quarter FY 2003.

Performing special reviews of projects that have not met predetermined performance standards (Activity 3).

Response: The FBI agrees with this recommendation. As part of the CONTROL design, the ITIM Program Office is developing a policy by which the investment review boards will be able to conduct special reviews, as needed, on those projects that have not met pre-determined standards. The PMO will develop the specific process. The process will monitor specific key scope, cost, and schedule performance indicators and an escalation of reporting requirements to serve as early warning of project deviation from expectations (see response to Recommendation Number 19 for additional details). The first pilot of CONTROL is expected to begin in December 2002 and the roll-out of CONTROL is expected to be completed by fourth quarter FY 2003.

Defining, documenting, and agreeing to corrective actions for each under-performing project by the appropriate IT investment board and the project manager (Activity 4).

Response: The FBI agrees with this recommendation. As part of the CONTROL design, the ITIM Program Office is developing the policy for defining, documenting and agreeing to corrective actions for each under-performing project by the appropriate IT investment board. The PMO will specify the procedures for executing the corrective actions. The CONTROL process will identify the specific actions required by the project manager/sponsor and alternatives available to the investment review board members. The first pilot of CONTROL is expected to begin in December 2002 and the roll-out of CONTROL is expected to be completed by fourth quarter FY 2003.

Tracking and implementing corrective actions until the desired outcomes are achieved (Activity 5).

Response: The FBI agrees with this recommendation. As part of the CONTROL design, the ITIM Program Policy mandates the necessary tracking, including the implementation of corrective actions to ensure that desired project outcomes are achieved. The first pilot of CONTROL is expected to begin in December 2002 and the roll-out of CONTROL is expected to be completed by fourth quarter FY 2003.

Recommendation Number 9, Page 46: We recommend that the Director of the FBI ensure: Establish a deadline for completing the creation of the FBI IT inventory and ensure progress toward completion is monitored.

Response: The FBI agrees with this recommendation. The established deadline for completing and validating the FBI IT inventory is the end of the second quarter FY 2003. The performance evaluation of the IT inventory is expected to be completed by third quarter FY 2003. Results of the evaluation will be incorporated into the overall ITIM governance framework. Progress is being monitored through periodic updates to the ITIM Program Office.

Recommendation Number 10, Page 47: Implement processes to ensure: a. Subsequent changes to IT projects and systems are identified and documented in the inventory; b. Information from the inventory is available on demand to decision-makers and other affected parties; and c. The IT project and system inventory and its information records are maintained to contribute to future investment selections and assessments.

Response: The FBI agrees with this recommendation. In addition to implementing the processes (see response to Recommendation Number 7 above) the ITIM framework requires, ongoing maintenance and performance evaluation of the IT inventory. As a fully integrated part of the process, this

information will be used to contribute to future IT investment decisions. Periodic updates to the IT inventory is planned for fourth quarter FY 2003.

Recommendation Number 11, Page 52: We recommend that the Director of the FBI ensures: Written policies and procedures are developed for identifying the business needs (and the associated users) of each IT project (Organizational Commitment 1).

Response: The FBI agrees with this recommendation and has made significant progress towards full implementation. As of March 2002 the SELECT Phase had been implemented for all new IT investment requests. As part of the SELECT process, high-level written policy and procedures were developed for identifying the business needs of each IT project. Specifically, the FBI has been using Concept Papers and the required 300 Exhibit to standardize the documentation of the business case.

Recommendation Number 12, Page 52: We recommend that the Director of the FBI ensures: Adequate resources are allocated to train ITIM users in identifying business needs and associated users (Prerequisites 1 and 3).

Response: The FBI agrees with this recommendation. Training for the overall IT Investment Management Framework and specifically the SELECT process was completed in March 2002 by the current ITIM Program Office staff and the FBI contractor. This training was offered bureau-wide and included the members of the three investment boards, in addition to the Business Lines' ITIM liaisons and other key stakeholders. Training for CONTROL and EVALUATE is planned just-in-time as those programs are respectively rolled out.

As personnel continue to change in the organization, the ITIM Office will (1) require staffing to maintain a 're-training' program, or (2) execute a 'train-the-trainer' program within the business units vis-à-vis the 'business liaison' role. Option 1 will require staffing support and Option 2 will require Senior Leadership Team support to include this responsibility within the liaison role.

Recommendation Number 13, Page 52: We recommend that the Director of the FBI ensures: Identified users participate in project management throughout a project's life-cycle (Activity 3).

Response: The FBI agrees with this recommendation. The PMO will, as part of its project management process, institute procedures involving the appropriate users throughout the development cycle. For example, the Trilogy Program has

established a Joint Application Development (JAD) process. This process has brought a broad range of users from a number of field offices to headquarters to participate in the development of requirements for the Trilogy Virtual Case File (VCF). The team will continue to function through the development life-cycle, reviewing designs and participating in testing, acceptance and implementation. This approach will be applied to all large-scale development projects. The PMO contains a VCF/JAD Unit, which will apply this methodology of requirements elicitation, definition and specification to FBI development projects.

Recommendation Number 14, Page 59: We recommend that the Director of the FBI ensures: The ITIM process applies to all IT project proposals, including proposals that are funded through the FBI's base funding.

Response: The FBI agrees with this recommendation and has made progress towards its implementation. The ITIM SELECT process was applied to all new investment requests for the new Budget Year FY 2004. As the ITIM process is matured, all IT project proposals including those funded through the FBI's base budget will be subject to the SELECT process. During FY 2003, it is planned that the FY 2003 base and enhancement requests will be subject to the ITIM program.

Recommendation Number 15, Page 59: We recommend that the Director of the FBI ensures: Sufficient staffing is provided to the ITIM Program Office, as recommended in the Post-Implementation Review.

Response: The FBI agrees with this recommendation and currently has requested 6 additional full-time FBI staff employees for the ITIM Program Office.

Recommendation Number 16, Page 67: We recommend that the Director of the FBI ensure: The recommendations set forth in the Post-Implementation Review relating to expanding the policies and procedures of the ITIM process are implemented.

Response: The FBI agrees with this recommendation. As of September 2002, the FBI has implemented all recommendations of the Post-Implementation Review relating to expanding polices and procedures of the ITIM process. The FBI plans to continually mature the ITIM process as needed.

Recommendation Number 17, Page 72: We recommend that the Director of the FBI ensures: The ITIM Program Office and the ITIM contractor incorporate the input from various ITIM users, including those from the enterprise architecture office, CJIS Division, the Laboratory Division, and the

Inspection Division as the control and evaluate phases of the ITIM process are being developed and refined. This input should be solicited through working group sessions scheduled on a periodic basis.

Response: The FBI agrees with this recommendation and has incorporated the input from each of the various ITIM users mentioned during the CONTROL and EVALUATE design phase. As of September 2002, interviews and working group sessions with each of the various ITIM user communities were completed and their input was used in the design of the CONTROL and EVALUATE design and pilot.

Recommendation Number 18, Page 72: We recommend that the Director of the FBI ensures: The ITIM process is modified so that the Technical Review Board and Enterprise Architecture Technical Committee perform a business architecture compliance review of IT project proposals to ensure these proposals support the mission of the FBI.

Response: The FBI agrees with this recommendation. The ITIM process is being modified to ensure that the TRB and the Enterprise Architecture Technical Committee will perform a business architecture compliance review of IT projects to ensure support of FBI missions. This modification will be completed by third quarter FY 2003.

Recommendation Number 19, Page 80: We recommend that the Director of the FBI ensures: The FBI prepares a plan that specifically details how the project management office will support the ITIM process. This plan should include the project management office's criteria and thresholds for: (1) selecting IT projects to manage, and (2) identifying projects that the Project Oversight Committee will review.

Response: The FBI agrees with this recommendation. The FBI is currently preparing a plan that addresses the FBI's implementation of the ITIM process. That plan will address how the PMO, and the new Planning Organization within the Office of the CIO will interact with and support the ITIM process. FBI's Office of the CIO plans to use the ITIM process to manage all FBI IT investments. The CIO's Planning Division will develop the FBI IT Architecture, coordinate all IT Planning and assist in evaluating the FBI's IT initiatives during the program select phase. The PMO will also assist in evaluating IT projects during the Select Phase. Once a project is selected for development through the ITIM review process, and funded through the Budget Process, the PMO will manage selected major projects and smaller or less critical projects will be assigned to the Operations Support Division in the Office of the CIO or to the Sponsoring Division.

The PMO will develop large and complex projects on behalf of sponsoring divisions to ensure their successful execution and free the operational FBI divisions to focus on their priority missions. Projects will originate within FBIHQ and field divisions. Sponsoring divisions will be required to make a business case that justifies the investment, through the ITIM process.

Examples of selection criteria for a project's development to be managed by the PMO are: 1) greater than $10M total value, 2) high risk, 3) high level of development complexity, 4) FBI priority project, and/or 5) emergency project (i.e., response to quick-reaction requirement). However, these criteria are currently being finalized; project selection will also depend upon resources available to the PMO to carry out their mission.

The ITIM process has proposed eight major decision points during the development life-cycle of a project. It is at these key decision points that the POC would review those top-level projects that the PMO is managing. At each decision point, a decision by senior FBI management will be made whether to proceed with a project and continue to commit resources to it or to end a project and reprogram its funds. The POC may desire more frequent reports of program status for those projects designated as requiring intense scrutiny, such as monthly Trilogy project briefings.

Recommendation Number 20, Page 80: We recommend that the Director of the FBI ensures: The FBI develops and implements a specific plan detailing how and when it will integrate the ITIM process with a system development life-cycle methodology such as the Project Management Process.

Response: The FBI agrees with this recommendation. The PMO will establish a Project Management Process that incorporates a system life-cycle methodology. This methodology, with appropriate tailoring, will be mandatory for all projects in the Bureau. The PMO will ensure that this process is fully integrated into and supports the ITIM process.

Recommendation Number 21, Page 85: We recommend that the Director of the FBI ensures: The FBI continues its efforts to establish a comprehensive enterprise architecture. The FBI must develop and implement a specific plan to integrate ITIM and enterprise architecture processes, even as these processes are being further refined and developed.

Response: The FBI agrees with this recommendation. The FBI enterprise architecture is under development within a single governance structure as established by the ITIM framework as

approved by DOJ in May 2002. FBI is accelerating the focus and attention on enterprise architecture and has a 6-month target to implement the first phase of a world-class enterprise architecture framework (April 2003). As with the ITIM program, the FBI plans to continually mature the Bureau's Enterprise Architecture.

Recommendation Number 22, Page 113: We recommend that the Director of the FBI: The IT Investment Review Boards initiate oversight of Trilogy, including: (a) the establishment of cost, schedule, technical, and performance baselines; and (b) tracking significant deviations from these baselines and taking corrective actions as necessary.

Response: The FBI agrees with this recommendation. Trilogy baselines for cost, schedule, and technical performance are being established. Trilogy is comprised of two components, TNC/IPC and UAC. The TNC/IPC and the UAC baselines will be established once the current Engineering Change Proposals (ECP's) are negotiated. Metrics are being included in those baselines that will allow tracking and recognition of significant deviation.

Because of the advanced stages of the Trilogy components and the significant schedule compression, the PMO, in conjunction with the IT Investment Review Boards, will establish a set of cost, schedule, and performance goals to be monitored. The PMO will monitor those factors on a regular basis and report the progress to the IT Investment Review Boards against set milestones.

Recommendation Number 23, Page 113: We recommend that the Director of the FBI: The technical requirements for Trilogy are adequately defined, documented, and shared with other IT users.

Response: The FBI agrees with this recommendation. For the UAC portion of Trilogy, the Virtual Case File (VCF) functional requirements were defined in a series of five Joint Application Development (JAD) sessions, and approximately twelve Working Groups that were made up of SAIC, Information Resources Division, and IT users. The IT users were the ones that identified the needs that were transferred into requirements. They did this utilizing a walkthrough of their business processes, while identifying areas of inefficiencies that could be facilitated through re-engineering. The IT users also served as reviewers of the subsequent requirements documentation, commenting on the appropriateness of the requirements. The IT users will continue to be a part of the VCF team throughout the development process.

For the TNC/ICP portion of Trilogy, the requirements have been defined, documented and made available.

Recommendation Number 24, Page 113: We recommend that the Director of the FBI: The Trilogy project managers prepare an action plan to address the risks identified by the three internal reports on Trilogy. This plan should include (a) actions already taken to mitigate these risks, (b) planned actions, including suspense dates, and (c) an explanation for why some risks cannot be mitigated, if applicable. The IT investment review boards should then approve this plan and monitor it for implementation.

Response: The FBI agrees with this recommendation. An action plan will be prepared by the Trilogy Project Management Office addressing the three reports (INSD, CJIS and IV&V assessment) by 12/31/02. Common actions from the reports will be combined resulting in a synthesized list of actions. This plan will include actions already taken to mitigate these risks, planned actions, including suspense dates, and an explanation for why some risks cannot be mitigated, if applicable. The plan will be approved by the CIO and monitored for compliance.

Recommendation Number 25, Page 113: We recommend that the Director of the FBI: For future IT deployments, ensure that processes are established for field offices to submit input and receive feedback from FBI Headquarters prior to installing equipment.

Response: The FBI agrees with this recommendation. A successful process was used for the site installation schedule for the Trilogy project. It was coordinated with each Field Office through an initial site survey. Due to the success of this process, it will be incorporated into the overall ITIM framework and will be used for all future IT deployments.

Recommendation Number 26, Page 113: We recommend that the Director of the FBI: Initiate action to remedy contractor deficiencies associated with inefficient: (a) operation of the service support center, and (b) maintenance support for Trilogy architecture.

Response: The FBI agrees with this recommendation. The Trilogy Program awarded a maintenance contract to DynCorp/Unisys to provide maintenance for the Trilogy deployed components. That service level agreement (SLA) contract runs through December 2003. There is another 3-year multi-year maintenance contract for Legacy and non-Trilogy maintenance components which runs through the end of fiscal 2004. The FBI is in the process of consolidating IT

maintenance contract requirements to benefit from economies-of-scale.

During the first month of the new maintenance contract, outstanding trouble tickets have been reduced from 260 to 140. As the contractor becomes fully engaged in this activity, the number of outstanding trouble tickets will decrease further. The new maintenance contract contains metrics. Contractor statistics are being monitored daily.

The Trilogy Program is working to develop and deliver an Enterprise Operations Center (EOC) with staffing, training, and tools to provide central management, monitoring, and administration of the Trilogy deployed infrastructure. The EOC will have a higher technical level of skill and ability to resolve and pro-actively manage the network components and any problem resolution for all FBI customers.

Until the EOC with its Enterprise Management System (EMS) is in place and operational, the problem will not be fully resolved. When the EMS is operational, it will provide a new way to manage, operate, and maintain Trilogy. The EMS will provide the EOC with the capability to centrally monitor and control the Trilogy system. This capability will enable the EOC to detect emerging problems and take corrective actions before they impact system performance. The EOC is expected to resolve the majority of all problems. The goal is to correct 80% of the problems at the EOC on the first call. The other 20% will be escalated but resolved within established timeframes. The EOC ITS will retain ownership of the problem ticket until the problem is resolved.

Recommendation Number 27, Page 113: We recommend that the Director of the FBI: Initiate action to enhance employee IT training by: (a) remedying problems associated with the FBI's on-line training system, and (b) developing a training plan specifically tailored to information technology specialists and electronic technicians.

Response: The FBI agrees with this recommendation.

(a) All issues identified during the first phase of MS Office 2000 training, March 2002 through May 2002, have been corrected.

The primary issue related to the FBI Virtual Academy Learning Management System (LMS) deployment in use for the Trilogy project had been related to password issues. Of the calls and e-mails fielded during the training sessions of the first 23 offices, 93% were related to users forgetting

their passwords. The remaining 7% of calls and e-mails were in support of the Training Technicians, Administrative Officers, or Training Coordinators roles in relation to the Approval Console and the Microsoft Office 2000 Computer-Based Training (CBT) courses.

The issues surrounding the CBT itself were problems with various programs within the suite of products received from the vendor, SmartForce, Inc. All of the problems that arose during the training were resolved by the vendor, SmartForce, Inc. A new CBT issue arose recently regarding a course freezing during the assessment portion of the first unit of a CBT. The contractor has been contacted and they are working to provide a new version of the software.

Additionally, an issue arose in two large field offices with the FBI Virtual Academy approval process. The heart of the issue had to do with the Field Office's implementation and allocation of resources to support the training, not the application itself. Lastly, one other issue that affected the full implementation of the FBI Virtual Academy was the e-mail capability. The Virtual Academy must reference a Simple Mail Transfer Protocol gateway on the network to transport e-mail to the end users. The LMS is currently operating without this e-mail capability until the Trilogy implementation of Exchange.

(b) The FBI has one Training Plan for Trilogy. Core technology training is being acquired for the Information Technology Specialist (ITS) and Electronic Technician (ET) personnel enhance their skills, necessary to operate and maintain the software and hardware deployed by Trilogy. This core technology training for EOC personnel is being coordinated by the EOC Program Manager. Vendors have been procured to provide instructional services in core technical areas to the ITS personnel at each deployment site. The ET Training Program, which has been in existence for 25 years and is well established, has been upgraded to accommodate the new TNC/IPC equipment and technology courses, as well. This program is servicing the core technology training for the ET staff.

The Trilogy IPC/TNC program enhances and compliments this core technology training by providing CBT courses and technical procedural training at the time of IPC/TNC Full Site Capability deployment. The procedural training will be specific to the duties and responsibilities of the ITS and ET population, both in the field and EOC, with respect to the Trilogy IPC/TNC implementation of system maintenance and administrator functions. Existing FBI video-teleconferencing (VTC) facilities will be used to instruct the field ITS and ET staff. Considering the disperse

geographical locations of the more than 800 IT support personnel, this training delivery approach presents a more cost-effective means than the traditional face-to-face instructor-led training. The VTC capability provides the capability to deliver instructor-led training from a single location while participants at multiple remote sites can receive the broadcast signal simultaneously. A video recording of the training will also be provided to each site as a back up to the VTC delivery since twenty-seven of the fifty-six Field Offices do not currently possess VTC capability. The training delivery method for the EOC staff located at FBI Headquarters and Fort Monmouth, NJ, will be face-to-face instructor-led training. CBT courses covering the IPC/TNC software and hardware technologies will also be available via the FBI Virtual Academy LMS.

Recommendation Number 28, Page 113: We recommend that the Director of the FBI: Initiate action to complete the Extended Fast Track deployment timely by: (a) delivering the remaining quantities of Extended Fast Track desktop computers, and (b) procuring sufficient quantities of fiber optic cables.

Response: The FBI agrees with Part (a) of this recommendation. The remaining Extended Fast Track desktop computers will be shipped to all sites except New York City by December 31,2002. The remaining computers for New York City will be shipped in February 2003 after they have completed the upgrade of their internal fiber cable plant.

The FBI agrees that sufficient quantities of fiber optic cables must be procured for extended Fast Track to be successful. Trilogy funded the Back Bone fiber optic upgrade at one Field Office, Los Angeles, but this was a one time expense, made to meet critical schedule constraints. Since Trilogy did not budget for fiber optic cable upgrades, the FBI has decided to pay for this requirement from other FBI funding.

Recommendation Number 29, Page 113: We recommend that the Director of the FBI: Initiate action to: (a) procure adequate trouble-shooting equipment for Trilogy architecture, and (b) complete timely development of FBI unique macros for MS Word.

Response: The FBI agrees with Part (a) of this recommendation. Once the EOC is operational, adequate trouble shooting equipment for Trilogy will be in place and operational.

The FBI disagrees with Part (b) of this recommendation. The FBI has chosen to use a Web based approach for

submissions previously supported by Word Perfect Macros. Therefore, there will be no Macro development required for Microsoft Word.

Recommendation Number 30, Page 118: We recommend that the Director of the FBI ensures: The IT Strategic Plan and Performance Plans are updated to: (1) Fully integrate these plans with the FBI's ITIM Process; and (2) include those performance goals and indicators included in DOJ's IT Strategic Plan.

Response: The FBI agrees with this recommendation and concurs with the advice that the ITIM process should be fully integrated into future IT and performance plans. The FBI intends to complete an IT Strategic Planning process by fourth quarter FY 2003 that is fully part of the ITIM overall framework. The ITIM Program Office will be fully involved in the IT Strategic Planning efforts. The resulting IT Strategic Plan will be aligned with the FBI's operational strategic plan.

Sensitivity Review Response: The review found no sensitive or classified information related to IT systems, however, this review did not cover sensitive information related to general FBI operational security. It is requested that the report be classified as For Official Use Only (FOUO) or Limited Official Use (LOU).

APPENDIX 8

OIG, AUDIT DIVISION ANALYSES AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

In its response to the draft report, the FBI requested that this report be classified For Official Use Only or Limited Official Use. However, in a sensitivity review conducted prior to issuance of the final report, the FBI did not request classification of the report or limitation of its distribution. Consequently, this report is unclassified and not restricted in its distribution.

Recommendation Number:

1. **Resolved.** This recommendation is resolved based on the FBI's agreement to plan for and take more timely action to allow board members and other ITIM users to execute assigned responsibilities competently. This recommendation can be closed when we receive documentation demonstrating that: (a) the ITIM Program Office has established regularly scheduled meetings for the investment boards with standing agendas of items to be discussed, and (b) the ITIM Program Office maintains an up-to-date list of items requiring board member action and the status of those items.

2. **Resolved.** This recommendation is resolved based on the FBI's agreement to ensure that all members of the IT investment boards receive sufficient education and training to execute assigned responsibilities effectively. The FBI's response states that additional training will be held in the second and third quarters of FY 2003; however, it does not explicitly state that education and training plans will be developed. This recommendation can be closed when we receive: (a) the ratified Roles and Responsibilities documents dated June 2002 that specifically identify the roles and responsibilities for each investment board member, and (b) education and training plans to ensure board members acquire the required core competencies.

3. **Resolved.** This recommendation is resolved based on the FBI's agreement to ensure FBI IT project mangers consistently follow official project management guidance. However, the FBI's response does not indicate a date when such a process will be established. We request that in its next corrective action correspondence the FBI provide a

timeframe for implementation of this recommendation. This recommendation can be closed when we receive documentation that official project management guidance has been implemented and consistently followed.

4. **Resolved.** This recommendation is resolved based on the FBI's agreement to develop written policies and procedures for management oversight of IT projects for use by the investment review boards. The FBI's response indicates that detailed written policies will be completed in the third quarter of FY 2003. This recommendation can be closed when we receive a copy of the written policies and procedures.

5. **Resolved.** This recommendation is resolved based on the FBI's agreement to support the IT investment review boards with a centralized project management office that operates in accordance with ITIM policies and procedures. The FBI's response indicates that a centralized project management office has been established and will be supporting the investment review boards during the Control phase of the ITIM pilot test.[67] This recommendation can be closed when we receive documentation such as organization charts, charters, and policy guidance demonstrating that the centralized project management office has been established and operates in accordance with ITIM policies and procedures.

6. **Resolved.** This recommendation is resolved based on the FBI's agreement to develop a project management plan for each IT project, approved by the Project Oversight Committee, that includes cost and schedule controls. While the FBI's response indicates that the centralized project management office will develop project management plans, it is not clear when these actions will be initiated. We request that in its next corrective action correspondence the FBI provide a timeframe for implementation of this recommendation. This recommendation can be closed when we receive documentation demonstrating that each IT project has a project management plan approved by the Program Oversight Committee.

7. **Resolved.** This recommendation is resolved based on the FBI's agreement to ensure that information in the IT asset inventory is

[67] The FBI's response states that the roll-out of the Control phase is expected to be completed by the fourth quarter of FY 2003.

made available to, and used by, the boards. The FBI's response indicates that an assessment of the IT asset inventory will initially be shared with the boards in the third quarter of FY 2003. This recommendation can be closed when we receive documentation demonstrating that the IT asset inventory is used by the boards as an investment decision-making tool.

8. **Resolved.** This recommendation is resolved based on the FBI's agreement to execute, by the fourth quarter of FY 2003, the key practice activities necessary for the investment review boards to maintain effective oversight of IT projects. These key practices are:

   - providing each project's up-to-date cost and schedule data to the appropriate IT investment board;

   - establishing criteria for the boards to review each IT project's performance by comparing actual cost and schedule data to expectations;

   - performing special reviews of projects that have not met predetermined performance standards;

   - defining, documenting, and agreeing to corrective actions for each under-performing project by the appropriate IT investment board and project manager; and

   - tracking and implementing corrective actions until the desired outcome is achieved.

   This recommendation can be closed when we receive documentation demonstrating that the five key practice activities listed above have been executed.

9. **Resolved.** This recommendation is resolved based on the FBI's agreement to ensure progress toward completing the IT asset inventory is monitored. The FBI's response states that the established deadline for completing and validating the IT inventory is end of the second quarter of FY 2003. This recommendation can be closed when we receive documentation demonstrating that progress toward completion is evaluated.

10. **Resolved.** This recommendation is resolved based on the FBI's agreement to implement processes that ensure: (a) subsequent changes to IT projects and systems are identified and documented in the inventory, (b) information from the inventory is available on demand to decision-makers and other affected parties, and (c) the IT project and system inventory and its information records are maintained to contribute to future investment selections and assessments. This recommendation can be closed when we receive documentation demonstrating that the processes have been implemented. The FBI's response indicates that periodic updates to the IT inventory are planned for the fourth quarter of FY 2003.

11. **Resolved**. This recommendation is resolved based on the FBI's agreement to develop written policies and procedures for identifying the business needs (and the associated users) for each IT project. The FBI's response states that since March 2002, the Concept Paper and Exhibit 300 have been used to standardize the documentation of the business case. While we agree that these forms can be used to document the business needs and users of IT projects, we do not agree that these forms are sufficient evidence that a policy or procedure exists. This recommendation can be closed when we receive a copy of the written policies and procedures for identifying the business needs and users of IT projects.

12. **Resolved.** This recommendation is resolved based on the FBI's agreement to train ITIM users in identifying business needs and associated users. While the FBI's response states that training for the Select phase was completed in March 2002, and that additional training will be held when the Control and Evaluate phases are rolled out (second and third quarters of FY 2003, respectively), it does not specify that the training encompasses business needs identification. This recommendation can be closed we receive documentation demonstrating that such training is taking place.

13. **Resolved.** This recommendation is resolved based on the FBI's agreement to ensure identified users participate in project management throughout a project's life-cycle. The FBI's response states that the project management office will institute procedures to ensure user involvement throughout a project's life-cycle, but does not specify when these procedures will be instituted. We request that in its next corrective action correspondence the FBI provide a timeframe

for implementation of this recommendation. This recommendation can be closed when we receive documentation demonstrating that the FBI instituted procedures requiring participation of end users throughout the project's life-cycle.

14. **Resolved.** This recommendation is resolved based on the FBI's agreement to ensure the ITIM process applies to all proposals, including those funded through the FBI's base funding. The FBI's response states that base funding requests are planned to be included in the FY 2003 Select phase. This recommendation can be closed when we receive documentation demonstrating that the ITIM process has been applied to all proposals.

15. **Resolved.** This recommendation is resolved based on the FBI's agreement to provide sufficient staffing to the ITIM Program Office, as recommended in the Post-Implementation Review. Although the FBI's response states that six additional full-time staff have been requested for the ITIM Program Office, it did not specify when such positions are expected to be filled. We request that in its next corrective action correspondence the FBI provide a timeframe for implementation of this recommendation. This recommendation can be closed when we receive documentation demonstrating that the staffing requests have been fulfilled.

16. **Resolved.** This recommendation is resolved based on the FBI's response stating that all recommendations set forth in the Post-Implementation Review relating to expanding policies and procedures were implemented by September 2002. This recommendation can be closed when we receive documentation demonstrating that the policies and procedures have been implemented.

17. **Resolved.** This recommendation is resolved based on the FBI's response that input from various ITIM users was incorporated into the design of the Control and Evaluate phases through interviews and working group sessions completed in September 2002. This recommendation can be closed when we receive documentation demonstrating that such working group sessions were conducted and that input was incorporated.

18. **Resolved.** This recommendation is resolved based on the FBI's agreement to modify the ITIM process so that the Technical Review

Board and Enterprise Architecture Technical Committee perform a business architecture compliance review of IT proposals to ensure these proposals support the missions of the FBI. The FBI's response states that this modification will be completed by the third quarter of FY 2003. This recommendation can be closed when we receive a copy of the modified ITIM process.

19. **Resolved.** This recommendation is resolved based on the FBI's agreement to prepare a plan that specifically details how the project management office will support the ITIM process. However, the FBI's response did not specify when this plan will be completed. We request that in its next corrective action correspondence the FBI provide a timeframe for implementation of this recommendation. This recommendation can be closed when we receive a copy of the completed plan.

20. **Resolved.** This recommendation is resolved based on the FBI's agreement to develop and implement a plan detailing how and when it will integrate the ITIM process with a system development life-cycle methodology. Although the FBI's response indicates that the project management office will integrate the ITIM process with a system development life-cycle methodology, it does not specify when this will be accomplished. We request that in its next corrective action correspondence the FBI provide a timeframe for implementation of this recommendation. This recommendation can be closed when we receive documentation demonstrating that this integration has been completed.

21. **Resolved.** This recommendation is resolved based on the FBI's agreement to continue its efforts to establish a comprehensive enterprise architecture. The FBI's response states that it has a target to implement the first phase of a world-class enterprise architecture framework by April 2003. This recommendation can be closed when we receive a documentation demonstrating that the first phase of the enterprise architecture has been developed and a maturation plan is in place.

22. **Resolved.** This recommendation is resolved based on the FBI's agreement to establish cost, schedule, technical, and performance baselines for Trilogy and track significant deviations from these baselines. The FBI's response states that baselines will be established

once the current Engineering Change Proposals are negotiated, although no target dates were provided. We request that in its next corrective action correspondence the FBI provide a timeframe for implementation of this recommendation. This recommendation can be closed when we receive documentation demonstrating that the baselines have been established and are being monitored.

23. **Resolved.** This recommendation is resolved based on the FBI's agreement to adequately define, document, and share technical requirements for Trilogy. The FBI's response states that functional requirements have been defined for Trilogy's User Application Component. This recommendation can be closed when we receive documentation demonstrating that the technical requirements for the User Application Component have been adequately defined, documented, and shared with appropriate users.

24. **Resolved.** This recommendation is resolved based on the FBI's agreement to prepare an action plan to address the risks identified by the three internal reports on Trilogy by December 31, 2002. This recommendation can be closed when we receive a copy of the approved action plans and documentation demonstrating that the plans are being monitored for implementation.

25. **Resolved.** This recommendation is resolved based on the FBI's agreement with our recommendation. The FBI's response states that a successful process was used for the site installation schedule for the Trilogy project. However, we do not believe that the initial site survey utilized in the Trilogy deployment is an adequate process to submit input and receive feedback from FBI field offices. Our position is that a more comprehensive process could have mitigated the lack of clear communication between FBI Headquarters and field offices that caused confusion over the number of desktop computers to be delivered and shortages of fiber optic cable. This recommendation can be closed when we receive documentation demonstrating that such a process has been established for future IT deployments.

26. **Resolved.** This recommendation is resolved based on the FBI's agreement to remedy contractor deficiencies associated with (a) operation of the service support center, and (b) maintenance support for Trilogy architecture. This recommendation can be closed

when we receive documentation regarding the new maintenance contract and reductions in outstanding trouble tickets.

27. **Resolved.** This recommendation is resolved based on the FBI's agreement to enhance employee training by: (a) remedying problems associated with the FBI's on-line training system, and (b) developing a training plan specifically tailored to information technology specialists and electronic technicians. This recommendation can be closed when we receive: (a) documentation demonstrating that the outstanding issues with the on-line training system have been resolved, and (b) documentation of the Trilogy training received by the information technology specialists and electronic technicians regarding Trilogy software and hardware.

28. **Resolved.** This recommendation is resolved based on the FBI's agreement to: (a) deliver the remaining Extended Fast Track desktop computers to all sites except New York City by December 31, 2002, and New York City by February 2002, and (b) obtain sufficient fiber optic cable from other FBI funding. This recommendation can be closed when we receive documentation demonstrating that: (a) the remaining Extended Fast Track desktop computers have been deployed, and (b) sufficient fiber optic cable has been obtained.

29. **Resolved.** This recommendation is resolved based on the FBI's agreement to: (a) procure adequate trouble-shooting equipment for Trilogy architecture when the Enterprise Operations Center is operational, and (b) choose a web-based approach for submissions previously supported by Word Perfect macros. While the FBI disagreed with the original part (b) of this recommendation (that it "complete timely development of FBI unique macros for Microsoft Word"), it offered the acceptable alternative action of web-based submissions. However, the FBI did not provide estimated completion dates for these planned actions. We request that in its next corrective action correspondence the FBI provide a timeframe for implementation of this recommendation. This recommendation can be closed when we receive documentation demonstrating that: (a) adequate trouble-shooting equipment for Trilogy equipment has been procured, and (b) a web-based approach has been established to replace Word Perfect macros.

30. **Resolved.** This recommendation is resolved based on the FBI's agreement to update the IT strategic and performance plans so that the plans: (a) are fully integrated with the FBI's ITIM process, and (b) include those performance goals and indicators included in the DOJ's IT Strategic Plan. The FBI's response states that its IT Strategic Planning process will be updated and integrated with the ITIM framework by the fourth quarter of FY 2003. However, the response does not state that the FBI's IT Strategic Planning process will incorporate performance goals and indicators included in the DOJ's IT Strategic Plan. This recommendation can be closed we receive a copy of the updated Strategic Planning process that includes the above requirements.