THE FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF INFORMATION TECHNOLOGY RECOMMENDATIONS

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

Audit Report 03-36
September 2003

FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF INFORMATION TECHNOLOGY RECOMMENDATIONS

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. For FY 2003, the FBI allocated nearly $606 million to information technology projects.

As computer technology has advanced, federal agencies have become increasingly dependent on information systems to carry out operations and process, maintain, and report essential information. The FBI's computerized information systems affect many mission-critical activities, such as financial management, security of sensitive and classified data, and investigative work.

Recognizing the importance and vulnerability of data processed, maintained and reported by the FBI, the Office of the Inspector General (OIG), the General Accounting Office (GAO), and other entities have conducted audits, investigations, and reviews of the FBI's management of IT. For years, reviews have found major weaknesses associated with the FBI's IT. The FBI has made upgrading its information technology one of its top ten priorities.

To assess the FBI's progress in improving its IT, the OIG conducted this audit of the FBI's implementation of prior OIG and GAO recommendations. To perform our audit, we conducted 27 interviews with officials from the FBI, OIG, and GAO. The FBI officials interviewed were from the Inspection Division, Information Resources Division, and National Infrastructure Protection Center. Additionally, we reviewed over 100 documents including prior GAO and OIG reports, Congressional testimony, and documentation on the FBI's process for tracking the resolution of recommendations.

1. Policies and Procedures for Following-Up on Report Recommendations

The Office of Management and Budget (OMB) and DOJ have issued policies and procedures for following-up on recommendations of audit reports. According to OMB Circular A-50, audit follow-up is an integral part of good management, and is a shared responsibility of agency management and auditors. OMB Circular A-50 requires agencies to establish systems to assure the prompt and proper resolution and implementation of audit recommendations. These systems are to provide for a complete record of action taken on both monetary and non-monetary findings and recommendations.

Department of Justice Order 2900.6A, Audit Follow-Up and Resolution, established Departmental policies and criteria for the follow-up and resolution of audit findings and recommendations to ensure that all OIG audit reports are adequately and timely resolved, and that all resolution actions are consistent with the governing laws and regulations. The order states that the head of the DOJ component is responsible for overall audit resolution and follow-up activities within his or her organizational unit and is accountable to the Deputy Attorney General. Further, the DOJ component should establish an audit follow-up and resolution system that ensures written comments on audit findings and recommendations are made within four months after the issuance of the report.

The order also states that DOJ components should assign a high priority to the immediate implementation of the order so that the DOJ will be in full compliance with the legislative and regulatory requirements pertaining to the timely resolution of audits. Although subjective, the timeliness of corrective actions is assessed on a recommendation-by-recommendation basis due to the inherent difficulties associated with implementing certain recommendations.

When issuing other OIG reports that contain recommendations, such as special investigations or reviews, the OIG elicits responses from components regarding planned corrective actions. When received by the OIG, the responses are reviewed to determine whether the planned corrective actions meet the intent of the recommendations. Periodically, the OIG makes subsequent inquiries with components to monitor the implementation of these actions. As with audit reports, component managers are ultimately responsible for ensuring that recommendations are implemented in a timely manner.

2. The FBI's Implementation of IT Recommendations

Since 1990, OIG reports have identified numerous deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training. While the FBI has implemented many of the recommendations contained in these reports (93 out of 148), significant further actions are necessary to ensure that the FBI's IT program effectively supports its mission. For example, recent audits and reviews conducted by the OIG have found repeated deficiencies with the FBI's IT control environment and compliance with information security requirements.

These repeated deficiencies indicate that, in the past, FBI management had not paid sufficient attention to improving its IT program. Until recently, the FBI lacked an effective system of management controls to ensure that recommendations issued by the OIG are implemented in a timely and consistent manner. However, current FBI leadership has stated that they are committed to enhancing controls to ensure recommendations are implemented in a consistent and timely manner. The FBI has recently established a system to facilitate the tracking and implementation of recommendations. Additionally, the FBI expects significant improvements from its current IT modernization efforts, which the FBI believes will correct many of the deficiencies identified by the OIG.

A. OIG Reports on the FBI's IT

To assess the FBI's progress in implementing recommendations directed toward improving its information technology, the audit examined the following OIG reports that related to the FBI's use and management of IT:

- the 1990 audit report on the FBI's automated data processing (ADP) controls;
- the 2002 audit report on the FBI's IT investment management (ITIM);
- five detailed reports issued in support of annual financial statement audits for FYs 1996 through 2001[1] on the FBI's control environment over its IT systems;

[1] The OIG issued one report for FYs 1996 and 1997.

- three audit reports pursuant to the Government Information Security Reform Act (GISRA) issued for FYs 2001 and 2002; and

- two special investigative reports that contained FBI IT-related recommendations issued in 1999 and 2002.

For the 1990 ADP audit report and the 2002 ITIM report, we examined similarities between the reports' findings to assess the FBI's progress in improving its IT. For the OIG's detailed IT reports, FY 2001 GISRA audit report, and special reports, we obtained the status of FBI IT-related recommendations. The table below summarizes the status of FBI IT-related recommendations contained in these reports.

Summary of the Status of IT Recommendations Issued to the FBI

Report Name	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
OIG Detailed Financial IT Reports	22	83	105
OIG FY 2001 GISRA Audit Report	17	6	23
OIG Special Reports	16	4	20
Total	**55**	**93**	**148**

Source: OIG analyses as of April 2003

The following sections provide background information on these reports and an assessment of the FBI's progress toward implementing IT-related recommendations contained in these reports.

(1) Reports on the FBI's ADP Controls and IT Investment Management

In 1990, the OIG issued an audit report entitled, "The FBI's Automatic Data Processing General Controls." This report found 11 major internal control weaknesses, many of which were still applicable 12 years later. Specifically, the report found the following.

1. The FBI's phased implementation of its 10-year Long Range Automation Strategy, scheduled for completion in 1990, was severely behind schedule.

2. 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.

3. The FBI had not developed and implemented a data architecture.[2]

4. The FBI had not adequately involved top management in FBI Headquarters (FBIHQ) or the field offices in systems development through an Executive Review Committee.

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

Many of the weaknesses identified in the 1990 report on ADP controls were mentioned again in the 2002 audit report on the FBI's ITIM. In December 2002, the OIG issued a report entitled, "The FBI's Management of IT Investments." The OIG concluded that the FBI had not effectively managed its IT investments because it had not fully implemented the management processes associated with successful IT investments.

The ITIM report contained 30 recommendations directed toward improving the FBI's management of its IT investments. Because our evaluation of the FBI's progress toward implementing recommendations was close to the final issuance of the ITIM report, we did not assess the FBI's progress in implementing the recommendations. However, our 2002 ITIM report found that many of the weaknesses described in the 1990 report on the FBI's ADP controls still existed.

- The FBI's IT infrastructure was severely outdated.

- The FBI's Information Resources Management program was decentralized. The FBI had completed several restructurings, including one in February 2002 that was intended to give the Information Resources Management program more authority over the divisions that manage IT.

- The FBI still had not completed an enterprise architecture framework, which included the technical and data architecture.

- The FBI did not have formally established IT investment review boards or committees until March 2002.

[2] Data architecture is the identification and definition of major types of data within an organization.

- The FBI's major investigative systems remained labor intensive, complex, non-user friendly, and many special agents still did not use these systems.

The OIG concluded that the FBI's ability to completely and timely implement the 30 recommendations listed in the ITIM report will, in part, depend on management's commitment to do so. This management commitment must be incorporated into a comprehensive process to ensure that the recommendations are tracked and implemented.

(2) Reports on the FBI's Control Environment over its Financial IT Systems

The OIG conducts annual financial statement audits of the FBI, with the most recent report covering FY 2001. Financial statement audits are intended to play a central role in (1) providing more reliable and useful financial information to decision-makers, and (2) improving the adequacy of internal controls and underlying financial management systems. In support of the FBI's annual financial statement audits, the OIG has issued detailed reports since FY 1996 on the effectiveness of the FBI's general and application controls over IT systems used to process financial transactions.

To conduct these reviews, the OIG used the GAO's Federal Information System Controls Audit Manual (FISCAM). The FISCAM describes the computer-related controls by category that auditors should consider when assessing the integrity, confidentiality, and availability of computerized data.

We found that the FBI made progress in correcting deficiencies identified in the detailed reports supporting the annual financial statement audits from FY 1996 to 2001. Of the 105 recommendations contained in these reports, 83 have been implemented and closed, and 22 are still open. The following table summarizes the status of the FBI's IT control environment recommendations by FISCAM category.

Status of the FBI's Financial IT Control Environment
Recommendations by FISCAM Category

FISCAM Category	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Entity-Wide Security Program Planning and Management Controls	2	6	8
Access Controls	10	32	42
Application Software Development and Change Controls	2	6	8
System Software Controls	0	7	7
Segregation of Duty Controls	1	4	5
Service Continuity Controls	2	15	17
Application Controls	5	10	15
Other Financial-Related IT Areas[3]	0	3	3
Total	**22**	**83**	**105**

Source: OIG analyses as of April 2003

By implementing 83 of the recommendations, the FBI improved its IT internal control environment. The FY 2001 report did not contain any system software control deficiencies.[4] The FBI also made progress toward correcting deficiencies in entity-wide security program planning, access controls, application software development and change controls, segregation of duties, service continuity, and application controls.

Despite the progress, however, as of April 2003 material weaknesses[5] remained in the following general control areas:

[3] These recommendations were not identified by FISCAM categories.

[4] The FISCAM distinguishes system software controls from application software development and change controls. Beginning on page 12, we provide more detailed information on these general control areas.

[5] As defined by the American Institute of Certified Public Accountants, a material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected by employees in the normal course of performing their assigned functions.

- entity-wide security program planning and management – increasing the risk that the integrity of sensitive information can be compromised;

- access controls – increasing the risk of erroneous or fraudulent financial transactions; and

- application software development and change controls –increasing the risk of inaccurate and unauthorized software changes.

In addition to these material weaknesses, other vulnerabilities existed in the following internal control areas:

- segregation of duty controls – increasing the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed;

- service continuity controls – increasing the risk that during an extended outage or disaster, information system processing functions and vital business operations will be damaged and unable to function since critical information and computer resources would be unavailable or inaccessible; and

- application controls – increasing the risk of inaccurate valuation or allocation of data, and unauthorized transactions.

We also noted that 30 of the both open and closed recommendations were repeated in subsequent reports on the FBI's financial IT systems' control environment. For example, the OIG's review for FY 1998 reported that an automated tool was used to perform an assessment of the technical controls over the FBI's Finance Division Local Area Networks (LAN). The assessment found weaknesses in three areas of security: account restrictions, system monitoring, and data confidentiality. In FY 1999, another automated tool was used to perform the assessment of the technical controls over the FBI's Finance Division LANs. Although corrective action had been initiated on the prior weaknesses found, the OIG reported that these weaknesses still existed during FY 1999. The FY 2000 review stated that auditing remained disabled on the Finance Division's Windows NT and Novell NetWare environments. In addition, according to the OIG FY 2001 review, although FBI management had stated that corrective actions have been taken with respect to the recommended settings for account restrictions, system monitoring, and data confidentiality, the conditions

continued to be identified during the annual financial statement audit process. Because of the uncorrected deficiencies identified in these audits, the FBI is at increased risk to failures in its financial management and computer security functions.

(3) Computer Security Reports in Response to GISRA

Beginning in FY 2001, the OIG was required by GISRA to perform an independent evaluation of the DOJ's information security program and practices using standards developed by the GAO and the National Institute of Standards and Technology (NIST).[6] In May 2002, pursuant to GISRA, the OIG issued an audit report on the FBI's investigative and administrative mainframe systems.

The NIST, in conjunction with GISRA, issued guidance detailing the specific controls that should be documented by federal agencies in their system security plan. The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.

The NIST separated the security plan controls into three major control areas: (1) management controls, (2) operational controls, and (3) technical controls. Within each of the three control areas, there are a number of subordinate categories of controls. For example, technical controls include password management, logon management, account integrity management, and system auditing management.

We found that the FBI made some progress in correcting deficiencies reported in the OIG FY 2001 GISRA audit. Of the 23 recommendations contained in the report, 6 have been implemented and closed, and 17 are still open. The following table summarizes the status of the FBI's FY 2001 GISRA audit report recommendations by category.

[6] The NIST is a non-regulatory entity of the U.S. Department of Commerce.

Status of the FBI's FY 2001 GISRA Report Recommendations by NIST Category

NIST Category	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Management Controls	4	2	6
Operational Controls	2	2	4
Technical Controls	11	2	13
Total	**17**	**6**	**23**

Source: OIG analyses as of April 2003

By implementing six of the recommendations, the FBI improved the security of its investigative and administrative mainframe systems at its Headquarters and Clarksburg Data Centers. These improvements included (a) defining and documenting all criticality levels used to classify applications, (b) establishing optimal operating system capacities and implementing procedures to alleviate the near capacity usage, (c) fully implementing and using the System Access Request function to document user logon and verify that user access is commensurate with assigned responsibilities, and (d) ensuring that the communication carrier signals are not connected to unencrypted network devices.

Despite the progress made, as of April 2003 vulnerabilities remained in the following areas:

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

The OIG assessed these vulnerabilities as a high-to-moderate risk for the protection of the FBI's administrative and investigative mainframe systems from unauthorized use, loss, or modification. These vulnerabilities occurred because 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 stated that the lack of timely and effective oversight from DOJ and FBI management caused inconsistencies in the implementation of security guidelines and resulted in a weakened security infrastructure.

The FY 2002 GISRA report on the Automated Case Support (ACS) and DRUGX systems, like the FY 2001 GISRA report, noted repeated deficiencies in general control areas. Specifically, vulnerabilities were noted within password management, logon management, account integrity management, system auditing management, and system patches. The report further stated that, if not corrected, these security vulnerabilities threaten the ACS system and its data with the potential for unauthorized use, loss, or modification.

According to the FY 2002 GISRA reports, the FBI did not maintain a system of recording, tracking progress, ensuring attention to, or determining the completion of action in response to any information security vulnerability uncovered during a non-OIG review. As a result, the FY 2002 GISRA reports recommended that the FBI determine the responsible organization for tracking and maintaining all vulnerabilities identified during audits and reviews. In addition, the reports recommended that the FBI develop a mechanism for tracking the vulnerabilities and the status of the associated corrective actions resulting from all IT audits and reviews. Since September 2002, the FBI has been developing new procedures and databases to assist with the audit resolution and follow-up process. FBI officials informed us that the Inspection Division now manages the audit follow-up and resolution process for both OIG and GAO audits. Additionally, for system audits, the FBI has reported that its Information Assurance Section has taken steps to centrally manage the status of vulnerabilities and corrective actions.

(4) Reports on Special Investigations of the FBI

Since 1998, the OIG has issued two special investigation reports containing significant FBI IT-related recommendations:

- the 1999 report on the DOJ's Campaign Finance Task Force investigation (Campaign Finance); and

- the 2002 report on the FBI's investigation into the Oklahoma City Bombing case (McVeigh).

These reports, among other issues, considered the policies and procedures related to the management of information within the FBI, the dissemination of the information to organizations outside the FBI, and the effectiveness of the information technology utilized by the FBI. The reports cited deficiencies in the FBI's management of IT, and provided 20 recommendations directed toward correcting these deficiencies.[7] The table below summarizes the status of the special investigation recommendations made to the FBI by report.

Status of Special Investigation Recommendations by Report

Report Name	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Campaign Finance Report	5	0	5
McVeigh Report	11	4	15
Total	**16**	**4**	**20**

Source: OIG analyses as of April 2003

We found the FBI's current and planned corrective actions, including the implementation of Trilogy, has the potential to address 16 of the 20 recommendations that we examined from the Campaign Finance and McVeigh reports. However, the ultimate success of Trilogy will not be determined until at least June 2004 when the final phases of the project are scheduled for completion.

The following section provides background information on Trilogy, since its successful completion is critical to not only addressing OIG recommendations, but also to the future of the FBI's IT program.

(a) Background on Trilogy

Trilogy is an IT modernization project designed to upgrade the FBI's: (1) hardware and software or Information Presentation Component (IPC), (2) communication networks or Transportation Network Component (TNC), and (3) User Application Component (UAC). The IPC and TNC upgrades will provide the physical infrastructure needed to run the applications from the UAC. The UAC is intended to replace five of the FBI's primary investigative applications in order to reduce agents' reliance on paperwork and improve efficiency. Through the creation of the Virtual Case File (VCF), a web-based

[7] We included recommendations related to document management because FBI documents are generally produced electronically or managed in automated databases and systems.

"point-and-click" case management system, agents are expected to have multi-media capability that will allow them to scan documents, photos, and other electronic media into the case file.

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 3-year period. In January 2002, Congress supplemented the FY 2002 Trilogy budget with $78 million to expedite the deployment of all three components. This supplemental appropriation increased the total funding of Trilogy to approximately $458 million. Even with these additional funds, the FBI missed its July 2002 milestone date for completing the "Fast Track" portion of the IPC and TNC phases.

In April 2003, the FBI Director reported to the Senate Appropriations Committee that over 21,000 new desktop computers and nearly 5,000 printers and scanners have been deployed (IPC phase). Additionally, the FBI reported that it completed the Trilogy Wide Area Network (TNC phase) on March 28, 2003. The new network, which has been deployed to 622 sites, provides increased bandwidth and three layers of security. According to the FBI, the network is highly expandable, so additional capacity or even additional sites could be added as needed. This network replaces the FBI's dated local area and wide area networks, enabling FBI personnel to transmit data at much greater speeds. Further, the FBI expects to use the network to transport the Investigative Data Warehouse, which will link 31 FBI databases for single-portal searches and data mining. Also, the network lays the foundation for improved information sharing with partner agencies, and other new applications, such as the VCF.

The VCF will 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 FBI expects to deploy the VCF in three releases. The initial VCF release will consolidate data from the current ACS and IntelPlus systems and 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 VCF 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 and third releases are intended to upgrade three other investigative applications into the VCF: the Integrated Intelligence Information Application (IIIA), Telephone Application, and Criminal Law

Enforcement Application. These releases have a targeted completion date of June 2004 and are 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 that are connected to the Investigative Data Warehouse.

The OIG ITIM report, issued in December 2002, stated that the VCF, which is recognized by FBI officials as the most important aspect of the Trilogy project in terms of improving agent performance, was at high risk of not being completed within the funding levels appropriated by Congress. FBI officials confirmed the OIG's assessment in January 2003 when they told us that an additional $138 million[8] was needed to complete Trilogy, bringing the total project cost to $596 million. Despite the cost overruns, FBI officials stated that they still expect to deliver the first release of VCF in December 2003, and that funding for the second and third releases of the VCF has been secured.

The following sections provide further details on the IT and document management related deficiencies noted in Campaign Finance and McVeigh reports, as well as an assessment of the how the VCF will address these deficiencies.

(b) Campaign Finance Report

In July 1999, the OIG issued a report entitled, "Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation" (Campaign Finance). In response to a request by the Attorney General, the OIG reviewed the FBI's practices for disseminating intelligence information associated with the Campaign Finance Task Force (Task Force) investigation.

With respect to the use and maintenance of the FBI's computer database systems, deficiencies were noted in: the Task Force's familiarity with the FBI's databases, the FBI's practices and policies that limited the usefulness of the databases, the training of FBI personnel on the ACS system, and the entry of foreign names into the FBI's databases. These findings highlighted the need for FBI and Task Force personnel to be familiar with information search techniques within the FBI's databases, how information should be entered into the databases in order to take advantage

[8] Of this amount, $57 million was needed for the VCF.

of search capabilities, and potential errors in data entry to ensure that all possible searches within the databases are conducted. Of the Campaign Finance report's 18 recommendations, 5 pertained to the IT-related deficiencies. These five recommendations related to revising the FBI's ACS and IIIA systems to require the uploading of documents and mandatory indexing of names, and training the users of these systems.

Regarding the uploading of documents, the FBI issued Electronic Communications (EC) in July 2000 and June 2002 that required all e-mails and ECs to be uploaded into the ACS system, unless otherwise prohibited by their sensitive nature. Additionally, FBI officials stated that with the VCF, documents will have to be uploaded since the VCF will contain all official records and case files.

Regarding the mandatory indexing of names, FBI officials stated that the VCF will facilitate indexing on various web-based documents by providing data fields in searchable databases. The index of data fields, except for narrative fields, will be automatically created once the document is approved and entered into the VCF. Agents and analysts can then search the index of data fields by using search screens or viewing the serialized document.

Regarding training, FBI officials said that they increased the ACS system training for veteran agents and have plans in place to train FBI employees and task force members on the VCF. Additionally, the FBI continues to offer training on the "Romanization" of foreign names, including those in Arabic and Chinese.

Despite the FBI's progress in taking corrective actions, a more comprehensive enterprise-wide solution to the underlying deficiencies will not occur until the VCF is implemented. As a result, some of these deficiencies have gone uncorrected for over three years.

(c) McVeigh Report

In March 2002, the OIG issued a report entitled, "An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case" (McVeigh). This report analyzed the causes for the belated production of many documents in the Oklahoma City bombing case.

The McVeigh report concluded that the belated production of case-related documents resulted in part from the following long-standing problems at the FBI: (1) antiquated and inefficient computer systems,

(2) inattention to information management, and (3) inadequate quality control systems. The report further stated that the FBI's troubled information management systems were likely to have a continuing negative effect on the FBI's ability to properly investigate crimes.

The report stated that the FBI had not given sufficient attention to correcting deficiencies in information management and the ACS system. The findings of the report relating to information technology showed that the ACS system is extraordinarily difficult to use, has significant deficiencies, and is not suitable for the FBI in the 21st century. The report noted that inefficiencies and complexities with the ACS system, combined with the lack of a true information management system, were significant factors in the FBI's failure to provide hundreds of investigative documents to the defendants in the Oklahoma City bombing case. To overcome these problems, the report made recommendations on how future information systems should be developed.

The McVeigh report provided 21 recommendations to the FBI, 15 of which directly related to IT. Eleven of the fifteen recommendations pertain to correcting deficiencies associated with the FBI's investigative systems, including the tracking of leads and other records management policies. FBI officials have stated that the VCF, when implemented, will address these 11 recommendations.

In May 2003, FBI officials stated that agents will be required to use the VCF, since all official case records and files (up to the Secret level) will be within the application. According to the FBI, unlike the currently used ACS system, agents will not be able to circumvent the use of the VCF. However, the FBI still has not finalized its policies for how agents will utilize VCF from remote locations. Additionally, the VCF has only been approved for use up to the Secret classification level, so Top Secret and Sensitive Compartmented Information (SCI) records will still be maintained in a SCI facility.

FBI officials stated that the VCF will streamline the workflow process by including electronic signatures and reducing the number of required forms. Under the FBI's current investigative process, a case file is started by using one of the FBI's many different standardized forms. The use of these forms will be replaced by the "intake" function of the VCF, which will simplify the initiation of a case file by eliminating the use of these forms. As a result, the VCF will essentially replace all paper copies of investigative events.

According to FBI officials, the VCF will operate in a "point-and-click" web environment that will simplify the FBI's workflow process for document storage and retrieval. Further, FBI officials told us that the VCF's automated document creation, receipt, and management system will partially eliminate the need for traditional tracking systems. The VCF will include capabilities to scan into the case file any documents received from sources external to the FBI, as well as to capture summary descriptions of any documents and items, such as physical evidence, that cannot be stored electronically. The FBI's intent is to eventually track external items through a bar code identification system that would be placed upon a physical label on the external document and then linked to an electronic record. Additionally, FBI officials said that the Records Management Division (RMD) is establishing systems and processes to effectively track documents and records contained in FBI systems.

While the VCF will consolidate five of the FBI's investigative applications, FBI officials recognize that the VCF is only a starting point since numerous other investigative and application systems exist that could be integrated into the VCF. Additionally, because of unresolved connectivity issues, crisis management software may still need to be used by agents after the initial deployment of the VCF. The FBI is identifying and defining other databases and crisis management software that should be included in future VCF releases to maximize the efficiency of the workflow process. FBI officials told us that additional funding will be needed to solve the connectivity issues at remote locations, as well as consolidate and eliminate other databases and crisis management software.

We believe the FBI has demonstrated progress toward implementing these recommendations in the McVeigh report, based on its corrective actions taken to date and its plans for the VCF. However, 11 of these recommendations remain open since the adequacy of the FBI's corrective actions cannot be determined until the VCF has been completed. Because the FBI's ability to implement many IT recommendations and improve its IT program depends on the successful implementation of the VCF, the following sections discuss the factors affecting the success of the VCF.

(d) Factors Affecting the Success of the VCF

In our judgment, if the VCF can do what the FBI expects, it will represent a significant technological advancement from the ACS system. The VCF has the potential to reduce redundancy in searching multiple databases, improve the FBI's case file management, and maximize the use of information in the FBI's possession.

While the VCF has the potential to significantly improve the FBI's information technology, as well as its record management and investigative efficiency, the ultimate success of VCF depends on a number of different factors, including whether the VCF will meet its technical and performance expectations and be accepted and used by FBI employees.

1. Technical and Performance Expectations of the VCF

To ensure its success, the VCF must meet technical and performance expectations. As mentioned above, the Trilogy project has encountered significant cost overruns and schedule delays due to the FBI not following critical management processes. The OIG's ITIM report stated that these management problems contributed to difficulties with establishing the technical requirements for the VCF. Because the VCF is focused on making significant changes to five of the FBI's investigative systems, documentation for the exact configuration of these legacy systems was critical to designing the requirements for the VCF. Lack of documentation for the configuration of these five investigative systems 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 had to perform reverse engineering on five systems, there are limitations as to how rapidly the VCF can be developed and deployed.

As of April 2003, the FBI was still defining the technical requirements for the second and third releases of the VCF. Because the technical requirements had not yet been finalized and funding has not been approved, baselines for the VCF had not been established. We believe that the lack of technical, cost, and schedule baselines not only creates uncertainties for how much the VCF will cost and when it will be completed, but also how it will perform upon implementation.

2. Acceptance and Use of the VCF

If the VCF is to be a vehicle for moving the FBI's information management into the 21st century, it must be accepted and used throughout the FBI. Historically, the FBI has been a paper-driven organization. A goal of the VCF is to move toward a near paperless environment so the FBI can maximize the use of technology to digitally capture information for data management and control. According to FBI officials, the VCF is the first real change in the FBI's workflow and processes that originated in the 1950's. Director Mueller recently stated that "Trilogy [VCF] will change the FBI culture from paper to electronic."

As noted in the Campaign Finance and McVeigh reports, special agents did not always use the ACS system to manage their case files. For various reasons, they found alternative ways to manage case files. The VCF must be used by all special agents for the FBI to fully realize its benefits.

FBI officials told us that since the VCF will contain the official case files, agents will have to use it since there will be no other acceptable means to manage case files. However, FBI officials also acknowledged that because of unresolved connectivity issues at remote locations, agents may still need to use crisis management software such as Rapid Start.

B. Other Reports Relating to the FBI's IT Program

Three GAO reports that we examined also noted deficiencies with certain aspects of the FBI's IT program. The first report, entitled "Gun Control: Implementation of the National Instant Criminal Background Check System," stated in 1999 that the FBI did not properly accredit and certify the IT system. We later found that the system subsequently was certified and accredited on March 31, 2000. The second GAO report, entitled "Campaign Finance Task Force: Problems and Disagreements Initially Hampered Justice's Investigation," stated in 1999 that the FBI lacked an adequate information system that could manage and interrelate the evidence that had been gathered in relation the Campaign Task Force's investigations. These deficiencies were similar to those reported by the OIG's Campaign Finance report. The third report, entitled "Enterprise Architecture Use Across the Federal Government Can Be Improved," stated in 2002 that the FBI lacked a foundation for managing an enterprise architecture. The recently released OIG ITIM report reiterated the importance of having an established enterprise architecture when developing an IT investment management process. Although these GAO reports did not include any FBI IT-related recommendations, the reports provide further support that previously identified deficiencies continue to affect the FBI.

Other entities have also issued reports in recent years that include analyses of the FBI's IT management. One report relating to IT security was issued by the Webster Commission in March 2002, entitled "A Review of FBI Security Programs." The Commission, chaired by former FBI Director William H. Webster, was established to review the FBI's security practices in light of the espionage by FBI Supervisory Special Agent Robert Hanssen.

The report identified a wide range of problems affecting the FBI's computer systems and information security policies, including:

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

- 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 had been deficient because it had 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, and when audits were performed, audit logs were reviewed sporadically, if at all.

The Webster Commission's report concluded that these findings resulted from the FBI's lack of attention to IT security in developing and managing computer systems.

C. FBI's Process for Following-Up on Recommendations

Until recently, the FBI had not implemented an effective system of management controls to ensure that recommendations are resolved and implemented in a timely and consistent manner. FBI personnel told us that while a formal process to track and resolve recommendations did not exist prior to September 2002, an informal process was used. Upon the final issuance of an OIG or GAO report containing recommendations, the recommendations were forwarded to the various FBI Divisions. Someone within the Division was then assigned to respond to the recommendations until closure occurred. The FBI recognized that this informal process was not sufficient to ensure corrective actions were timely and responsive. Specifically, the FBI officials acknowledged that the informal process:

- was not documented in formal policies and procedures,

- was not adequately monitored by executive management and not kept up-to-date,

- used multiple applications,

- did not keep measures of timeliness and responsiveness, and

- did not provide for sufficient follow-up once the original response or corrective action plan was submitted.

According to the Deputy Assistant Director of the Inspection Division, high turnover within FBI management also contributed to problems with maintaining current responses to OIG and GAO reports. Under the informal process, when individuals left the FBI or were reassigned within the FBI, their replacements were not always made aware of recommendations or requests that were left pending. As a result, responses to recommendations and any related corrective action were often delayed, and the auditing or investigating agency had to again request a response to its recommendations.

The FBI recognized that improvements in its system of managing follow-up were needed to resolve and timely implement recommendations resulting from OIG and GAO reports. In September 2002, the FBI's Inspection Division began to establish a new management process to improve the FBI's timeliness and responsiveness of corrective actions resulting from OIG and GAO recommendations and to bring the FBI in compliance with applicable regulations (OMB Circular A-50 and DOJ Order 2900.6A) for the follow-up and resolution of audit recommendations. To facilitate the implementation of this new management process, the Inspection Division developed a database, referred to as the "Automated Response and Compliance System" (ARCS). According to FBI documentation, ARCS is an automated tool that is intended to:

- document and track audits and data requests from OIG, GAO, and others;

- track OIG and GAO audits, investigations, and reviews until closure; and

- provide status information to FBI's executive management on, or close to, a real time basis.

The FBI's new database tracks the receipt and resolution of audits, investigations, and data requests from OIG, GAO, and others. It also tracks the tasks associated with FBI's current engineering efforts. Among its functions, the database is intended to provide information to FBI managers on a regular basis to keep them informed of a report's progress and to ensure timely implementation of recommendations. However, this database does not include vulnerabilities generated by system audits required by GISRA. The FBI's Information Assurance Section has taken steps to develop a separate database to manage the status of system audit vulnerabilities.

In conjunction with the development of the ARCS database, the FBI has also developed policies and procedures for the Inspection Division's responsibilities for resolving OIG and GAO reports. These policies and procedures require the Inspection Division to assign a liaison for each report with outstanding recommendations or for scheduled audits and reviews. The liaison has the primary responsibility for entering information into the database, including deadlines for when tasks should be completed. The liaison also has the responsibility to ensure that the report is assigned to a "project manager" – who ensures that all tasks are assigned to appropriate FBI personnel. This control ensures that appropriate FBI personnel can be held accountable for taking timely corrective actions. The liaison monitors the completion of tasks and is instructed to send periodic e-mail notices when tasks are near their due date or past due. Additionally, Inspection Division management reviews the activities of the liaisons to ensure that they are adequately monitoring their assigned projects.

FBI officials said that the database, which is maintained on the FBI's intranet, generates reports for senior FBI management on upcoming suspense dates. For example, FBI Deputy Directors are required to perform quarterly reviews on their Division's progress in completing outstanding tasks. According to FBI officials, the Inspection Division Assistant Director uses reports generated by the ARCS database to discuss outstanding tasks at weekly executive meetings, which are attended by FBI Assistant Directors, Executive Assistant Directors, and the Director. These and other reports have been periodically forwarded to the Director, upon his request. FBI officials told us that the Director has taken a particular interest in the timeliness and responsiveness of the FBI's corrective actions, re-engineering efforts, and responses to Congressional requests. The Director asks to be notified, especially with regard to high profile reviews, when the FBI has not been timely and responsive in its planned actions.

While the FBI's database can be a useful tool for the FBI's establishment of a management process directed toward improving the timeliness and responsiveness of its corrective actions, the ultimate effectiveness of this system depends on formal and consistent oversight from senior FBI management. Thus far, however, the FBI has not promulgated written directives FBI-wide that instruct program managers and senior officials (outside of the Inspection Division) regarding their obligation to take corrective actions that will close recommendations. In our judgment, the FBI must develop and institute a formal written process that requires senior management oversight over the timeliness and responsiveness of recommendations. These written procedures should also incorporate the policies for tracking the status of vulnerabilities generated by system audits.

3. OIG Recommendations

In this report, we make three recommendations for the FBI to improve its implementation of IT recommendations. These recommendations are:

- Develop, document, and implement Bureau-wide procedures to follow-up and close audit and investigative recommendations (including those generated from system audits), in accordance with OMB Circular A-50 and DOJ Order 2900.6A.

- Ensure that the ARCS database is complete and includes recommendations from all sources of OIG audits and special reviews.

- Demonstrate through the timely closure of OIG audit and other recommendations that managers are being held accountable for taking corrective actions.

TABLE OF CONTENTS

INTRODUCTION

1. Background

The Federal Bureau of Investigation (FBI) 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 April 2003, 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 was nearly $4.3 billion for FY 2003.[9] Of this budget authority, $606 million was allocated to information technology (IT) projects.

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 FYs 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."

Additionally, in July 2002, the DOJ released an IT Strategic Plan that included the following goals:

- sharing information quickly, easily and appropriately — inside and outside the DOJ;
- securing and protecting information;
- providing reliable, trusted, and cost-effective IT services; and
- using IT to improve program effectiveness and performance.

[9] This figure excludes Federal Retiree and Health Benefit Costs.

To meet these goals, the DOJ's IT Strategic Plan focuses on four key areas considered to be the building blocks of the IT program: (1) IT infrastructure, (2) information security, (3) common solutions,[10] and (4) management roles and processes.[11]

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. Although the core missions of the FBI remain intact, the changes are intended to transform the Bureau's role from reactive to preventive. To accomplish this transition, FBI officials repeatedly have told Congress that new and improved IT is required to support a redesigned and refocused FBI. In testimony 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. Reports on the FBI's IT

Because of the significance of IT to the FBI's mission-critical activities, the Office of Inspector General (OIG) has issued numerous audits and special reviews over the past 12 years relating to the Bureau's IT management processes. These reports resulted from reviews of the FBI's internal controls of financial IT systems, compliance with the Government Information Security Reform Act (GISRA), and management of IT investments.

[10] According to the DOJ's IT Strategic Plan, common solutions help to achieve improved collaboration, secured information sharing, and work simplification through the use of shared applications and databases.

[11] According to the DOJ's IT Strategic Plan, management roles and processes refer to the DOJ's Chief Information Officer's responsibilities, which include: promulgating departmental IT policies, processes, and standards; formulating departmental IT strategic plans; developing, implementing, and maintaining an enterprise architecture; developing guidance for, reviewing, and making recommendations concerning, component IT budget requests; reviewing and monitoring the design and implementation of major IT projects; and providing shared departmental services.

Additionally, the OIG has conducted special reviews that considered the FBI's use of computer applications in its investigative activities. Both the OIG audit and special review reports have highlighted many IT deficiencies at the FBI and have provided recommendations directed toward improving those vulnerabilities.

Other entities (such as the General Accounting Office (GAO), private contractors, Congressional committees, and specially formed commissions) have conducted reviews that discuss the FBI's IT management practices, but do not necessarily contain IT-related recommendations. While the focus of our audit was to assess the FBI's progress in implementing IT recommendations, in Appendix 3 of this report we discuss the findings of reports issued by the GAO and the Commission for the Review of FBI Security Programs (Webster Commission) due to their relevance to the FBI's IT program.[12]

3. Policies and Procedures for Following-Up on Report Recommendations

The Office of Management and Budget (OMB) and DOJ have issued policies and procedures for following-up on recommendations of audit reports. According to OMB Circular A-50, audit follow-up is an integral part of good management, and is a shared responsibility of agency management officials and auditors. Corrective action taken by management on resolved findings and recommendations is essential to improving the effectiveness and efficiency of government operations. OMB Circular A-50 requires agencies to establish systems to assure the prompt and proper resolution and implementation of audit recommendations. These systems are to provide for a complete record of action taken on both monetary and non-monetary findings and recommendations.

The DOJ issued Order 2900.6A, Audit Follow-Up and Resolution, to establish the Departmental policies and criteria for the follow-up and resolution of audit findings and recommendations, to ensure that all OIG audit reports are adequately and timely resolved, and that all resolution actions are consistent with the governing laws and regulations. The order states that DOJ components should assign a high priority to the immediate implementation of the order so that the DOJ will be in full compliance with the legislative and regulatory requirements pertaining to the timely

[12] In March 2002, the Webster Commission issued its report entitled, "A Review of FBI Security Programs."

resolution of audits.

The order also states that the heads of DOJ components are responsible for overall audit resolution and follow-up activities within their organizations and are accountable to the Deputy Attorney General. Further, DOJ components should establish an audit follow-up and resolution system that ensures written comments on audit findings and recommendations are made within a 4-month period.

OIG audit reports generally contain recommendations that have a status of either open or closed. Open recommendations should be resolved[13] within six months of the final report issuance date. Recommendations are closed by the OIG when the OIG is satisfied that the component has taken the agreed upon corrective actions, or when the corrective action is waived. To determine if the agreed upon corrective actions were taken, the OIG may request that FBI officials provide documentation demonstrating that the stated corrective actions were completed. In other cases, the OIG may perform additional review to verify that the stated corrective actions were taken. Although subjective, the timeliness of corrective actions is assessed on a recommendation-by-recommendation basis due to the inherent difficulties associated with implementing certain recommendations.

Upon issuing other OIG reports that also contain recommendations, such as special investigations or reviews, the OIG elicits responses from components regarding planned corrective actions. When received by the OIG, the responses are reviewed to determine whether the planned corrective actions meet the intent of the recommendations. Periodically, the OIG makes inquiries with components to monitor the implementation of these actions. However, as with audit reports, component management is ultimately responsible for ensuring that recommendations are implemented in a timely manner.

[13] The OIG considers a recommendation to be "resolved" when agreement is reached with the component on the corrective actions that will be necessary to close the recommendation.

OIG FINDINGS AND RECOMMENDATIONS

Since 1990, OIG reports have found numerous deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training. While the FBI has implemented many of the OIG's IT recommendations (93 out of 148), significant further actions are necessary to ensure that the FBI's IT program effectively supports its mission. Recent audits and reviews conducted by the OIG have found repeated deficiencies in the FBI's IT control environment and compliance with information security requirements. These repeated deficiencies illustrate that, in the past, FBI management had not paid sufficient attention to improving its IT program. Until recently, the FBI lacked a system of management controls to ensure that recommendations issued by the OIG were implemented in a timely and consistent manner. Inadequate progress toward implementing IT recommendations and correcting deficiencies contributed to breaches in computer security and failures in mission-critical investigative activities. However, current FBI leadership has stated that they are committed to enhancing controls to ensure recommendations are implemented in a consistent and timely manner, and the FBI recently established a system to facilitate the tracking and implementation of recommendations. Additionally, the FBI expects significant improvements from its current IT modernization efforts, which the FBI believes will correct many of the deficiencies identified by the OIG.

1. OIG Reports on the FBI's IT

To assess the FBI's progress in implementing recommendations directed toward improving its information technology, this audit examined the following OIG reports that considered the FBI's use and management of IT:

- the 1990 report on the FBI's automated data processing (ADP) controls,

- the 2002 report on the FBI's IT investment management (ITIM),

- five reports issued for FYs 1996 through 2001 on the FBI's control environment over its financial IT systems,[14]

- three reports issued for FYs 2001 and 2002 specific to the FBI's compliance with GISRA, and

- two special review reports issued in 1999 and 2002 that contained FBI IT-related recommendations.

Although the FBI made measurable progress in implementing the OIG's IT recommendations contained in these reports (93 out of 148), it still must take significant actions to achieve a successful IT program. For the recommendations we examined, we assessed the status of the recommendations (whether open or closed). To accomplish our assessment, we reviewed the latest available correspondence between the OIG and FBI regarding actions required to close recommendations, and made inquiries with FBI officials.[15] We considered recommendations with a closed status to be implemented, based on the OIG's judgment that the requirements of the recommendation were met. As a result, we considered closed recommendations to be an indicator of the FBI's progress in addressing deficiencies. Yet, while closed recommendations can be an indicator of progress, the underlying deficiency may re-appear in future audits and reviews.

The following sections provide background information on these reports and an assessment of the FBI's progress toward implementing IT-related recommendations contained in them.[16]

A. Report on the FBI's ADP Controls

In 1990, the OIG issued a report entitled, "The FBI's Automatic Data Processing General Controls." The objectives of the audit were to determine whether the ADP general controls: (1) had been designed according to management direction and known legal requirements; and (2) were operating effectively to provide reliability of, and security over, the data being processed.

---

[14] The OIG issued one report for FYs 1996 and 1997.

[15] Unless otherwise noted, our review of correspondence was as of April 2003.

[16] The OIG recommendations that we examine are listed in Appendix 2. Appendix 2 also shows the status of the recommendations (whether open or closed), and a summary of the FBI's progress toward implementing the recommendations.

(1) Background on Report Findings

This report found 11 major internal control weaknesses, many of which still exist today. Specifically, the report found the following.

1. The FBI's phased implementation of its 10-year Long Range Automation Strategy, scheduled for completion in 1990, was severely behind schedule.

2. 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.

3. The FBI had not developed and implemented a data architecture.

4. The FBI had not adequately involved top management in FBI Headquarters (FBIHQ) or the field offices in systems development through an Executive Review Committee.

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

(2) FBI's Progress in Taking Corrective Actions

As discussed in more detail in the following section, the December 2002 OIG report entitled, "The FBI's Management of IT Investments," noted that many of the weaknesses identified in the 1990 report on ADP controls still existed 12 years later. Regarding the first weakness, the FBI's IT infrastructure is still severely outdated. Regarding the second weakness, the FBI has completed several restructurings, including one in February 2002 that was intended to give the Information Resources Management program more authority over the divisions that manage IT. Regarding the third weakness, the FBI is still developing an enterprise architecture framework, which includes the technical or data architecture. Regarding the fourth weakness, the FBI did not formally establish 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 do not use these systems.

B. Report on the FBI's IT Investment Management

In December 2002, the OIG issued a report entitled, "The FBI's Management of IT Investments." The objectives of the audit were 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) Background on Report Findings

The OIG concluded that the FBI had not effectively managed its IT investments because it had not fully implemented the management processes associated with successful IT investments. As discussed in the ITIM report, the foundation for sound IT investment management 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. The FBI did not have a fully-functional investment review board operation because the FBI did not provide adequate resources for operating the IT investment boards. Specifically, the OIG found insufficient evidence to demonstrate that: (1) executives and line managers supported and carried out IT investment board decisions and (2) board members understood the board's policies and procedures and were knowledgeable in using the IT investment approach through training, education, or experience. Additionally, 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 insufficient 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.

The OIG also found that the FBI was not effectively overseeing its IT projects. For example, while the FBI had issued project management guidance, the guidance was not being followed consistently. The OIG obtained differing answers from the FBI as to which document represented the official project management guidance.

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

The OIG concluded that these shortcomings primarily resulted from a lack of management attention in the past to IT investment management. However, the FBI has recognized that its past methods for managing IT projects have been deficient, and the FBI 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 highest probability of improving mission performance are selected. Further, the process is intended to provide the methods, structures, disciplines, and management framework that govern how IT projects are controlled and evaluated.

In addition to developing a conceptual model for a new IT investment management process, in early 2002 the FBI began a pilot test of the new process for the selection of IT proposals. The OIG 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 FBI IT managers, selected new IT proposals for inclusion in the FY 2004 budget request.

The OIG ITIM report concluded that while the FBI had 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 IT investment management 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 IT investment management process as well as advance its investment management capability.

The ITIM report also included a review of the FBI's management of Trilogy, the FBI's largest and most critical IT modernization project. The report noted 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. In addition, the user application (Virtual Case File) component of Trilogy, recognized by FBI officials as the most important aspect of the project in terms of improving agent performance, was at high risk of not being completed within the funding levels appropriated by Congress.

The ITIM report also concluded that the FBI's IT strategic planning and IT performance measurement was inadequate. The FBI's strategic plan did not include goals for IT investment management, and the FBI's strategic plan and performance plan were not consistent with the DOJ's annual performance plan.

(2) FBI's Progress in Taking Corrective Actions

The ITIM report contained 30 recommendations directed toward improving the FBI's management of its IT investments. Because the ITIM report was issued in December 2002, too little time had passed (as of April 2003) to enable us to assess the FBI's progress in implementing the recommendations identified in that report.

While FBI management has stated that improving technology is a high priority, the ITIM report demonstrates that the FBI must take significant action to implement a successful IT program that fully supports its mission. It also demonstrates that a successful IT program depends on effective management control processes. Without effective management controls in place, major projects designed to improve technology, such as Trilogy, may not deliver their intended benefits on schedule and on budget. The following section discusses in more detail OIG findings and recommendations related to the FBI's control environment over its IT systems.

C. Reports on the FBI's Control Environment over its Financial IT Systems

The OIG conducts annual financial statement audits of the FBI, with the most recent report covering FY 2001. To support these financial statement audits, the OIG performs detailed reviews of the FBI's control environment over its financial IT systems. Financial statement audits are intended to play a central role in (1) providing more reliable and useful financial information to decision-makers, and (2) improving the adequacy of internal controls and underlying financial management systems.

In FY 1996, the OIG began conducting annual reviews of the FBI's internal controls over IT systems using the GAO's Federal Information System Controls Audit Manual (FISCAM). The FISCAM describes the computer-related controls that auditors should consider when assessing the integrity, confidentiality, and availability of computerized data.

The general methodology applied to assess computer-related controls requires auditors and reviewers to evaluate:

- general controls at the entity or installation level;
- general controls as they are applied to the applications being examined, such as a payroll system or a loan accounting system; and
- application controls, which are the controls over input, processing, and output of data associated with individual applications.

According to the FISCAM, general controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect computer application programs, prevent system software from unauthorized access, and ensure continued computer operations in case of unexpected interruptions. The FISCAM provides six categories for assessing the effectiveness of general controls. These categories are:

- entity-wide security program planning and management controls,
- access controls,
- application software development and change controls,
- system software controls,
- segregation of duty controls, and
- service continuity controls.

The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. Without effective general controls, application controls may be rendered ineffective by circumvention or modification.

Application controls are directly related to individual computerized applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Both general and application controls must be effective to help ensure the reliability, appropriate confidentiality, and availability of critical automated information.

The nature and extent of audit procedures required to assess computer-related controls varies depending on the audit objectives and other factors. If general controls are not operating effectively, the application-level controls are generally not tested. However, if an audit objective is to identify control weaknesses with an application where more employees may have the potential to take advantage of a weakness, an assessment of the application controls may be appropriate.

During the course of these IT reviews, the OIG grouped the vulnerabilities and weaknesses found into the following categories defined by Government Auditing Standards and the American Institute of Certified Public Accountants.

- Reportable Conditions — matters coming to the auditors' attention that, in their judgment, should be communicated because they represent significant deficiencies in the design or operation of internal control, which could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

- Material Weaknesses — reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected by employees in the normal course of performing their assigned functions.[17]

As of April 2003, the OIG had issued reports for FYs 1996 through 2001 that indicated consistent weaknesses in the FBI's general and application controls. However, we found that the FBI had made progress in correcting deficiencies associated with the control environment over its financial IT systems. Of the 105 recommendations contained in the detailed reports supporting the financial statement audits from FYs 1996 to 2001, 83 have been implemented and closed, and 22 are still open. Of the 22 open recommendations, 13 correspond to material weaknesses in the FBI's IT management controls, indicating that without compensating controls there is an increased risk that material misstatements to the financial statements will not be detected.

We concluded that while the FBI has made some progress, it must take further action to enhance its controls over its IT environment. As of April 2003, material weaknesses and other control vulnerabilities remained in each of the FISCAM general control areas, except for system software. The following sections provide further details on each of these control categories, the weaknesses noted in these control categories, as well as the FBI's progress toward correcting the weaknesses.

[17] A third category of vulnerabilities are management letter comments, which the OIG considers to be a reportable matter that does not meet the criteria of a reportable condition or material weakness.

(1) Entity-Wide Security Program Planning and Management Controls

According to the FISCAM, an entity-wide process for security program planning and management is the foundation of an organization's security control structure and a reflection of senior management's commitment to addressing security risks. The security program should establish a framework and a continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

According to the FISCAM, without a well-designed security program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

(a) Background of Entity-Wide Security Program Planning and Management Control Findings

Reviews of the FBI's general computer controls for FYs 1996 through 2001 included repeated deficiencies pertaining to entity-wide security program planning and management controls. During the FY 1998 review, the OIG reported that the Payroll System did not have a security plan. That condition was reported again during the FY 1999 review. Additionally, the OIG reported in FY 2000 that a security plan had been written, but it did not address (1) specific rules of behavior, (2) training, and (3) the rules of the system. Further, the OIG reported in FY 2001 that the plan did not address an incident response capability, rules of behavior, and system interconnection. These reports for FYs 1998 through 2001 also stated that vulnerabilities existed because FBI management did not thoroughly review the FBI's "Payroll System Security Plan" that was written by a contractor.

As of April 2003, the deficiencies associated with the FBI's security program plans were considered to be a material weakness. The OIG made eight recommendations in the reviews for FYs 1996 through 2001 that were directed toward correcting the identified security program planning and management control vulnerabilities. Four of these recommendations were repeated in more than one year's report.

(b) FBI's Progress in Taking Corrective Actions

Since FY 1996, the FBI has made progress in correcting the vulnerabilities in its entity-wide security planning and management controls. Six of the eight recommendations were closed as of April 2003, while the other two remained open. Of the six recommendations that were implemented, four were last reported by the OIG as material weaknesses, while the other two were reportable conditions. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

Summary of Open and Closed Entity-Wide Program Planning and Management Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	2	4	6
Reportable Condition	0	2	2
Management Letter Comment	0	0	0
Total	**2**	**6**	**8**

Source: OIG analyses as of April 2003

By implementing six of the recommendations, the FBI improved its entity-wide security program planning and management controls by:

- taking steps to clearly assign, identify, and communicate information security responsibilities (reportable condition);

- allocating sufficient resources to ensure the proper implementation of its Automated Data Processing and Telecommunications (ADPT) policy (reportable condition);

- ensuring that risk assessments of the FBI Headquarters Data Center, its other supporting systems, and all major applications are conducted as required by OMB Circular A-130 and by the FBI's Manual of Investigative Operations and Guidelines (material weakness);

- ensuring that the systems and applications are accredited every three years (material weakness);

- renewing the interim accreditation for general control systems and major applications (material weakness); and

- improving security and application controls by determining which of its systems are classified as "major applications" (material weakness).

Despite the progress, additional corrective actions are necessary to mitigate the remaining weaknesses. Specifically, the FBI must still ensure that:

- the ADPT security plans are completed appropriately (material weakness), and

- the Payroll System Security Plan incorporates an incident response capability and rules of behavior (material weakness).

Regarding the completion of ADPT security plans, the OIG first recommended this action in the FY 1998 report, and has since repeated it in the FY 1999, 2000, and 2001 reports because the FBI's corrective actions to date have been inadequate. Without an approved security plan, the integrity of sensitive information maintained by the FBI is at risk of being compromised.

(2) Access Controls

(a) Background of Access Control Findings

Reviews of the FBI's general computer controls for FYs 1996 through 2001 included repeated deficiencies pertaining to access controls. The access control findings discussed in the FY 2001 report were considered to be a material weakness of the FBI. In the reviews for FYs 1996 through 2001, the OIG made 42 recommendations that were directed toward correcting the identified access control vulnerabilities.[18] Ten of these recommendations were repeated in subsequent reports.

[18] These recommendations are listed in Appendix 2.

The OIG's most recent report, covering FY 2001, stated that there were two findings associated with access controls: (1) auditing controls over the local area network (LAN), and (2) excessive access privileges granted to systems programmers.

1. Auditing Controls Over the Local Area Network

The OIG's review for FY 1998 reported that an automated tool was used to assess the technical controls over the FBI's Finance Division LANs. The assessment found weaknesses in three areas of security: account restrictions, system monitoring, and data confidentiality.

In FY 1999, another automated tool was used to perform the assessment of the technical controls over the FBI's Finance Division LANs. Although corrective action had been initiated on the prior weaknesses found, the OIG reported that these weaknesses still existed during FY 1999. The FY 2000 report stated that auditing remained disabled on the Finance Division's Windows NT and Novell NetWare environments.

According to the OIG FY 2001 review, although FBI management had indicated that corrective actions have been taken with respect to the recommended settings, the conditions continued to be identified during the annual financial statement audit process. The FY 2001 report further stated that the cause for this weakness was the Finance Division LAN administrators not fully implementing the FBI's audit policy on logical access controls on their Windows NT and NetWare LANs.

2. Excessive Access Privileges Granted to Systems Programmers

The FY 2001 report stated that access control profiles were not configured to restrict access to sensitive database utilities and payroll files. Specifically, the report noted instances where three systems programmers had access to database utilities and had full control of the payroll and Oracle datasets. The FY 2001 report further stated that the cause was due to the FBI granting systems programmer profiles to database programmers, thus providing them with unnecessary access to sensitive utilities. The OIG also reported in FY 2001 that the FBI's Systems Programming and Integration Unit (SPIU) was in the process of developing a database programmer profile that would provide access control to the needed datasets.

(b) FBI's Progress in Taking Corrective Actions

The FBI has made progress in correcting the vulnerabilities in this FISCAM category area since FY 1996. Of the 42 recommendations, 32 were closed as of April 2003, while the other 10 remained open. Of the 32 recommendations that were implemented, 15 were last reported by the OIG as material weaknesses, 13 were reportable conditions, and 4 were management letter comments. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

Summary of Open and Closed Access Control Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	5	15	20
Reportable Condition	5	13	18
Management Letter Comment	0	4	4
Total	**10**	**32**	**42**

Source: OIG analyses as of April 2003

By implementing 32 of the recommendations, the FBI improved its access control environment. These improvements included:

- establishing procedures that require new users to immediately change their initial password (reportable condition);
- reviewing user access to sensitive system files (reportable condition);
- establishing and distributing procedures requiring local security administrators to periodically, at least quarterly, review employees' access privileges in relation to their current job functions (reportable condition);
- deleting users that no longer require access to the network or do not have a demonstrated need for their access (material weakness); and
- requiring all system administrators to change their passwords at least every 30 days (material weakness).

Despite the progress made, additional corrective actions are necessary to mitigate the remaining weaknesses. Specifically, the FBI still must ensure that:

- an entity-wide data assessment of network systems is periodically performed to determine where potential vulnerabilities exist (reportable condition);

- user authentication controls are strengthened by an active token for user authentication (reportable condition);

- computer security training is provided to users at least annually (reportable condition);

- policies and procedures for the FBI's IT environments are complied with (material weakness); and

- the auditing function on the Finance Division's Netware environment is enabled (material weakness).

With respect to complying with policies and procedures and enabling the auditing function, the OIG first recommended these actions in the FY 1998 report, and has since repeated them in the FY 1999, 2000, and 2001 reports because the FBI's corrective actions to date have been inadequate. These actions are necessary to reduce the risk of processing erroneous or fraudulent transactions, and ensure that there can be a reconstruction of events if a system compromise or malfunction occurs.

(3) Application Software Development and Change Controls

According to the FISCAM, application software is designed to support a specific operation, such as payroll or loan accounting. Typically, several applications may operate under one set of operating system software. Establishing controls over the modifications of application software programs helps to ensure that only authorized modifications are implemented. Without proper application software development and change controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

(a) Background of Software Development and Change Control Findings

Reviews of the FBI's general computer controls for FYs 1996 through 2001 included repeated deficiencies pertaining to software development and change control findings. During the FY 2000 review, the OIG noted that although the FBI had developed a change control manual in July 1997 entitled "The Architecture Change Management (ACM) Plan," it did not address changes to the computer-based application and its environment. The OIG also reported in FY 2000 that project managers were not using the ACM because the procedures set forth by the ACM did not reflect the FBI's current information technology architecture, including recent changes to hardware, software, and firmware.

During the FY 2001 review, the OIG noted that the FBI had documented a change control process entitled, "Change Management Rules, Standards and Procedures," which replaced the ACM. However, this process had not been implemented on the Property Management Application (PMA) and the Payroll Application.

According to the FY 2001 report, the failure to implement the change management rules occurred because the FBI's Quality Configuration and Methods Unit (QCMU) did not enforce the Change Management Rules, Standards, and Procedures. The FY 2001 report further stated that the Unit plans to perform audits of divisions as a means of enforcing the procedures. The OIG reported that this weakness increases the chance that two or more independent changes to the system will conflict with one another and, consequently, the system will not function properly.

In the reviews for FYs 1996 through 2001, the OIG made eight recommendations that were directed toward correcting the identified system software development and change control findings.[19] Four of these recommendations were repeated in subsequent reports. As of the issuance of the FY 2001 report, the deficiencies associated with the FBI's software development and change controls were considered to be a material weakness.

[19] These recommendations are listed in Appendix 2.

(b) FBI's Progress in Taking Corrective Actions

Since FY 1996, the FBI has made progress in correcting the software development and change control deficiencies. Six of the eight recommendations pertaining to this FISCAM category were closed as of April 2003, while the other two remained open. Of the six recommendations that were implemented, three were last reported by the OIG as material weaknesses, while the other three were management letter comments. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

Summary of Open and Closed Application Software Development and Change Control Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	1	3	4
Reportable Condition	0	0	0
Management Letter Comment	1	3	4
Total	**2**	**6**	**8**

Source: OIG analyses as of April 2003

By implementing six of the recommendations, the FBI improved its software development and change controls by:

- developing and maintaining a configuration management process addressing changes to overall ADPT resources (management letter comment);
- expediting the implementation of the ACM methodology entity-wide (management letter comment);
- developing and implementing procedures to ensure all system problems are recorded (management letter comment);
- ensuring that the Information Resources Division enhances the ACM document to comprehensively address any type of change to the computer based application system and its environment (material weakness);

- ensuring that the methodology set forth with the ACM is consistently applied to the Financial Management System application (material weakness); and

- enforcing the emergency change procedures stated within ACM (material weakness).

Despite the progress made, additional corrective actions are necessary to mitigate the remaining weaknesses. Specifically, the FBI must ensure that:

- a policy is developed and implemented requiring periodic independent reviews of all major systems development activities at each major activity milestone (management letter comment); and

- an automated software management system is implemented in order to automate the transfer of all program code necessary to run a system (material weakness).

Regarding the implementation of an automated software management system, the OIG first recommended this action in the FY 1996/1997 report, and has since repeated it in the FY 1998, 1999, and 2000 reports because the FBI's corrective actions to date have been inadequate. Change requests maintained in multiple databases increase the risk that the FBI's Information Resources Division may not have the most current and accurate status of all requests. Additionally, poor change controls can create risks that inaccurate and unauthorized computer changes are implemented into the production environment. This weakness could cause inaccurate data or loss of data to the application.

(4) System Software Controls

According to the FISCAM, system software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, one set of system software is used to support and control a variety of applications that may run the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. Inadequate controls over system software could enable unauthorized individuals to circumvent security controls to read, modify, or delete critical or sensitive information and programs; authorized users of the system to gain unauthorized privileges to conduct unauthorized actions; or system software being used to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud and sabotage.

(a) Background on System Software Control Findings

The FY 2001 review did not report any material weaknesses associated with system software controls. The most recent vulnerabilities were noted in the FY 2000 and FY 1999 reports.

(b) FBI's Progress in Taking Corrective Actions

The FBI has corrected the deficiencies identified in the detailed IT reports for FYs 1996 through 2000. The reports for FYs 1996 through 2000 made seven recommendations that were directed toward correcting the identified system software control vulnerabilities.[20] All seven recommendations pertaining to this FISCAM control category were closed as of April 2003. Two of the recommendations were last reported by the OIG as material weaknesses, one was a reportable condition, and the remaining four were management letter comments. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

[20] These recommendations are listed in Appendix 2.

Summary of Open and Closed System Software Control Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	0	2	2
Reportable Condition	0	1	1
Management Letter Comment	0	4	4
Total	**0**	**7**	**7**

Source: OIG analyses as of April 2003

By implementing the seven recommendations, the FBI improved its system software control environment as of the issuance of the FY 2001 IT report. Examples of these improvements include:

- performing an analysis to determine which libraries and associated members are necessary for proper system performance (management letter comment);

- implementing procedures to ensure that all system documentation is current and complete and that changes to documentation are reflected timely and disseminated to applicable individuals (management letter comment);

- implementing a system software control policy to ensure that system software is current (management letter comment);

- configuring the parameters in order to log all the associated transactions for the respective System Management Facility records (material weakness); and

- establishing and implementing a formal change control process for changes to system software (reportable condition).

Regarding the implementation of a formal change control process, the OIG first recommended this action in the FY 1996/1997 report, and then repeated it in the FY 1998 and 1999 report before the FBI completed adequate corrective action. While no open recommendations pertaining to system software controls remain for the FYs 1996 through 2001 reports, testing conducted for the FY 2002 review indicates additional vulnerabilities exist with system software controls. The FBI's ability to make lasting

improvements to its IT control environment depends on a strong commitment from management, rather than short-term fixes that represent temporary progress.

(5) Segregation of Duty Controls

According to the FISCAM, work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed. The extent to which duties are segregated depends on the size of the organization and the risk associated with its facilities and activities. A large organization will have more flexibility in separating key duties than a small organization that must depend on only a few individuals to perform its operation. Smaller organizations may rely more extensively on supervisory review to control activities. Similarly, activities that involve extremely large dollar transactions, or are otherwise inherently risky, should be divided among several individuals and be subject to relatively extensive supervisory review.

(a) Background on Segregation of Duty Findings

Reviews of the FBI's general computer controls for FYs 1996 through 1998, and 2000 through 2001 included repeated deficiencies pertaining to segregation of duty controls. The OIG made five recommendations in the reviews for FYs 1996 through 1998 and 2000 through 2001 that were directed toward correcting the identified segregation of duty vulnerabilities.[21] Two of these recommendations were repeated in the FY 2001 report.

[21] These recommendations are listed in Appendix 2.

The FY 2001 report stated that there were three findings associated with segregation of duty controls pertaining to: (1) policies and procedures for segregation of duties, (2) physical and logical controls for segregation of duties, and (3) documented procedures for the FBI's Payroll Application.

1. Policies and Procedures for Segregation of Duties

The OIG stated in its FY 2000 report that the FBI has not established guidance, policies, procedures, or awareness of segregation of duties within the divisions and units. The result is unclear segregation of job responsibilities. This condition was also reported in the FY 2001 report.

According to the FY 2001 report, unclear, inconsistent policies and a lack of guidelines to separate the units created an environment where duties occasionally overlap. As a result, it was difficult to define responsibilities between the various units within the FBI.

2. Physical and Logical Controls for Segregation of Duties

The OIG reported in FY 2000 that application programmers had access to both the test and production regions in the PMA and Payroll Application. The FY 2001 report further stated that the application system administrator for the PMA was appropriately granted program update access to the test environment. However, the application system administrator also could move programs back into the production environment. Specifically, the Payroll Application programmers had the ability to move programs (source code) from the library to the test environment, make changes, and move the programs back into the quality assurance environment for testing.

According to the FY 2001 report, inadequate segregation of duties within the units and divisions caused application administrators and programmers to inappropriately be granted access to both the test and production regions.

3. Documented Procedures for the Payroll Application

The FY 2001 report stated that documented procedures do not exist for the Payroll Application's administrative functions. The report further stated that this weakness is caused by the failure to require a consistent administrative process for payroll-related functions by the Payroll Administration and Processing Unit and the Personnel Staffing Unit.

(b) FBI's Progress in Taking Corrective Actions

Since FY 1996, the FBI has made progress in correcting deficiencies associated with segregation of duty controls. Four of the five recommendations pertaining to this FISCAM category were closed as of April 2003, while one remained open. Of the four recommendations that were implemented, two were last reported by the OIG as a material weakness, while the other two were management letter comments. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

Summary of Open and Closed Segregation of Duty Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	1	2	3
Reportable Condition	0	0	0
Management Letter Comment	0	2	2
Total	**1**	**4**	**5**

Source: OIG analyses as of April 2003

By implementing four of the recommendations, the FBI improved its segregation of duty controls by:

- assessing the need for additional personnel at the staff level within the data security administrative function (management letter comment);

- performing an analysis of the potential benefits of applying business process re-engineering and/or activitiy-based costing processes to current operations in order to enhance effectiveness, efficiency, and productivity (management letter comment);

- ensuring application administrators and programmers do not have direct update access to both test and production application programs (material weakness); and

- establishing guidance policies, procedures, and awareness of segregation of duties within the divisions and units (material weakness).

Despite the progress made, an additional corrective action is necessary to mitigate the remaining weaknesses. Specifically, the FBI still must ensure that the payroll-related functions are documented and maintained to ensure the consistent application of the payroll-related administrative process (material weakness).

Because a segregation of duty deficiency was not corrected as of April 2003, the FBI is subject to the risk that erroneous transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed.

(6) Service Continuity Controls

According to the FISCAM, losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions, and (2) a plan to recover critical operations should interruption occur. The procedures and plan should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by the users of specific applications. To determine whether the recovery plan will work as intended, the plan should be tested periodically in disaster simulation exercises.

Although often referred to as disaster recovery plans, controls to ensure service continuity should address the entire range of potential disruptions. These disruptions may include relatively minor interruptions, such as temporary power failures, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. For some operations, such as those involving health care or safety, system interruptions could also result in injuries or loss of life.

To mitigate service interruptions, it is essential that the related controls be understood and supported by management and staff throughout the organization. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing. In addition, all staff with service continuity

responsibilities, such as staff responsible for backing up files, should be fully aware of the risks if these duties are not fulfilled.

(a) Background on Service Continuity Control Findings

Reviews of the FBI's general computer controls for FYs 1996 through 2000 reported repeated deficiencies pertaining to service continuity controls. The FY 2000 report identified two service continuity findings that were included in the material weakness. During the FY 2001 review, the OIG did not report any additional service continuity control deficiencies, although certain previously reported material weaknesses remained. These weaknesses are discussed below.

The FY 2000 report stated that the FBI's Contingency/Disaster Recovery Plans did not address specific applications, were incomplete, outdated, and did not include requirements such as testing scenarios and plans. While the FBI's Headquarters Data Center unit chief has attempted to update the plans, the business process owners had not adequately defined risks and critical recovery needs.

Because of this deficiency, during an extended outage or disaster, information system processing functions and vital business operations may be damaged and unable to function since critical information and computer resources are unavailable or inaccessible.

Additionally, the OIG reported in FY 1999, and again in FY 2000, that Data Center employees still had not been trained in disaster recovery, emergency, and contingency procedures. Without proper knowledge of procedures and priorities, the staff may be unable to perform critical duties to resume operations.

The reports for FYs 1996 through 2000 made 17 recommendations that were directed toward correcting the identified service continuity control vulnerabilities.[22] Nine of these recommendations were repeated in subsequent reports.

(b) FBI's Progress in Taking Corrective Actions

Since FY 1996, the FBI has made progress in correcting deficiencies associated with service continuity controls. Of the 17 recommendations pertaining to this FISCAM category, 15 were closed as of April 2003, while the other two remained open. Of the 15 recommendations that were

[22] These recommendations are listed in Appendix 2.

implemented, 13 were last reported by the OIG as material weaknesses, while the remaining 2 were management letter comments. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

Summary of Open and Closed Service Continuity Control Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	2	13	15
Reportable Condition	0	0	0
Management Letter Comment	0	2	2
Total	**2**	**15**	**17**

Source: OIG analyses as of April 2003

By implementing 15 of the recommendations, the FBI improved its service continuity control environment. Examples of these improvements include:

- developing procedures to ensure that daily back-up tapes are stored in a fireproof vault that is secure and not located within the immediate Data Center (management letter comment);

- developing a comprehensive contingency plan that provides an entity-wide approach for the recovery of mission-critical data processing operation in the event of a disaster (material weakness);

- assigning responsibility to a team of individuals to ensure full back-up and recovery is performed (material weakness);

- ensuring all data personnel are informed when the ADPT contingency plan has been completed and approved and that employees have access to the plan (material weakness); and

- briefing Data Center personnel on emergency procedures and responsibilities through training sessions and by distributing written policies and procedures (material weakness).

Despite the progress made, additional corrective actions are necessary to mitigate weaknesses previously reported in the FY 1999 and 2000 reports. The FBI still must:

- continue to update the ADPT contingency plan, addressing the weaknesses identified in the FY 1999 report (material weakness); and

- ensure that the Finance Division has developed and distributed to end-users, a contingency plan covering its information technology applications (material weakness).

The OIG first recommended in the FY 1999 report that the Finance Division develop and distribute a contingency plan covering its IT applications. This recommendation was repeated in the FY 2000 report, indicating that the FBI had not taken adequate corrective action. Without effective service continuity controls, information system processing functions and vital business operations may be damaged and unable to function during an extended outage or disaster because critical information and computer resources could be unavailable or inaccessible.

(7) Application Controls

According to the FISCAM, application controls are the structure, policies, and procedures that apply to separate, individual application systems such as accounts payable, inventory, payroll, grants, or loans. An application system is typically a collection or group of individual computer programs that relate to a common function. Some applications may be complex, comprehensive systems involving numerous computer programs and organizational units, such as those associated with benefit payment systems.

Application controls help ensure that transactions are valid, properly authorized, and completely and accurately processed by the computer. These controls are commonly categorized into three phases of a processing cycle:

- input — data is authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner;

- processing — data is properly processed by the computer and files are updated correctly; and

- output — files and reports generated by the application actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

According to the FISCAM, inadequate application controls can result in invalid, incomplete, or improperly classified data. Additionally, there is a heightened risk of inaccurate valuation or allocation of data and unauthorized transactions.

(a) Background on Application Control Findings

Reviews of the FBI's general computer controls for FYs 1998 through 2001 included deficiencies in application controls. The FY 2001 report reviewed the FBI's PMA and reported two findings: excessive access privileges were granted over the PMA, and input and processing control weaknesses existed on the PMA. The FY 2001 report further stated that these weaknesses occurred because the FBI lacked security oversight to monitor access of all users, and the PMA did not have the appropriate input and processing controls built in during its initial design. According to the FBI, adding the controls to the application was not a priority due to limited PMA resources.

Because of these application control weaknesses, the PMA allowed users to make unauthorized changes to property data, leading to errors in the property computer application. In the reviews for FYs 1998 through 2001, the OIG made 15 recommendations to correct the identified application control weaknesses.[23]

(b) FBI's Progress in Taking Corrective Actions

Since FY 1998, the FBI has made progress toward correcting the identified weaknesses. Of the 15 recommendations pertaining to this FISCAM category, 10 were closed as of April 2003 while the other 5 remained open. Of the ten recommendations that were implemented, nine were considered reportable conditions, while one was a material weakness. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

[23] These recommendations are listed in Appendix 2.

Summary of Open and Closed Application Control Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	2	1	3
Reportable Condition	3	9	12
Management Letter Comment	0	0	0
Total	**5**	**10**	**15**

Source: OIG analyses as of April 2003

By implementing ten of the recommendations, the FBI improved its application control environment. Examples of these improvements include:

- defining, documenting, and communicating the roles and responsibilities for changing code to the Payroll Application (reportable condition);

- reviewing the list of users having access to code, determining which users should not be making changes in accordance with their duties and responsibilities, and revoking access to users who should not be making changes (reportable condition);

- ensuring that user access to payroll code is authorized, documented, and periodically reviewed (reportable condition);

- adhering to the FBI's change management processes for applications and system software once formal processes have been developed (reportable condition); and

- reviewing the budgetary module of the Financial Management System (FMS), determining the cause of the application security weakness allowing the transfer of funds beyond an authorized balance, and taking the appropriate measures to ensure adequate controls are in place (material weakness).

Despite the progress made, additional corrective actions are necessary to mitigate the remaining weaknesses. Specifically, the FBI must:

- coordinate with the General Services Administration to synchronize file formats so that data sent via Simplified Intergovernmental Buying and Collection will correctly interface with the FMS application (reportable condition);

- ensure the Federal Procurement Data Statistics (FPDS) screen is modified to include all the fields required for accurate procurement reporting (reportable condition);

- remove the additional access capability from any PMA user not authorized or required to have the additional access to complete their job function (material weakness); and

- develop and implement a plan to ensure: (a) input control weaknesses identified in the PMA are appropriately addressed, and (b) the risk associated with the processing control weaknesses in the PMA is mitigated to ensure that all property is entered and purchase order and property numbers are accounted for (material weakness).

Inadequate input controls on the PMA can lead to errors in the property data, cause time consuming physical inventory counts and reconciliation, and require the Property Management Unit to correct errors in the application data.

(8) Other Financial-Related IT Recommendations

In the FY 1996/1997 detailed report issued in support of the Financial Statement Audit, the OIG provided the FBI with three recommendations not categorized by FISCAM general control areas.[24] These recommendations, reported as management letter comments, involved the Year 2000 issue, strategic planning, and network encryption. All of the recommendations were closed upon issuance of the final report. The following table summarizes how the closed recommendations correspond to the reported vulnerability.

[24] These recommendations are listed in Appendix 2.

Summary of Open and Closed Non-FISCAM Category Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	0	0	0
Reportable Condition	0	0	0
Management Letter Comment	0	3	3
Total	**0**	**3**	**3**

Source: OIG analyses as of April 2003

By implementing these recommendations, the FBI:

- provided to the FBI Director monthly briefings on the status of the Year 2000 project (management letter comment);
- developed a strategic plan that includes projects technology spending for a 3 to 5-year period (management letter comment); and
- evaluated encryption alternatives to reduce the risk of compromising sensitive information (management letter comment).

(9) Summary

The FBI made progress in correcting deficiencies associated with the control environment over its IT systems. Of the 105 recommendations contained in the detailed reports supporting the financial statement audits from FYs 1996 to 2001, 83 have been implemented and closed, and 22 are still open. The following table summarizes the status of the FBI's IT control environment recommendations by category.

Status of the FBI's Financial IT Control Environment Recommendations by FISCAM Category

FISCAM Category	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Entity-Wide Security Program Planning and Management Controls	2	6	8
Access Controls	10	32	42
Application Software Development and Change Controls	2	6	8
System Software Controls	0	7	7
Segregation of Duty Controls	1	4	5
Service Continuity Controls	2	15	17
Application Controls	5	10	15
Other Financial-Related IT Areas	0	3	3
Total	**22**	**83**	**105**

Source: OIG analyses as of April 2003

Of the 83 recommendations that have been implemented, 40 were originally reported by the OIG as material weaknesses, 25 were reportable conditions, and 18 were management letter comments. The following table summarizes how the open and closed recommendations correspond to the reported vulnerability.

Summary of Open and Closed Recommendations by Vulnerability Type

Type of Vulnerability	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Material Weakness	13	40	53
Reportable Condition	8	25	33
Management Letter Comment	1	18	19
Total	**22**	**83**	**105**

Source: OIG analyses as of April 2003

By implementing 83 of the 105 recommendations, the FBI improved its IT internal control environment. The FY 2001 report did not contain any system software control deficiencies. The FBI also made progress toward correcting deficiencies in entity-wide security program planning, access controls, application software development, segregation of duties, service continuity, and application controls.

Despite the progress made, as of April 2003 uncorrected deficiencies remained in the following general control areas:

- entity-wide security program planning and management;
- access controls; and
- application software development and change controls.

In addition to these findings, other vulnerabilities existed in the remaining FISCAM control areas (except for system software controls). The FBI is at increased risk of failures in its financial management and computer security functions. As a result, the FBI must take additional actions to correct these deficiencies. Also, 13 of the 22 open recommendations related to material weaknesses, which suggests that without compensating controls, there is an increased risk that material errors in the financial statements will not be detected.

We noted that 30 of the open and closed recommendations were repeated in subsequent reports. Further, many of the findings and recommendations noted in these internal control reports of the FBI's IT environment were also repeated in audits of the FBI's compliance with GISRA. The following table summarizes the status of recommendations that have been repeated in subsequent OIG reports.

Status of the FBI's Financial IT Control Environment Repeated Recommendations by Category

FISCAM Category	Number of Open Recommendations Repeated	Number of Closed Recommendations Repeated	Total Number of Repeated Recommendations
Entity-Wide Security Program Planning and Management Controls	1	3	4
Access Controls	3	7	10
Application Software Development and Change Controls	1	3	4
System Software Controls	0	1	1
Segregation of Duty Controls	0	2	2
Service Continuity Controls	1	8	9
Application Controls	0	0	0
Other Financial-Related IT Areas	0	0	0
Total	**6**	**24**	**30**

Source: OIG analyses as of April 2003

Because of the uncorrected and repeated deficiencies identified in these reviews, we believe that the FBI's overall progress in implementing financial-related IT internal control recommendations has been weak. Moreover, FBI management had not consistently responded to OIG inquiries about the status of corrective actions and the FBI lacked an effective management process for tracking, responding to, and implementing recommendations. However, during FY 2002, the OIG noted significant improvement in the FBI's responsiveness to responding to inquiries about corrective actions. During FY 2002, the Inspection Division began developing written policies and procedures designed to assist the FBI with its audit follow-up responsibilities. Further, the Inspection Division created a database to track audit recommendations, responses to the OIG and other inquiries, and corrective actions. The FBI's efforts to improve its audit follow-up responsibilities are discussed in more detail later in this report.

While the Inspection Division has improved the FBI's responsiveness to audit recommendations, the ability of the FBI to correct many of its IT deficiencies ultimately rests with the commitment and actions from senior FBI management.

D. Computer Security Reports in Response to GISRA

The FY 2001 Defense Authorization Act (Public Law 106-398) includes Title X, subtitle G, "Government Information Security Reform Act." GISRA became effective on November 29, 2000, and amended the Paperwork Reduction Act of 1995 by enacting a new subchapter on "Information Security." It required federal agencies to:

- perform an annual independent evaluation of their information security practices;
- ensure information security policies are founded on a continuous risk management cycle;
- implement controls that appropriately assess information security risks;
- promote continuing awareness of information security risks;
- continually monitor and evaluate information security policies;
- control effectiveness of information security practices; and
- provide a risk assessment and report on the security needs of the agencies' systems, and include the report in their budget request to the Office of Management and Budget.

Beginning in FY 2001, GISRA also required the OIG to independently evaluate the DOJ's information security program and practices. In addition to the FISCAM, the OIG used standards provided by the National Institute of Standards and Technology (NIST) as the basis for its audit approach.[25]

[25] The NIST is a non-regulatory entity of the U.S. Department of Commerce. According to the NIST, its mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

The NIST has issued guidance detailing the specific controls that should be documented by federal agencies in their system security plan.[26] The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.

The NIST has separated the security plan controls into three major control areas: (1) management controls, (2) operational controls, and (3) technical controls. Within each of the three control areas, there are a number of subordinate categories of controls. For example, technical controls include password management, logon management, account integrity management, and system auditing management.

Management controls address security topics that can be characterized as managerial. These controls represent techniques and concerns that normally are addressed by management in the organization's computer security program. In general, these controls focus on the management of the computer security program and the management of risk within the organization.

Operational controls address security controls that are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). These controls often require technical or specialized expertise and rely upon management activities as well as technical controls.

Technical controls focus on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization.

For FY 2001, the OIG selected the FBI's administrative and investigative mainframe systems as two of four classified systems it reviewed for the GISRA audit. For FY 2002, the OIG selected two FBI

[26] This guidance is contained in the NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."

investigative applications, the Automated Case Support (ACS) system[27] and the DRUGX Interactive Trusted Guard,[28] as two of three classified systems it reviewed. The criteria used for findings and recommendations were based upon the guidelines established by the NIST.

(1) FY 2001 GISRA Report

In May 2002, the OIG issued its FBI GISRA audit report for FY 2001. The objective of the audit was to determine DOJ compliance with GISRA requirements. The OIG assessed whether adequate computer security controls existed to protect DOJ systems from unauthorized use, loss, or modification.

The OIG found that since May 2002, the FBI made progress in correcting some of the management, operational, and technical control deficiencies that were identified in the report. Of the 23 recommendations contained in the GISRA report, 6 have been implemented and closed, and 17 are still open.

Despite the progress made, the FBI must take further action to enhance these controls. As of April 2003, vulnerabilities remained in the security controls of the FBI's administrative and mainframe IT systems. The following sections provide details on: (1) the background of the FY 2001 GISRA report findings related to management, operational, and technical controls; and (2) the FBI's progress in taking corrective actions.

[27] The FBI uses the ACS system, which resides on the FBI's investigative mainframe, to store information related to FBI investigations and cases, including criminal and intelligence cases. The system allows FBI personnel to open and assign cases, set and assign leads, store text of documents, index, search, and retrieve these documents.

[28] The FBI uses the Drug Enforcement Administration (DEA) DRUGX application to share information on current drug investigations. This application was a DOJ joint agency effort involving the FBI and the DEA. The DRUGX Investigative trusted guard (DRUGX trusted guard) permits FBI personnel interactive one-way access to the DRUGX application via the FBI's network. Access to the DRUGX application provides FBI investigative personnel with query access to basic information concerning current drug investigations being conducted by the FBI and the DEA. The purpose of a trusted guard system is to provide a secure interconnection between two computer systems or networks, each of which operates at a different classification level.

(a) Background on Management Control Findings

The FY 2001 GISRA report identified management control vulnerabilities with enforcement of security policies, procedures, standards, and guidelines governing the FBI's administrative and investigative mainframes. The report stated that although the FBI has established security policies, procedures, standards, and guidelines, management failed to ensure that they were performed and enforced. The report made six recommendations that were directed toward correcting the identified management control vulnerabilities.[29]

(b) FBI's Progress in Taking Corrective Actions

The FBI has made progress in correcting management control weaknesses since the report was issued in May 2002. Two of the six recommendations pertaining to management controls were closed, while the other four remain open as of April 2003. The recommendations that were closed related to (1) defining and documenting all criticality levels used to classify applications, and (2) documenting a corrective action plan to address the vulnerabilities identified in the risk analyses for the investigative and administrative mainframe systems.[30]

Despite the progress made, additional actions are necessary to mitigate the remaining management control vulnerabilities. Specifically, the FBI still must demonstrate that it is:

- distributing, obtaining, and maintaining signed statements of end-users' acceptance of the Automated Information System Rules of Behavior for the investigative and administrative mainframe systems;

- ensuring that the Management of Investigative Operations and Guidelines (MIOG) and other FBI security policies reflect the evolving systems environment and are enforced;

- obtaining a full accreditation for the investigative and administrative mainframe systems from the FBI's approving authority — a conditional accreditation should be unacceptable; and

[29] These recommendations are listed in Appendix 2.

[30] According to NIST Special Publication 800-18, information stored within, processed by, or transmitted by a system provides for the value of the system and is one of the major factors in risk management, making the criticality of system applications' definitions essential.

- conducting annual refresher computer training for all employees.

The OIG in its FYs 1998 and 2000 reports on the FBI's control environment over its financial-related IT systems reported findings on security policies, procedures, standards, and guidelines. Accordingly, the OIG made recommendations in its FY 1998 (recommendation 15) and FY 2000 (recommendation 1) reports that were similar to the recommendations made in the FY 2001 GISRA report. These recommendations remained open as of April 2003. Additionally, four of the six GISRA recommendations pertaining to management control issues remained open as of April 2003. As a result, we believe that the FBI has not taken adequate corrective actions to reduce the potential for sensitive information from being compromised, lost, misused, or altered without authorization.

(c) Background on Operational Control Findings

The FY 2001 GISRA report identified operational control vulnerabilities with physical controls and system and network backup and restoration controls. The report stated that vulnerabilities existed because FBI management: (1) did not enforce physical controls at FBI Headquarters, and (2) had not taken the necessary steps to identify priorities of the system for restoration or to ensure Data Center personnel were aware of and tested appropriate contingency planning and backup procedures. The report made four recommendations directed toward correcting the identified operational control vulnerabilities.[31]

(d) FBI's Progress in Taking Corrective Actions

The FBI has made progress in correcting operational control weaknesses since the report was issued in May 2002. Two of the four recommendations pertaining to operational controls were closed as of April 2003, while the other two remain open. The recommendations that were closed related to (1) restricting physical access to all wiring closets, and (2) establishing optimal operating system capacities and implementing procedures to alleviate the near capacity usage.

[31] (U) These recommendations are listed in Appendix 2.

Despite the progress made, additional actions are necessary to mitigate the remaining operational control vulnerabilities. Specifically, the FBI must:

- document procedures for identifying and restoring mission-critical systems; and

- complete the production test exercise involving the transfer of production operations and applications to the backup site and training Data Center staff for this contingency control.

The OIG in its FYs 1999 and 2000 reports on the FBI's control environment over its financial-related IT systems reported findings in system and network backup and in restoration controls. Accordingly, the OIG made seven recommendations in its FY 1999 report (recommendations 23 and 25-31) and three recommendations in its FY 2000 report (recommendations 13-15) that were similar to the recommendations made in the FY 2001 GISRA report. Because two of the four GISRA recommendations pertaining to operational controls remained open as of April 2003, we conclude that the FBI has not demonstrated that adequate corrective action was taken to reduce the potential for failed restoration procedures or unexpected loss or disruption of services.

(e) Background on Technical Control Findings

The FY 2001 GISRA report identified technical control vulnerabilities with password management, logon management, account integrity management, system auditing management, and system patches. The report stated that vulnerabilities existed because of the following.

- FBI management did not ensure that operating systems' password settings were appropriate and DOJ security policies were being followed.

- FBI security management did not implement logon management controls or provide oversight to ensure DOJ and FBI security policies were followed.

- Budgetary constraints have prevented the FBI from being able to implement automated software change controls. Additionally, the FBI had not established procedures consistent with its security policy or updated them to reflect its current information technology environment.

- Security parameters were not appropriately set to enable auditing.

- FBI management had not taken the necessary measures to ensure proper safeguards were in place to prevent unauthorized access, loss, or misuse to the system.

The report made 13 recommendations that were directed toward correcting the identified technical control vulnerabilities.

(f) FBI's Progress in Taking Corrective Actions

The FBI has made limited progress in correcting technical control weaknesses since the report was issued in May 2002. Two of the 13 recommendations pertaining to technical controls were closed as of April 2003, while the other 11 remained open. The closed recommendations related to: (1) fully implementing and using the System Access Request function to document user logon and verify that user access is commensurate with assigned responsibilities, and (2) ensuring that the communication carrier signals are not connected to unencrypted network devices.

Additional actions are necessary to mitigate the remaining technical control vulnerabilities. Specifically, the FBI still must demonstrate to the OIG that it is:

- implementing and enforcing DOJ password policies by re-setting and monitoring operating system settings accordingly,

- requiring that system administrators periodically review and delete all system accounts that have been unused for more than 90 days,

- enabling account lockout on all systems so that lockout occurs after three unsuccessful logon attempts,

- enforcing the use of the FBI's Service Center as a centralized approval point to track all change requests from initiation through final disposition,

- implementing the format and content standards for information technology development and maintenance support test plans,

- updating the Architecture Change Management Policy to reflect the FBI's current information application and system software environment,

- documenting procedures to establish the supervisory review process of software change when deviations from normal procedures occur,

- enabling audits to capture the necessary system information to comply with DOJ policy, and

- applying manufacturer patches in a timely manner to prevent system compromise to all network operating systems.

Additionally, the FBI disagreed with one OIG recommendation in the report, and this recommendation was in an "unresolved" status as of April 2003.[32] The recommendation relates to enforcing DOJ security policies and ensuring sufficient controls for FBI systems to operate.

Findings with password management, logon management, account integrity management, system auditing management, and system patches were reported by the OIG in its FYs 1996 to 2000 reports on the FBI's control environment over its IT systems. Accordingly, the OIG made one recommendation in its FY 1996/97 report (recommendation 18); three recommendations in its FY 1998 report (recommendations 6, 8, and 21); seven recommendations in its FY 1999 (recommendations 6, 8, 10, 17-19, and 35) and FY 2000 reports (recommendations 2-4, 7, 8, 16, and 17) that were similar to the recommendations made in the FY 2001 GISRA report. Because 11 of the 13 GISRA recommendations remained open as of April 2003, in our judgment the FBI has not demonstrated that adequate corrective action was taken to reduce the potential for: (1) unauthorized disclosure, unauthorized data modification, and the misuse and abuse of the FBI's automated resources; and (2) critical system data pertaining to individual user accountability, reconstruction of system events, and problem identification to be permanently lost.

[32] Appendix 2 provides more detail on the FBI's response to the unresolved recommendation. Unresolved recommendations occur when the component disagrees with all or part of the finding.

(g) Summary

The FBI made limited progress in correcting deficiencies reported in the OIG FY 2001 GISRA audit. Of the 23 recommendations contained in the report, 6 have been implemented and closed, and 17 remain open. The following table summarizes the status of the FBI's FY 2001 GISRA report recommendations by NIST category.

Status of the FBI's FY 2001 GISRA Report Recommendations by NIST Category

NIST Category	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Management Controls	4	2	6
Operational Controls	2	2	4
Technical Controls	11	2	13
Total	**17**	**6**	**23**

Source: OIG analyses as of April 2003

By implementing six of the recommendations, the FBI made improvements to its computer security over its Headquarters and Data Centers investigative and mainframe systems. These improvements included: (a) defining and documenting all criticality levels used to classify applications, (b) establishing optimal operating system capacities and implementing procedures to alleviate the near capacity usage, (c) fully implementing and using the System Access Request function to document user logon and verify that user access is commensurate with assigned responsibilities, and (d) ensuring that the communication carrier signals are not connected to unencrypted network devices.

Despite the progress made, as of April 2003 significant vulnerabilities remained with management, operational, and technical controls. The OIG assessed these vulnerabilities as high-to-moderate risk for the protection of the FBI's administrative and investigative mainframe systems from unauthorized use, loss, or modification. Specifically, vulnerabilities remained in the following areas:

- security policies, procedures, standards, and guidelines;
- system and network backup and restoration controls;
- password management;

- logon management;
- account integrity management;
- system auditing management; and
- system patches.

These vulnerabilities resulted from DOJ and FBI security management not enforcing existing security policies, not developing a complete set of policies to effectively secure the administrative and investigative mainframes, and not holding FBI personnel responsible for timely correction of recurring findings. Further, the report stated that the lack of timely and effective oversight from DOJ and FBI management caused inconsistencies in the implementation of security guidelines and resulted in a weakened security infrastructure.

The FY 2001 GISRA report stated that FBI management has been slow in correcting deficiencies and implementing suggested corrective actions in its systems' environment. Since FY 1996, the OIG has reviewed the FBI's Headquarters Data Center computer systems' general controls as part of the FBI annual financial statement audit. Many of the vulnerabilities previously reported to the FBI in reviews of general controls as part of the FBI financial statement related reports from FYs 1996 through 2000 continued to exist during the FY 2001 GISRA audit. As a result, the FY 2001 GISRA report concluded that there was a lack of commitment and oversight from DOJ and FBI management regarding corrective action on prior audit findings. This lack of oversight caused inconsistencies in the implementation of security guidelines and resulted in a weakened data security infrastructure. As discussed in the following sections, some of these vulnerabilities were reported again in the FY 2002 GISRA audits.

(2) FY 2002 GISRA Report on the ACS System

In November 2002, the OIG issued the FY 2002 GISRA report on the ACS system.[33] The objective of the audit was to determine the DOJ's compliance with GISRA requirements. The ACS system was selected as one of the subset of systems to be tested to determine the effectiveness of the DOJ's overall security program for FY 2002. In determining if the DOJ was

[33] Because the FY 2002 GISRA report on the ACS system was issued in November 2002, we did not examine the FBI's progress toward implementing the recommendations contained in the report.

compliant with GISRA requirements, the OIG assessed whether adequate computer security controls existed to protect the ACS system from unauthorized use, loss, or modification.

(a) Background on Report Findings

The FY 2002 GISRA report on the ACS system found the following improvements or satisfactory operations in the ACS system's information security.[34]

- The overall policy for change control dictates the creation of a Change Control Board, which is an important control in ensuring that changes made to the system are approved.

- Security requirements are included in each requirement document to ensure that security is reviewed and integrated into the initial stages of system development.

- The investigative mainframe applications, including the ACS system, have been certified and accredited in accordance with the National Information Assurance Certification and Accreditation Process.

- Record counts are used within the Investigative Case Management system to track cases and investigative leads.[35]

- The FBI has developed a system security plan for the investigative mainframe applications that has been approved by management and includes the elements identified in the NIST Publication 800-18.

- Effective procedures are in place requiring re-investigations (which strengthen personnel security) to be performed in a timely manner.

- Controls are in place over the security of personally identifiable information.

[34] These improvements or satisfactory operations relate to specific security criteria set forth by GISRA. As a result, these improvements are not indicative of the overall functionality of the ACS system, which is discussed later in this report.

[35] Investigative Case Management is a case management system within the ACS system.

- A help desk is in place for the ACS system users.

- The IT contingency plan for the FBI Headquarters Data Center identifies critical data files and operations. The plan also identifies the frequency of data backups and includes procedures to allow the FBI to continue essential functions if information technology support is interrupted.

- The FBI's investigative mainframe applications use the mainframe security software to control password derivations, which complies with DOJ Order 2640.2D.

- The FBI has an up-to-date network diagram of the FBI LAN rings on which the investigative mainframe resides, which houses the ACS system.

- An automated system is used to request and approve access to the ACS system. This system has automated capabilities for requesting access and ensuring that approvals are received before access is granted. In addition, this system automatically adds requests into a queue for the access administrator's workload, thereby minimizing the time required to turn these requests around and eliminating the possibility of lost requests.

However, security controls needed improvement to protect the ACS system from unauthorized use, loss, or modification. Specifically, the report identified vulnerabilities in 6 of the 17 control areas, including life cycle, personnel security, security awareness, training and education, incident response capability, and logical access. The report stated that similar technical control vulnerabilities were noted in the FY 2001 GISRA audit.

These vulnerabilities occurred because the managers of the ACS system management did not consistently apply DOJ and FBI policies and procedures.

(b) FBI's Progress in Taking Corrective Actions

The FY 2002 GISRA report on the ACS system made eight recommendations directed toward correcting the noted deficiencies. As of April 2003, six of the recommendations were open, and two were closed. Although we did not formally assess the FBI's progress in taking corrective actions given the relatively recent issuance of the report, the report stated that it is critical for the FBI to take immediate corrective actions on the

recommendations pertaining to technical control vulnerabilities because of similar vulnerabilities noted in prior audits. As a result, the FY 2002 GISRA report on the ACS system, like the FY 2001 GISRA report, noted repeated deficiencies in general control areas. Specifically, vulnerabilities were noted within password management, logon management, account integrity management, system auditing management, and system patches. The report further stated that, if not corrected, these security vulnerabilities threaten the ACS system and its data with the potential for unauthorized use, loss, or modification.

(3) FY 2002 GISRA Report on the DRUGX Trusted Guard

In November 2002, the OIG also issued the FY 2002 GISRA report on the DRUGX Interactive Trusted Guard (DRUGX Trusted Guard).[36] The objective of the audit was to determine the DOJ's compliance with the requirements of GISRA. The DRUGX Trusted Guard was selected as one of the subset of systems to be tested to determine the effectiveness of the DOJ's overall security program for FY 2002. In determining if the DOJ is compliant with GISRA requirements, the OIG's contractor assessed whether adequate computer security controls existed to protect the DRUGX Trusted Guard from unauthorized use, loss, or modification.

(a) Background on Report Findings

The FY 2002 GISRA report on the DRUGX Trusted Guard found improvements or satisfactory operations in the DRUGX Trusted Guard's information security. Specifically, improvements or satisfactory operations included:

- The FBI has developed a comprehensive system security plan for the DRUGX Trusted Guard system that follows the NIST Special Publication 800-18 and contains required data concerning existing controls of the system and the environment.

- Effective procedures are in place requiring re-investigations to be performed in a timely manner.

- Controls are in place over the security of personal information.

[36] Because the FY 2002 GISRA report on the DRUGX Trusted Guard was issued in November 2002, close to the issuance of this report, we did not examine the FBI's progress toward implementing the recommendations contained in the report.

- The connection between the FBI's network and the DRUGX application is completed through a trusted guard, providing a secure interconnection between two computer systems or networks.

- No printers are attached to the DRUGX Trusted Guard, which eliminates the possibility of printed output falling into unauthorized hands.

- All damaged media from the DRUGX Trusted Guard is destroyed and an associated electronic communication is created to account for that media.

- The FBI has a current network diagram of the FBI LAN rings, to which the DRUGX Trusted Guard is connected.

However, security controls needed improvement to protect the DRUGX Trusted Guard from unauthorized use, loss, or modification. Specifically, the OIG found security vulnerabilities in 8 of the 17 control areas, including security controls, personnel security, contingency planning, security awareness, training and education, incident response capability, identification and authentication, logical access, and audit trails.

These vulnerabilities occurred because FBI management did not enforce the documented policies and procedures for the DRUGX Trusted Guard. Additionally, FBI management did not always ensure that IT policies and procedures were implemented.

(b) FBI's Progress in Taking Corrective Actions

The FY 2002 GISRA report on the DRUGX Trusted Guard made 12 recommendations directed toward correcting the noted deficiencies. As of April 2003, eight of the recommendations were open and four were closed. Although we did not formally assess the FBI's progress in taking corrective actions, the security vulnerabilities documented in this report, if not corrected, threaten the DRUGX Trusted Guard and its data with the potential for unauthorized use, loss, or modification.

(4) Summary of Reports on the FBI's Compliance with GISRA

As stated in the sections above, the three GISRA reports issued by the OIG related to FBI systems have found vulnerabilities associated with management, operational, and technical controls. Additionally, the FY 2001 GISRA report stated that the FBI has been slow to take corrective actions

since many of these vulnerabilities were previously reported in annual audits of general controls. Further, the FY 2002 GISRA report on the FBI's ACS system stated that similar vulnerabilities continued.

The FY 2002 GISRA reports on the FBI's ACS and DRUGX Trusted Guard systems stated that within the FBI, only the Inspection Division tracked remedial actions to reported computer security vulnerabilities. With the exception of audits performed by the OIG, the FBI's Inspection Division did not track the ACS or DRUGX systems' vulnerabilities identified in other audits and the corresponding corrective actions. Further, these reports stated that the Inspection Division did not receive any other audit results or reviews outside of the OIG audits and therefore has limited knowledge of other reported vulnerabilities.

According to the FY 2002 GISRA reports, without an effective tracking system, the FBI is unable to identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems. As a result, the FY 2002 GISRA reports recommended that the FBI determine the responsible organization for tracking and maintaining all vulnerabilities identified during audits and reviews. In addition, the reports recommended that the FBI develop a mechanism for tracking the vulnerabilities and the status of the associated corrective actions resulting from all IT audits and reviews.

During FY 2002, the Inspection Division began developing written policies and procedures designed to assist the FBI with its audit follow-up responsibilities. To help in this effort the Inspection Division created a database to track: (1) recommendations; (2) responses to OIG, GAO, and other inquiries; and (3) the status of corrective actions. However, for system audits, the FBI has reported that its Information Assurance Section has taken steps to centrally manage the status of vulnerabilities and corrective actions. We believe that the FBI should consider using the Inspection Division to oversee all recommendations, including those generated from system audits. The FBI's recent actions to improve its audit follow-up responsibilities are discussed in more detail later in this report.

E. Reports on OIG Special Investigations of the FBI

Since 1998, the OIG has issued the following two special investigation reports containing FBI IT or document management related recommendations:

- the 1999 report on the DOJ's Campaign Finance Task Force investigation (Campaign Finance); and

- the 2002 report on the FBI's investigation into the related production of documents in the Oklahoma City Bombing case (McVeigh).

These reports considered the policies and procedures related to the management of information and documents within the FBI, the dissemination of information to organizations outside the FBI, and the effectiveness of information technology utilized by the FBI. The reports cited deficiencies in the FBI's IT and document management and contained 20 IT-related recommendations designed to correct IT deficiencies.[37] The following table summarizes the status of the recommendations issued to the FBI.

Status of the FBI's Special Investigation Recommendations by Report

Report Name	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
Campaign Finance Report	5	0	5
McVeigh Report	11	4	15
Total	**16**	**4**	**20**

Source: OIG analyses as of April 2003

We found the FBI's current and planned corrective actions, including the implementation of Trilogy, have the potential to address 16 of the 20 recommendations that we examined from the Campaign Finance and McVeigh reports. However, the ultimate success of Trilogy will not be determined until at least June 2004 when the final phases of the project are scheduled for completion.

The following section provides background information on Trilogy, since its successful completion is critical to not only addressing OIG recommendations but also the future of the FBI's IT program.

[37] We included recommendations related to document management because FBI documents are generally produced electronically or managed in automated databases and systems.

(1) Background on Trilogy

Trilogy is an IT modernization project designed to upgrade the FBI's: (1) hardware and software or Information Presentation Component (IPC), (2) communication networks or Transportation Network Component (TNC), and (3) User Application Component (UAC). The IPC and TNC upgrades will provide the physical infrastructure needed to run the applications from the UAC.

- 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 TNC is the complete communications infrastructure and support to create, run, and maintain the FBI's networks. The TNC includes high capacity wide-area and local-area networks, authorization security, and encryption of data transmissions and storage.

- The UAC is intended to replace five of the FBI's primary investigative applications in order to reduce agents' reliance on paperwork and improve efficiency. Through the creation of the Virtual Case File (VCF), a web-based "point-and-click" case management system, agents are expected to have multi-media capability that will allow them to scan documents, photos, and other electronic media into the case file.

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 3-year period from the date contractors were hired. The $100.7 million was a combination of new program funding and a reprogramming of base resources. When the FBI requested contractor support for Trilogy, it combined the IPC and TNC portions for continuity because both portions encompass physical IT infrastructure enhancements. By direction of the DOJ Procurement Executive, the TNC/IPC and the UAC contracts were awarded to two different contractors. The contractor for the IPC and 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 September 11, 2001, terrorist attacks, 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.

In January 2002, Congress supplemented the FY 2002 Trilogy budget with $78 million to expedite the deployment of all three components.[38] 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 "Fast Track" portion of the IPC and TNC phases.[39]

In April 2003, the FBI Director reported to the Senate Appropriations Committee that over 21,000 new desktop computers and nearly 5,000 printers and scanners have been deployed throughout the FBI (IPC phase). Additionally, the FBI reported that it completed the Trilogy Wide Area Network (TNC phase) on March 28, 2003. The new network, which has been deployed to 622 sites, provides increased bandwidth and three layers of security. According to the FBI, the network is highly expandable, so additional capacity or even additional sites can be added as needed. This network replaces the FBI's antiquated local area and wide area networks, enabling FBI personnel to transmit data at much greater speeds. Further, the FBI expects to use the network to transport the Investigative Data Warehouse, which will link 31 FBI databases for single-portal searches and data mining. Also, the network lays the foundation for improved information sharing with partner agencies and other new applications, such as the VCF.

The VCF will 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 FBI expects to deploy the VCF in three releases. The initial VCF release will consolidate data from the current ACS and IntelPlus systems and 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 from their desktop computers a variety of information that is specific to their individual needs. This VCF release is also intended to enhance the FBI's capability to establish and track case leads, index case information, and with digital signatures move document drafts more quickly through the approval process.

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

[39] The FBI referred to the accelerated deployment of Trilogy as the "Fast Track."

The second and third releases are intended to install three other investigative applications into the VCF: the Integrated Intelligence Information Application (IIIA), Telephone Application, and Criminal Law Enforcement Application. These releases have a targeted completion date of June 2004 and are intended to provide agents with audio/video streaming capability and content management capability. According to the FBI, content management should help agents access information from the FBI's data warehouse, based on a single query from all of the FBI's systems.

The OIG ITIM report, issued in December 2002, stated that the VCF, which FBI officials have stated is the most important aspect of the Trilogy project in terms of improving agent performance, was at high risk of not being completed within the funding levels appropriated by Congress. FBI officials confirmed the OIG's assessment in January 2003 when they told us that an additional $138 million was needed to complete Trilogy, bringing the total project cost to $596 million.[40] Despite the cost overruns, FBI officials stated that they still expect to deliver the first release of VCF in December 2003, and that funding for the second and third releases of the VCF has been secured.

The following sections provide further details on the IT and document management related deficiencies noted in Campaign Finance and McVeigh reports, as well as an assessment of the how the VCF will address these deficiencies.

(2) Campaign Finance Report

In July 1999, the OIG issued a report entitled "Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation" (Campaign Finance). In response to a request by the Attorney General, the OIG reviewed the FBI's practices for disseminating intelligence information associated with the Campaign Finance Task Force (Task Force) investigation.

The report noted deficiencies in the use and maintenance of the FBI's computer database systems, including: the Task Force's lack of familiarity with the FBI's databases, the FBI's practices and policies that limited the usefulness of the databases, the training of FBI personnel on the ACS system, and the entry of foreign names into the FBI's databases. These findings highlighted the need for FBI and Task Force personnel to be familiar with information search techniques within the FBI's databases, how

[40] Of this amount, $57 million was needed for the VCF.

information should be entered into the databases in order to take advantage of search capabilities, and potential errors in data entry to ensure that all possible searches within the databases are conducted. Of the Campaign Finance report's 18 recommendations, 5 pertained to the IT-related deficiencies.[41] These five recommendations included:

A. revising the FBI's Manual of Administrative Operations and Procedures (MAOP) to require more comprehensive indexing of names appearing in any FBI document and requiring that all documents be uploaded into the Electronic Case File database (Recommendation IV.A),

B. training agents who are principally responsible for the information that is entered into the ACS system (Recommendation IV.B),

C. making agents responsible for determining what information is entered into the IIIA[42] system (Recommendation IV.C),

D. ensuring that any task force using the FBI's databases should obtain at least a fundamental appreciation for their operation (Recommendation IV.D), and

E. ensuring that the FBI's database operators are conversant with the format of Chinese and other foreign names (Recommendation IV.E).

(a) Recommendation IV.A

Regarding the uploading of documents, the FBI issued ECs in July 2000 and June 2002 that required all e-mails and ECs to be uploaded into the ACS system, unless otherwise prohibited by their sensitive nature. Additionally, FBI officials stated that with the VCF, most documents will have to be uploaded since the VCF will contain all official records and case files, except for Top Secret/Sensitive Compartmented Information (SCI) information.[43] As a result, FBI officials stated that agents will no longer be

[41] These five recommendations, along with a summary of the FBI's responses to the recommendations, are listed in Appendix 2.

[42] According to the FBI, the IIIA is a real-time collection system that houses over 20 million records to support the counterintelligence and counterterrorism programs.

[43] The FBI is currently working on a TS/SCI network, but at this time the VCF is only approved up to the Secret level.

able circumvent the case management system by not uploading documents.

Rather than revising the MAOP, the FBI is implementing alternative corrective action by ensuring that the VCF will facilitate the comprehensive indexing of names appearing in FBI documents. FBI officials stated to us that the VCF will provide indexing on various web-based documents by sorting data fields into searchable databases. The index of data fields, except for narrative fields, will be automatically created once the document is approved and entered into the VCF. Agents and analysts can then search the index of data fields by using search screens or viewing the serialized document. Because the first release of the VCF is not scheduled for completion until December 2003, this recommendation remains open.

(b) Recommendation IV.B

FBI officials said that they increased the ACS system training for veteran agents. According to the FBI, since 1999 over 400 veteran and 2,300 new agents received training on the ACS system. However, it is not clear whether the ACS training provided to veteran agents has been adequate since this represents less than 25 percent of all FBI agents. Additionally, we were unable to assess the FBI's web-based training for the VCF since it will not occur until October and November 2003. As a result, this recommendation remains open.

(c) Recommendation IV.C

According to the FBI, during 2000 several initiatives were undertaken to make agents responsible for determining what information is entered into the IIIA system and improving the accuracy of information in the IIIA system. These initiatives included:

- expanding the amount of data electronically transferred from the ACS to the IIIA systems;
- establishing a more user-friendly IIIA search interface;
- using a macro to collect accomplishment information electronically;
- automating the indexing, serialization, and entry of certain data;
- improving the oversight provided to the uploading of particular surveillance logs; and

- automating the selection of approved cryptonyms (codenames/codewords).

In addition to these improvements, the FBI stated that the IIIA system will ultimately be replaced by the second and third releases of the VCF. Further changes are planned for the IIIA system since the VCF development is not based on a system-by-system replacement per se, but rather a re-engineering of business practices and policies. As a result, certain sub-systems and data sets will be retired, while others will be transferred to the VCF. The FBI is continuing to schedule and prioritize the functional components that must be integrated into the VCF for each delivery through June 2004. Because the second and third releases of the VCF are not scheduled for completion until June 2004, this recommendation remains open.

(d) Recommendation IV.D

According to the FBI, appropriate training will be conducted whenever a relevant task force is created. In May 2003, the FBI said that the VCF training plan includes all Bureau task force members who will have access to the VCF application. To prepare for the VCF training scheduled in October and November 2003, the FBI is assessing its FBI employees' basic computer literacy skills. This assessment identifies employees in need of additional computer skills so that the necessary supplemental training can be taken prior to the scheduled VCF training. Because training on the VCF has not yet taken place, this recommendation remains open.

(e) Recommendation IV.E

The FBI said that it made enhancements to the IIIA system in July 2000 so that variations of a name are identified during a search. Additionally, FBI officials told us that on May 3, 2002, the Language Training and Assessment Unit (LTAU) announced a project to adopt and implement standards for the uniform "Romanization" of foreign personal and place names. Also in May 2002, the LTAU began work on implementing standardization systems for "Romanizing" Arabic by offering training to all applicable FBI employees. According to the FBI, by the end of the second quarter of FY 2003, 371 FBI employees had received training in Arabic "Romanization," while classes continue to be held. Regarding Chinese "Romanization," the LTAU announced in September 2002 that training on Chinese "Romanization" was being offered to all applicable FBI employees. As of June 9, 2003, a total of 80 FBI employees had been trained in Chinese "Romanization," while classed continue to be held. Further, the LTAU has

been working with the VCF project management team to create a keyboard for the "Romanization" of names.

In addition to training, the FBI expects the VCF to help database operators apply foreign names to searches within databases. For example, the VCF will allow the addition of standard telegraphic code (STC) for Asian names, Unicoded[44] for other foreign names, and it will deploy a name search engine that incorporates variations on names. Because the first release of the VCF is not scheduled for completion until December 2003, this recommendation remains open.

(f) Summary

Despite the FBI's progress in taking corrective actions, a more comprehensive enterprise-wide solution to the underlying deficiencies will not occur until the VCF is implemented. As a result, some of these deficiencies have gone uncorrected for over three years.

(3) McVeigh Report

In March 2002, the OIG issued a report entitled, "An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case." The McVeigh report concluded that the belated production of case-related documents resulted in part from the following long-standing problems at the FBI: (1) antiquated and inefficient computer systems, (2) inattention to information management, and (3) inadequate quality control systems. The report further stated that the FBI's troubled information management systems were likely to have a continuing negative effect on the FBI's ability to properly investigate crimes.

The McVeigh report stated that the FBI had not given sufficient attention to correcting deficiencies in information management and the ACS system. The IT-related findings of the report showed that the ACS system was extraordinarily difficult to use, had significant deficiencies, and was not suitable for the FBI in the 21st century. The report noted that inefficiencies and complexities within the ACS system, combined with the lack of a true information management system, contributed to the FBI's failure to provide hundreds of investigative documents to the defendants in the Oklahoma City bombing case. To overcome these problems, the report made recommendations on how future information systems should be developed.

[44] Unicode provides a unique number for every character. Fundamentally, computers just deal with numbers. They store letters and other characters by assigning a number for each one.

The McVeigh report provided 21 recommendations to the FBI, 15 of which directly related to IT.[45] Of these 15 recommendations, 11 involved the FBI's completion of the VCF, 3 involved special agent computer training, and 1 pertained to deadlines for the completion of case leads.

(a) Deadlines for the Completion of Leads

In the McVeigh report, the OIG recommended (recommendation 13) that the FBI ensure that deadlines for the completion of investigative leads are clear and not undermined by the automated system, such as the ACS system's setting of a 60-day deadline for "immediate" leads. The FBI stated that as of August 26, 2002, the settings for deadlines within the ACS system were changed to one day for "immediate" and "priority" leads. Based on the OIG's review of the policy changes for leads documented in three Electronic Communications (EC) and the MIOG, we believe that the FBI's actions to address this recommendation are adequate.

(b) Special Agent Computer Training

The McVeigh report contained the following three recommendations related to computer training for special agents:

- the FBI should evaluate its computer training in order to develop a clear understanding of what agents need to perform their jobs effectively (recommendation 8);

- the FBI should consider whether computer usage should be a part of the core skills needed to graduate from new agent training (recommendation 9); and

- the FBI should consider mandatory refresher training for veteran agents (recommendation 10).

Regarding recommendation 8, the FBI has reported to the OIG that it has undertaken various initiatives to improve its computer training for special agents. In April 2003, the FBI stated that its Training Division was assessing the computer skills agents need to perform their jobs and was determining the need for additional improvements to the computer training curriculum for new agents. The Training Division was using instruments

[45] These 15 recommendations, along with a summary of the FBI's responses to the recommendations, are listed in Appendix 2.

such as surveys, evaluations, and questionnaires to evaluate and make adjustments to its computer training. These instruments, which are completed by agents and managers in the field, were to help the FBI determine whether the curriculum adequately prepared new agents. In May 2003, the FBI provided the OIG with copies of the instruments used, as well as two ECs issued in July 2002, which included a request to add additional computer training for new agents. We believe that the FBI's actions to address this recommendation are adequate.

Regarding recommendation 9, the FBI reported to the OIG that the Training Division has implemented a policy requiring all new agents to pass an exam on core computer competency skills prior to graduation. In May 2003, the FBI provided the OIG with an EC dated August 14, 2002, that mandates the "Final Investigative Computer Competency Skills Assessment," as the twelfth examination required for graduation from the new agent training. After examining this computer skills assessment, we believe that the FBI's actions to address this recommendation are adequate.

Regarding recommendation 10, the FBI has reported to the OIG that it has implemented a program of continual mandatory training for veteran agents and all employees. On December 12, 2000, the Training Division issued an EC requiring that each FBI employee receive 15 hours of training per year. The Training Division developed a continuing education program to establish employee and supervisor responsibilities for complying with the program and to identify training opportunities for FBI employees. To enforce the training requirement, the FBI linked the continuing education requirement to the performance evaluations of employees and supervisors. Additionally, in June 2001 the FBI revised the training section of the MAOP to incorporate the new continuing education policies. After examining continuing education program guidelines and policy changes, we believe that the FBI's actions to address this recommendation are adequate.

In our judgment, the FBI has demonstrated that it has taken adequate corrective actions to address the training deficiencies identified in the McVeigh report. While these actions have clearly been important, the FBI must also ensure that agents receive adequate training on the VCF, which will be critical to its success.

(c) Recommendations Involving the VCF

FBI officials have stated that when implemented, the VCF or UAC portion of Trilogy will address 11 of the 15 IT-related recommendations

contained in the McVeigh report. These 11 recommendations are to:

- foster an attitude among all employees that information management is an essential part of the FBI's mission and that automation is a key tool in managing the storage, analysis, and retrieval of information (recommendation 1);

- consider whether Trilogy's document management systems can be simplified, such as by having supervisors review electronic copies of documents, and whether its record keeping formats can be reduced in number (recommendation 2);

- evaluate whether inserts should be eliminated (recommendation 3);[46]

- evaluate its practices regarding "originals" of FBI created documents (such as FD-302s) (recommendation 4);

- ensure any new automation is user-friendly, meaning that the steps required to obtain information should be few in number and intuitive (recommendation 5);

- ensure any new automation system include an effective document tracking system (recommendation 6);

- eliminate crisis management software and other independent systems (recommendation 7);

- ensure that leads cannot be covered without an explanation of what has been done to the task assigned (recommendation 11);

- ensure future automation systems incorporate a system to allow supervisors to easily track the status of leads (recommendation 12);

- evaluate the feasibility of developing a system of universal lead numbers to eliminate the use of local lead numbers as a tracking mechanism (recommendation 14); and

- evaluate the use of lead numbers on leads and responding reports and determine whether new policies, better enforcement

[46] Inserts are forms used by the FBI to record investigative activity that is not considered to be significant to the investigation.

of existing policies, improved training, or better automation is the best method of fixing the problem (recommendation 15).

The following paragraphs discuss how, when completed, the VCF will help implement these 11 recommendations.

Recommendation 1

While the FBI has taken steps to foster an attitude among all employees that information management is an essential part of the FBI's mission (including the creation of a Records Management Division), the VCF must be used by all levels at FBI Headquarters and by field supervisors to ensure its success. In May 2003, FBI officials stated that agents will be required to use the VCF since all official case records and files up to the Secret level will be within the application. According to the FBI, unlike the currently used ACS system, there will not be ways for agents to circumvent the use of the VCF. However, the FBI still has not finalized its policies for how agents will utilize VCF from remote locations.

Recommendation 2

FBI officials stated that the VCF will streamline the workflow process by including electronic signatures and reducing the number of required forms. Under the FBI's current investigative process, a case file could be started by using one of many different standardized forms, such as FD-72, FD-801, and FD-822, depending on the type of investigative category. The forms will be replaced by the "intake" function of the VCF, which simplifies the initiation of a case file by eliminating the need for these forms.

Recommendation 3

FBI officials stated that inserts would be eliminated with the deployment of the VCF. All VCF records will be considered "resident to the case," meaning that they will be considered an official investigative record.

Recommendation 4

FBI officials told us that the VCF will essentially replace all paper copies of investigative events. Because the Records Management application will interface with the VCF, the only official record of the case file will be maintained in the VCF. The intent of the VCF is to reduce, and in some cases eliminate, the need for paper copies of documents.

Recommendation 5

According to FBI officials, the VCF will operate in a "point-and-click" web environment that will simplify the FBI's workflow process for document storage and retrieval. Agents not familiar with using a computer keyboard can have their secretaries type information into the VCF, but the agents will still have to sign-off on the file using a mouse to create an electronic signature. Additionally, the FBI is building an integrated data warehouse comprised of data from the ACS system, analyzed terrorism and intelligence data, and other law enforcement data. Through servers built on the FBI's new Trilogy networks, the VCF will interface with the data warehouse. The VCF will contain tools to assist FBI agents and analysts in performing queries and searches.

Recommendation 6

FBI officials told us that the VCF's automated document creation, receipt, and management system will partially eliminate the need for traditional tracking systems. The VCF will include capabilities to scan into the case file any documents received from sources external to the FBI, as well as to capture summary descriptions of any documents and items, such as physical evidence, that cannot be stored electronically. The FBI's intent is to eventually track external items through a bar code identification system that would be placed upon a physical label on the external document and then linked to an electronic record. Additionally, FBI officials said that the Records Management Division (RMD) is establishing systems and processes to effectively track documents and records contained in FBI systems.

Recommendation 7

According to FBI officials, the VCF will consolidate five of the FBI's investigative applications. However, FBI officials recognize that the VCF is only a starting point since numerous other investigative and application systems exist that could be integrated into the VCF. Additionally, because of unresolved connectivity issues, crisis management software may still need to be used by agents after the initial deployment of the VCF. The FBI is identifying and defining other databases and crisis management software that should be included in future VCF releases to maximize the efficiency of the workflow process. FBI officials told us that additional funding will be needed to solve the connectivity issues at remote locations, as well as to consolidate and eliminate other databases and crisis management software.

Recommendations 11, 12, 14, and 15

FBI officials said that upon the entry of a lead into the VCF, the system will automatically assign a universal lead number that is unique to each case. The supervisor will then approve and assign the lead to a subordinate agent or receiving office. The VCF allows the supervisor to view the subordinate agent's leads and caseload to allow for the leads and cases to be assigned effectively. Leads can viewed by anyone in the FBI with appropriate access privileges, or by anyone with a profile query established to receive information pertaining to specific types of cases. Additionally, split leads, or leads created from an original lead, will reflect the derivative or parent-child relationship in its lead number to facilitate the tracing of all leads to their origin. This feature allows the originating office and all receiving offices to determine to whom the leads are assigned or whether action on the leads has occurred, which provides agents and managers with a user-friendly tool to ensure lead accountability. Because all leads will be part of the case file, leads cannot be covered without an appropriate explanation unlike the FBI's current system.

Summary

We believe that the FBI has demonstrated progress toward implementing the recommendations in the McVeigh report, based on its corrective actions taken to date, as well as its plans for the VCF. However, the adequacy of the FBI's corrective actions generally cannot be determined until the VCF has been deployed. The FBI's ability to implement many of the OIG's IT recommendations and improve its IT program depends on the successful implementation of the VCF. The following section, therefore, discusses factors affecting the success of the VCF.

(4) Factors Affecting the Success of the VCF

In our judgment, if the VCF can do what the FBI expects, the VCF will represent a significant technological advancement from the ACS system. The VCF has the potential to reduce redundancy in searching multiple databases, improve the FBI's case file management, and maximize the use of information in the FBI's possession.

While the VCF has the potential to significantly improve the FBI's IT, as well as its record management and investigative efficiency, the ultimate success of the VCF depends on a number of different factors, including whether the VCF will meet its technical and performance expectations and be accepted and used by FBI employees.

(a) Technical and Performance Expectations of the VCF

To ensure its success, the VCF must meet technical and performance expectations. As mentioned above, the Trilogy project has encountered significant cost overruns and schedule delays due to the FBI not following critical management processes. The OIG's ITIM report stated that these management problems contributed to difficulties with establishing the technical requirements for the VCF. Because the VCF is focused on making significant changes to five of the FBI's investigative systems, documentation for the exact configuration of these legacy systems was critical to designing the requirements for the VCF. The lack of documentation for the configuration of these five investigative systems 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 had to perform reverse engineering on the five systems, there are limitations as to how rapidly the VCF can be developed and deployed.

As of April 2003, the FBI was still defining the technical requirements for the second and third releases of the VCF. Because the technical requirements had not yet been finalized and funding has not been approved, baselines for the VCF had not been established. We believe that the lack of technical, cost, and schedule baselines not only creates uncertainties over how much the VCF will cost and when it will be completed, but also how it will perform upon implementation.

Performance of the VCF could be measured by how well it: (1) allows special agents to access, import, create, and scan documents through a web-based point and click environment; (2) allows supervisors to track case files and lead numbers; (3) streamlines the workflow process through the use of electronic signatures and the reduction of paper forms; and (4) eliminates the need for special agents to use other applications, such as crisis management software. For VCF to make these and other improvements, it must have built-in security features that allow special agents and analysts to access information according to their security clearances and "need to know." Additionally, it must be able to meet the needs of all FBI employees, including those performing counterterrorism duties, which is the FBI's highest priority. It must also lay the foundation for information sharing outside the FBI. We believe that the performance of VCF and, specifically, how it meets the needs of special agents and analysts, will determine how quickly the VCF is accepted and used.

(b) Acceptance and Use of the VCF

If the VCF is to be a vehicle for moving the FBI's information management into the 21st century, it must be accepted and used. Historically, the FBI has been a paper-driven organization. A goal of the VCF is to move toward a near paperless environment so the FBI can maximize the use of technology to digitally capture information for data management and control. According to FBI officials, the VCF is the first real change in the FBI's workflow and processes since the 1950's. Director Mueller recently stated that "Trilogy [VCF] will change the FBI culture from paper to electronic."

As noted in the Campaign Finance and McVeigh reports, special agents did not always use the ACS system to manage their case files. For various reasons, they found alternative ways to manage case files. The VCF must be used by all special agents for the FBI to fully realize its benefits.

FBI officials told us that since the VCF will contain the official case files, agents will have to use the VCF since there will be no other acceptable means to manage case files. However, FBI official also acknowledged that because of unresolved connectivity issues at remote locations, agents may still need to use crisis management software.

2. FBI's Process for Following-Up on Recommendations

Until recently, the FBI had not implemented an effective system of management controls to ensure that recommendations are resolved and implemented in a timely and consistent manner. As previously stated in this report, the FBI is required under OMB Circular A-50 and DOJ Order 2900.6A to establish a process for resolving audit deficiencies and taking corrective actions in a timely manner. As a result, we do not believe that the FBI was in full compliance with OMB Circular A-50 and DOJ Order 2900.6A.

FBI personnel told us that while a formal process to track and resolve recommendations did not exist prior to September 2002, an informal process was used. Upon the final issuance of an OIG or GAO report, the recommendations were forwarded to the responsible FBI Divisions. Someone within the responsible Division was then assigned to respond to the recommendations until closure occurred. However, the FBI recognized that this informal process was not sufficient to ensure corrective actions were timely and responsive. Specifically, the FBI officials indicated to us that the informal process:

- was not documented in formal policies and procedures,
- was not adequately monitored by executive management and not kept up-to-date,
- used multiple applications,
- did not keep measures of timeliness and responsiveness, and
- did not provide for sufficient follow-up once the original response or corrective action plan was submitted.

We believe that the lack of management attention was a significant cause of the FBI's failure to implement prior OIG and GAO recommendations. According to the Deputy Assistant Director of the Inspection Division, high turnover within FBI management contributed to problems with maintaining current responses to OIG and GAO reports. Under the informal process, when individuals left the FBI or were reassigned within the Bureau, their replacements were not always made aware of recommendations or requests that were left pending. As a result, responses to recommendations and any related corrective action were often delayed, and the auditing or investigating agency had to again request a response to its recommendations.

The FBI has also recognized that improvements in its system of managing follow-up were needed to resolve and timely implement recommendations resulting from OIG and GAO reports. In September 2002, the FBI's Inspection Division began to establish a new management process to improve the FBI's timeliness and responsiveness of corrective actions resulting from OIG and GAO recommendations and to bring the FBI in compliance with applicable regulations (OMB Circular A-50 and DOJ Order 2900.6A) for the follow-up and resolution of audit recommendations. To facilitate the implementation of this new management process, the Inspection Division developed a database, referred to as the "Automated Response and Compliance System" (ARCS). According to the FBI, ARCS is an automated tool that is intended to:

- document and track initiated, ongoing audits and data requests from OIG, GAO, and others;
- track recommendations made in OIG and GAO audits, investigations, and reviews until closure; and

- provide status information to FBI's executive management on, or close to, a real time basis.

The FBI's new database tracks the receipt and resolution of audits, investigations, and data requests from the OIG, GAO, and others. It also tracks the tasks associated with FBI's current re-engineering efforts. Among its functions, the database is intended to provide information to FBI management on a regular basis to keep them informed of a report's progress and to ensure timely implementation of recommendations. However, this database does not include vulnerabilities generated by system audits required by GISRA. The FBI's Information Assurance Section has taken steps to develop a separate database to record and manage the status of system audit vulnerabilities.

The ARCS database tracks audit reports within four hierarchical levels: (1) the report level, (2) the findings level, (3) the recommendation level, and (4) the action or task level. The report level provides general information about the report, such as the report title and number, status, classification level, requesting official (for GAO audits), issue date, received date, response due date, and FBI Division point-of-contact. The findings level describes the findings of the audit. The recommendation level is under the findings level and describes the issuing entity's suggestions to address the findings. The action or task level specifies what corrective actions the Bureau will take in order to satisfy the recommendations (and therefore, the findings).

In conjunction with the development of the database, the FBI has developed policies and procedures for the Inspection Division's responsibilities for resolving OIG and GAO reports. These policies and procedures require the Inspection Division to assign a liaison for each report with outstanding recommendations and for scheduled audits and reviews. The liaison has the primary responsibility for entering information into the database, including deadlines for when tasks should be completed. The liaison also has the responsibility to ensure that the report is assigned to a "project manager" and that individual tasks are assigned to appropriate points-of-contact. This control ensures that appropriate FBI personnel can be held accountable for taking timely corrective actions. The liaison monitors the completion of tasks and is instructed to send periodic e-mail notices when tasks are near their due date or past due. Additionally, Inspection Division management reviews the activities of the liaisons to ensure that liaisons are adequately monitoring their assigned projects.

In January 2003, the Inspection Division officials trained its liaisons on the ARCS system. An Inspection Division official told us that any new liaisons will be trained on an as-needed basis. As of May 2003, 13 liaisons have been trained on the ARCS database.

As of May 2003, the FBI was still adding relevant information to the ARCS database for open GAO reports. For OIG reports, Inspection Division personnel told us that the database had been updated to include all reports with open recommendations. However, we found that the ARCS database did not include the OIG Campaign Finance report that contained 18 open recommendations. Inspection Division personnel told us that certain highly sensitive reports — such as the Campaign Finance report or matters involving the Office of Professional Responsibility may not be added to the database, due to the classified nature of the reports. Based on our inquiry, the Inspection Division began researching the status of the Campaign Finance recommendations.

FBI officials said that the database, which is maintained on the FBI's intranet, generates reports for senior FBI management that provide information on upcoming suspense dates. For example, the Deputy Directors are required to perform quarterly reviews of their Division's progress in completing outstanding tasks. According to FBI officials, the Inspection Division Assistant Director uses reports generated by the ARCS database to discuss outstanding tasks at weekly executive meetings, which are attended by the Assistant Directors, Executive Assistant Directors, and the Director. These and other reports have been periodically forwarded to the Director, upon his request. FBI officials told us that the Director has taken a particular interest in the timeliness and responsiveness of the FBI's corrective actions, re-engineering efforts, and responses to Congressional requests. The Director wants to be notified, especially with regard to high profile reviews, when the FBI has not been timely and responsive in its planned actions.

While the ARCS database can be a useful tool for the FBI's establishment of a management process directed toward improving the timeliness and responsiveness of its corrective actions, the ultimate effectiveness of this system depends on formal and consistent oversight from senior FBI management. Thus far, however, the FBI has not promulgated written directives Bureau-wide that instruct program managers and senior officials outside of the Inspection Division regarding their obligation to take corrective actions that will close recommendations. In our judgment, the FBI must develop and institute formal written procedures that require senior management oversight of the timeliness and responsiveness

of recommendations. These written procedures should also incorporate the policies for tracking the status of vulnerabilities generated by IT system audits.

3. Summary

Since 1990, reports issued by the OIG have found numerous deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training. While the FBI has implemented many of the recommendations contained in these reports, significant further actions are necessary to ensure that the FBI's IT program effectively supports its mission. Of the 148 IT-related recommendations issued by the OIG, 93 have been closed by the OIG, while 55 remain open. The following table provides a summary of the status of IT recommendations issued to the FBI by the OIG.

Summary of the Status of IT Recommendations Issued to the FBI

	Number of Open Recommendations	Number of Closed Recommendations	Total Number of Recommendations
OIG Detailed Financial IT Reports	22	83	105
OIG FY 2001 GISRA Report	17	6	23
OIG Special Reports	16	4	20
Total	**55**	**93**	**148**

Source: OIG analyses as of April 2003

OIG audits and reviews indicated that deficiencies remained in the area of general controls over FBI Headquarters data systems, except for system software. As of April 2003, 22 out of 105 recommendations issued for FY reports 1996 through 2001 remained open. Additionally, the FY 2001 GISRA report stated that the FBI has been slow to take corrective actions since many of the vulnerabilities were previously reported in annual audits of general controls. Of the 23 recommendations from the FY 2001 GISRA audit, 17 remained open as of April 2003. Further, the FY 2002 GISRA report on the FBI's ACS system stated that similar vulnerabilities that were reported in the FY 2001 report continued.

The FBI GISRA reports issued in May and November 2002 identified vulnerabilities with management, operational, and technical controls over computer security. These reports also stated that within the FBI, only the Inspection Division tracked remedial actions for reported computer security vulnerabilities. With the exception of audits performed by the OIG, the FBI's

Inspection Division did not track the ACS or DRUGX systems' vulnerabilities identified in other audits and their corresponding corrective actions. Further, these reports stated that the Inspection Division did not receive any other audit results or reviews outside of the OIG audits and therefore has limited knowledge of other reported vulnerabilities.[47]

Until recently, the FBI did not establish a system of management controls for tracking recommendations, as required by OMB Circular A-50 and DOJ Order 2900.6A. As a result, the FBI did not consistently implement recommendations and did not adequately improve its information technology to ensure that data is safeguarded and reliable, and computer application programs are secured and protected from unauthorized access. Additionally, non-implementation of previously identified IT problems, especially regarding the ACS system, have contributed to problems in sensitive investigations, such as the Campaign Finance and McVeigh investigations. However, current FBI leadership has stated that they are committed to enhancing controls to ensure recommendations are implemented in a consistent and timely manner. To this end, the FBI recently established a system to facilitate the tracking and implementation of recommendations. Also, the FBI expects the VCF, as part of the Trilogy project, to significantly improve its IT and correct many of the deficiencies identified by the OIG.

According to the FBI, the VCF is intended to not only correct many of the deficiencies identified in the Campaign Finance and McVeigh reports, but also to revolutionize the FBI's workflow process. We believe that the corrective actions underway, including the planned implementation of the VCF, has the potential to address 16 of the 20 open OIG recommendations we examined from the Campaign Finance and McVeigh reports. However, the ultimate effect of the VCF remains to be seen. We believe that the success of the VCF depends on whether it can meet its technical and performance expectations, and be accepted and used by FBI employees.

[47] In April 2003, the Inspection Division began tracking findings and recommendations issued by the GAO.

4. Recommendations

We recommend that the Director of the FBI:

1. Develop, document, and implement Bureau-wide procedures to follow-up and close audit and investigative recommendations, in accordance with OMB Circular A-50 and DOJ Order 2900.6A. This process should include the tracking and resolution of system audit recommendations.

2. Ensure that the ARCS database is complete and includes recommendations from all sources of OIG audits and reviews.

3. Ensure that managers are held accountable for the tracking, resolution, and timely implementation of OIG recommendations.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

In accordance with Government Auditing Standards, we audited the FBI's implementation of OIG recommendations related to information technology. In connection with the audit, we reviewed management processes and records to obtain reasonable assurance about the FBI's compliance with laws and regulations that if not complied with, could in our judgment, 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 OMB Circular A-50; and
- the DOJ Order 2900.6A.

Our audit identified areas where the FBI was not in compliance with the laws and regulations referred to above. With respect to those transactions 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 implementation of OIG recommendations related to information technology, 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 track, resolve, and implement audit and investigation recommendations. During our audit, we found the following management control deficiency — the FBI lacked a fully established and documented process that ensures recommendations are implemented in a timely and consistent manner.

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 recommendation resolution and closure process.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The primary objective of the audit was to determine if the FBI has implemented prior OIG and GAO recommendations directed toward improving its information technology.[48]

Scope and Methodology

The audit was performed in accordance with Government Auditing Standards, and included tests and procedures necessary to accomplish the audit objective. We conducted work at FBI Headquarters in Washington, D.C., and GAO Headquarters in Washington, D.C. We also visited internal offices within the Office of the Inspector General, specifically the Financial Statement Audit Office, the Computer Security and Information Technology Audit Office, and the Office of Oversight and Review.

To perform our audit, we conducted 27 interviews with officials from the FBI, OIG, and GAO. The FBI officials interviewed were from the Inspection Division, Information Resources Division, and National Infrastructure Protection Center. Additionally, we reviewed over 100 documents, including prior GAO and OIG reports, Congressional testimony, and documentation on the FBI's process for tracking the resolution of recommendations.

To determine if the FBI has implemented IT recommendations issued by the OIG in the last five years, we made inquiries with OIG management in the Audit Division, Investigations Division, Evaluation and Inspections Division, and the Office of Oversight and Review to identify the applicable reports. Based on our inquiries, we determined that the OIG's detailed internal control reports over the FBI's IT systems in support of the annual financial statement audits (fiscal years 1996 to 2001), the FY 2001 and FY 2002 GISRA reports, and two special review reports contained recommendations related to the FBI's information technology and information management. Based on the records and opinions of the OIG offices responsible for preparing the reports and interviews with FBI

[48] We included recommendations related to document management because FBI documents are generally produced electronically or managed in automated databases and systems.

officials, we then analyzed and summarized the current status of the recommendations.

To determine if the FBI has implemented IT recommendations issued by the GAO in the last five years, we searched the GAO website for reports that included references to the FBI and information technology or information management. From this sample, we reviewed reports to identify recommendations made to the FBI that pertain to IT. Our search indicated that one report contained one recommendation that met our criteria.[49] Additionally, we made inquiries with GAO personnel to determine if they issued any classified reports relating to FBI IT that would not be listed on the website. We were told by GAO personnel that no such classified reports were issued. From the GAO's website, we obtained the status of the recommendation and confirmed the status through inquiries with GAO and FBI personnel, as well as by reviewing supporting documentation.

[49] This report is discussed in Appendix 3.

THE FBI'S PROGRESS TOWARD IMPLEMENTING IT RECOMMENDATIONS

To understand the full context of these recommendations, it is necessary to view the associated report in its entirety. Recommendations that have been repeated in subsequent reports are designated in the following tables by having multiple years in the FY column. The FY column also contains the recommendation number and a designation as to whether the recommendation resulted from a material weakness (MW), reportable condition (RC), or management letter comment (MLC).[50]

1. Recommendations in the Detailed IT Reports Issued in Support of the Annual FBI Financial Statement Audits

Entity-Wide Security Program Planning and Management Controls: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1998 RC#16	The FBI should take steps to clearly assign, identify, and communicate information security responsibilities. Such steps should include the development of detailed organizational charts, job descriptions, and security plans, all of which should be kept current.	The FBI hired a contractor in August 1999 to complete this task. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.
1998 RC#17	Allocate sufficient resources to ensure the proper implementation of its policy requiring all ADPT systems used to process, store, or transmit classified or sensitive information to be accredited every three years.	The FBI hired a contractor in August 1999 to complete this task. This recommendation was closed in October 2002 based on a review of the corrective actions taken.

[50] This only applies to the recommendations from the detailed IT reports issued in support of the annual FBI financial statement audits.

1999 MW#1 1998 RC#14	Ensure that risk assessments of the FBIHQ Data Center, its other general support systems, and all major applications are conducted as required by OMB Circular A-130, and by the FBI's Manual of Investigative Operations and Guidelines: FBI ADPT Security Policy, Part II, Section 35:8.1.3, ADPT Security Policy.	The FBI's March 2001 response to the recommendation stated that a contractor was to conduct a risk assessment and revise the system security plan for the administrative Information Support Systems. This recommendation was closed by the OIG on final issuance of the FY 1999 report, based on a review of risk assessments provided.
1999 MW#3 1998 RC#17	Ensure that the systems and applications are accredited every three years.	The FBI's March 2001 response to the recommendation stated that the re-accreditation of the FBIHQ and Clarksburg Data Centers, the FBI LAN/Wide Area Network (WAN) and the legacy administrative applications were completed during June 2000. This recommendation was closed by the OIG upon final issuance of the FY 1999 report, after a review of the accreditation packages.
1999 MW#4	Renew the interim accreditation for general control systems and major applications and ensure these accreditations: a. reflect a more accurate estimate of the anticipated final accreditations, according to the contractor's planned deliverable due dates and actual progress to date; and b. address the increased threats and vulnerabilities to the FBI's systems, applications, and connectivity, which were identified during penetration test work.	The FBI's March 2001 response to the recommendation stated that the re-accreditation of the FBIHQ and Clarksburg Data Centers, the FBI LAN/WAN, and the legacy administrative applications were completed during June 2000. This recommendation was closed by the OIG in October 2002 based on a review of corrective actions taken.

1999 MW#5 1998 RC#18	The FBI should improve security and application controls by determining which of its systems are classified as "major applications," and ensuring that for each major application, including the Financial Management System and Bureau Personnel Management System (BPMS): • security plans are developed in accordance with OMB Circular A-130, implemented, disseminated to systems users, and periodically updated, as necessary; • risks are assessed when there is a major systems modification, or, at a minimum, every three years; and • the system is accredited at least every three years.	The FBI's March 2001 response to the recommendation stated that the necessary actions were completed and the FBIHQ and Clarksburg Data Centers, the FBI LAN/WAN, and the legacy administrative systems were re-accredited. This recommendation was closed by the OIG upon final issuance of the FY 1999 report based on a review of risk assessment, security plans, and accreditation statements.

Source: OIG analyses as of April 2003

Entity-Wide Security Program Planning and Management Controls: Open Recommendations

FY(s)	Recommendation	FBI's Progress
2001 MW#1 2000 MW#1 1999 MW#2 1998 RC#15	Recommend that the FBI Director: Ensure the ADPT Security Policy requiring security plans are completed appropriately and include: a. system specific rules of behavior; b. training; and c. documentation that outlines the rules of the system, as required by OMB Circular A-130 and National Institute of Standards and Technology Special Publication 800-18.	The FBI's September 2002 response to the recommendations stated that the current certification and accreditation (C&A) effort has been addressing these requirements. In addition, the Education, Training, and Awareness Program intends to sponsor a variety of awareness campaigns targeting the users and IT support staff of the FBI mission-critical and mission essential systems. The FBI has provided a July 2003 estimated completion date for closure of these recommendations.
2001 MW#2	Ensure the Payroll System Security Plan incorporates: a. an incident response capability; b. rules of behavior; and c. system interconnection documentation, if applicable.	The Payroll System Security Plan is currently on the legacy systems' C&A schedule that has been prioritized in coordination with the FBI's Designated Approving Authority and the DOJ Chief Information Officer. The FBI's C&A process will address all aspects of system security in the payroll system. The FBI has provided a July 2003 estimated completion date for closure of these recommendations.

Source: OIG analyses as of April 2003

Access Controls: Closed Recommendations

	Recommendation	FBI's Progress
1996/97 RC#2	The FBI should consider reducing the PWEXP[51] duration from 90 days. Further, the grace period for the expiration of user passwords should be reduced to 5 days.	The FBI's February 1999 response to the recommendation stated that no action would be taken and that that the Bureau was well within the DOJ mandate that called for password expiration every 180 days. Upon further review, the OIG agreed with the FBI's position that no corrective action was necessary. As a result, this recommendation was closed by the OIG upon the issuance of the FY 1996/97 final report.
1996/97 RC#3	Set the TAPE parameter (from the FBI's mainframe computer security package) to "ON."	The FBI's February 1999 response to the recommendation stated that if the Bureau followed the recommendation, the software would not function properly. Upon further review, the OIG agreed with the FBI's position that no corrective action was necessary. As a result, this recommendation was closed on issuance of the FY 1996/97 final report.
1996/97 RC#4	The PWVIEW parameter (from the FBI's mainframe computer security package) should always be set to "NO." If this parameter is changed, proper authorization should be obtained from the data security officer.	The FBI's February 1999 response to the recommendation stated that the Bureau agreed with the recommendation. This recommendation was closed by the OIG upon issuance of the FY 1996/97 final report based on a review of the corrective actions taken.
1996/97 RC#5	Establish procedures that require new users to immediately change their initial password. These procedures should be distributed to the user when they are notified that access has been established.	The FBI's July 1999 response to the recommendation provided information demonstrating adequate corrective actions. This recommendation was closed by the OIG in December 1999 based on a review of the corrective actions taken.
1996/97 RC#6	The FBI should review user access to sensitive system files. After the review, data set access should be modified to restrict user access, including READ and EXECUTE, to sensitive system files.	The FBI's February 1999 response to the recommendation stated that although the Bureau was performing this function, it did not have a formal process documenting these reviews. This recommendation was subsequently closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.

[51] According to the OIG's 1996/97 report, PWEXP is a parameter from the FBI's mainframe computer security package.

1996/97 RC#10	Develop the Authorized Program Facility administrative policies and procedures to ensure compliance with the manufacturer's integrity rules for all its mainframe operating systems.	The FBI's February 1999 response to the recommendation stated that the Bureau conducted semiannual audits to ensure that data sets that no longer needed to be authorized had been removed. This recommendation was closed by the OIG upon issuance of the final report, based on a review of the corrective actions taken.
1996/97 RC#11	Establish policies and procedures to ensure that Novell users are assigned unique passwords.	The FBI's February 1999 response to the recommendation stated that the FBI agreed with the recommendation and that immediate corrective action had been taken. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 RC#12	Modify the Novell Network Administrator facility to prevent Finance Division users from viewing other users' access capabilities.	The FBI's February 1999 response to the recommendation stated that corrective action had been taken. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 RC#13	Establish and distribute procedures requiring local security administrators to periodically, at least quarterly, review employees' access privileges in relation to their current job functions.	The FBI's February 1999 response to the recommendation stated that alternative corrective actions were implemented. The recommendation was closed by the OIG upon the final report's issuance based on acceptable corrective actions taken.
1996/97 RC#14	Evaluate the risks of retaining inactive user identifications beyond 180 days on the system. Modify policies and procedures to ensure compliance.	The FBI's February 1999 response to the recommendation stated that the user accounts were being removed after 180 days of inactivity. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#23	Develop and implement exit procedures that require the local security administrator or security officer to promptly remove user access for terminated employees.	The FBI's February 1999 response to the recommendation stated that the FBI recommended an alternative corrective action. This recommendation was closed by the OIG upon the final report's issuance based on a review of the corrective actions taken.

1996/97 MLC#24	Create an electronic file that identifies terminated and transferred employees. In addition, continue periodically reviewing user access profiles and privileges.	The FBI's February 1999 response to the recommendation stated that the corrective action for this recommendation was completed in October 1998. This recommendation was closed in December 1999 based on a review of the corrective actions taken.
1996/97 MLC#25	Implement appropriate access controls in order to operate at the B1 level of trust.	The FBI's February 1999 response to the recommendation stated that factual inaccuracies existed in the recommendation. However, the recommendation was subsequently closed by the OIG upon issuance of the final report based on acceptable alternative corrective action taken.
1996/97 MLC#26	Review daily reports for the System Management Facility (SMF) record 07 to ensure that SMF records are not being lost due to the untimely dumping of buffer files to tape. Record and include SMF records 17, 18, and 60-69 in normal backup procedures.[52]	The FBI's February 1999 response to the recommendation stated that an alternative corrective action was implemented. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1998 RC#1 1996/97 RC#1	Set the MODE parameter to "FAIL."	The FBI's February 1999 response to the recommendation stated that the testing of the "FAIL" global mode would be initiated to determine if any adverse problems surfaced that would preclude making this a permanent setting. This recommendation is revisited annually by the OIG and was closed on final issuance of the FY 1996/97 and 1998 reports based on a review of the corrective actions taken.

[52] According to the OIG's FY 1996/97 report, SMF record 07 is a control function that shows the quantity of SMF records being lost by untimely dumping of any one of the three SYS1.MAN buffer files to tape. Additionally, SMF records 17 and 18 pertain to the deleting and renaming of data files, respectively. Also, SMF records 60 – 69 pertain to the virtual storage access method data files.

1998 RC#2	Initiate, plan and execute a project to refine the CA-Top Secret[53] profiles to support role-based access controls based upon the access required by system users to complete the responsibilities of assigned roles and responsibilities.	The FBI's June 2000 response did not address this recommendation. However, the recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.
1998 RC#3	Periodically perform an entity-wide data assessment on network systems to determine where potential liabilities exist.	The FBI's June 2000 response to the recommendation stated that the FBI did not agree with the recommendation. Although in their response the FBI disagreed with the finding, documentation was subsequently provided that supported corrective actions taken. The recommendation was closed by the OIG upon issuance of the final report.
1999 MW#7 1998 RC#8a	Delete users that no longer require access to the network or do not have a demonstrated need for their access.	The FBI's March 2001 response to the recommendations stated that the Financial Division Systems Administrators had completed the recommended secure networking environment changes pertaining to these recommendations. These recommendations were closed by the OIG based upon a review of the corrective actions taken.
1999 MW#8 1998 RC#8e 1998 RC#8b 1998 RC#8c 1998 RC#8d	Require unique passwords for all user accounts, particularly system administrators. Restrict users from having concurrent logins. Enable time restrictions for user accounts. Assign account expiration for temporary user accounts.	
1999 MW#9 1998 RC#8f	Require all system administrators to change their passwords at least every 30 days.	

[53] According to the OIG's FY 1996/97 report, CA-Top Secret is the FBI's mainframe computer security package.

1999 MW#11	Conduct a complete audit of the CA-Top Secret and FMS application security to identify all security control weaknesses and develop a plan of action for implementing an effective security program.	The FBI's March 2001 response to the recommendation stated that the FBI is continuing its efforts to modify and hone the FMS Top-Secret Security profiles to ensure the "least privilege" type of access is provided to the FMS customers. This recommendation was closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.
1999 MW#12 1998 RC#4 1996/97 RC#8	Periodically perform an entity-wide data assessment on the mainframe and network systems to determine where potential liabilities exist.	The FBI's March 2001 response to the recommendations stated that during FY 2000, a number of actions were completed relative to the recommendations. These recommendations were closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.
1999 MW#13 1998 RC#5 1996/97 RC#7	Initiate, plan, and execute a project to refine the CA-Top Secret profiles to support role-based access controls based upon the access required by the systems users to complete the responsibilities of assigned roles and responsibilities.	
1999 MW#14 1998 RC#10 1996/97 RC#9	Consider installing "smart card" technology to provide a more robust means of authentication for legitimate users of the FBI systems.	
1999 MW#15	Establish and implement a policy that prevents employees from indiscriminately activating dial-up access to FBI systems.	FBI's March 2001 response to the recommendation stated that the Bureau had purchased commercial-off-the-shelf software and was developing a procedure to perform "war dialing" exercises on all FBI Private Branch Exchange lines. This recommendation was closed by the OIG based on a review of the corrective actions taken.
1999 MW#16	Review the Finance Division's access privileges on the Novell NetWare file and directory objects to ensure that only those individuals requiring read, write, create, modify, and scan have such privileges.	The FBI's March 2001 response to the recommendation indicated that the Finance Division system administrators reviewed the access privileges on the Novell NetWare file and directory objects and made changes to insure proper access. This recommendation was closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.

2000 MW#5	Ensure that the Finance Division Windows NT configuration meets the criteria presented in the FBI Windows NT baseline documentation.	The FBI's September 2001 response to the recommendation stated that the Finance Division system administrators reviewed access privileges on the Novell NetWare file and directory objects and made changes to insure proper access. Changes were made to allow access to file and directory objects based on assignment. This recommendation was closed by the OIG upon issuance of the FY 2000 final report based on a review of corrective actions taken.
2000 MW#6	Ensure all shares providing full access are removed. In addition, all Finance Division administrators should receive network security training to properly ensure that they are kept abreast of current and proper administrative techniques.	The FBI's June 2002 response to the recommendation stated that all employees responsible for the Division's servers had been properly trained and certified. The FBI also provided a list of the courses offered. This recommendation was closed by the OIG in October 2002 based on a review of corrective actions taken.
2000 MW#7	Ensure all user accounts inactive for over 90 days are suspended and user accounts inactive for 180 days are deleted from the Finance Division's LAN.	The FBI's June 2002 response to the recommendation provided information and evidence of corrective action. This recommendation was closed by the OIG in October 2002.
2000 MW#8	Ensure the current service pack is installed on all Microsoft Windows NT environments.	The FBI's September 2001 response to the recommendation stated that a team was formed to ensure that proper software updates and configuration standards are maintained. The recommendation was closed by the OIG upon issuance of the FY 2000 final report based on a review of corrective actions taken.
2000 MW#9	(U) Ensure the database administrator Top Secret Accessor Identification (ACID) profile is reviewed and altered to ensure that only the least amount of privileges are granted to complete assigned job tasks.	The FBI's September 2001 response to the recommendation stated that the FBI reviewed the profile of the database administrator and altered the profile to provide privileges required to complete tasks. The OIG closed this recommendation in October 2002 based on a review of the corrective actions taken.
2000 MW#10	Ensure the removal of the IBMUSER account from the mainframe.	The FBI's September 2001 response to the recommendation stated that this issue was resolved before December 2000. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.

Source: OIG analyses as April 2003

Access Controls: Open Recommendations

FY(s)	Recommendation	FBI's Progress
1998 RC#7	Periodically perform an entity-wide data assessment on network systems to determine where potential liabilities exist.	The FBI's June 2000 response to the draft report stated that the FBI's Information Resources Division (IRD) Server Team installed a Gateway 8400 server to address this recommendation. Verification is still required to close this recommendation.
1998 RC#9	Develop formal procedures to establish audit trails in the security features of networks that are consistent across all divisions/departments, including the activation of NetWare's "Intruder Detection." These procedures should include provisions to reinforce the active monitoring of that security information.	The FBI's June 2000 response to the draft report stated that the FBI is taking corrective actions, but technical controls over the Finance Division LAN were not fully implemented. This recommendation can be closed when annual financial statement audit test work verifies that the FBI has developed formal procedures to establish audit trails in the security features of its networks that are consistent across all divisions and departments, including the activation of NetWare's "Intruder Detection."
1998 RC#11	Strengthen user authentication controls by implementing an active token for user authentication.	The FBI's June 2000 response to the draft report stated that the necessary corrective action had been completed. This recommendation can be closed when annual financial statement audit test work verifies that user authentication controls have been strengthened by implementation of an active token for user authentication.
1998 RC#12	Provide computer security training to users at least annually. Training should include a process for reporting computer-related incidents.	The FBI's June 2000 response to the draft report stated that the necessary corrective action had been completed. This recommendation can be closed when annual financial statement audit test work verifies that computer security training has been provided to users at least annually.
1998 RC#13	Establish a computer incident response team to manage computer related security incidents.	The FBI's June 2000 response to the draft report stated that the necessary corrective action had been completed. This recommendation can be closed when annual financial statement audit test work verifies that the FBI has established a computer incident response team for managing computer related security incidents.

2000 MW#4 1999 MW#17,18	Ensure all accounts have strong passwords.	The FBI's March 2001 response to the recommendation stated that a new policy was created requiring unique passwords, and those passwords had to be changed every 90 days. The OIG's October 2002 response to the FBI stated that this recommendation remains open until it can be verified that strong password controls are in place and the FBI has established a policy requiring a unique password and each user account is periodically reviewed for compliance.
1999 MW#19	Ensure that the Finance Division's LAN administrators check their Novell NetWare configuration against the parameters in the FBI Novell NetWare Baseline Documentation and ensure it agrees with the recommended FBI MIOG, and FBI ADPT Security Policy configuration settings.	The FBI's March 2001 response to the recommendation stated that the Finance Division system administrators enabled auditing on all volumes with the exception of CD-ROM volumes. The FBI's response dated June 2002 stated that all Finance Division servers had been upgraded and configured to meet current security guidelines and that auditing has been enabled on all volumes. The OIG's response dated October 2002 stated that this recommendation can be closed when annual financial statement audit test work verifies that auditing is enabled as required.
2001 MW#3 2000 MW#2 1999 MW#6 1998 RC#6	Ensure compliance with documented policies and procedures as they pertain to account restrictions, system monitoring, and data confidentiality for the FBI's information technology environments.	According to OIG correspondence to the FBI, these recommendations can be closed when annual financial statement audit test work verifies the FBI's Trilogy upgrades, scheduled for February 2003, include automated systems for monitoring server configurations to ensure that settings that affect policies and procedures are not changed accidentally.
2001 MW#4 2000 MW#3 1999 MW#10 1998 RC#8g	Enable the auditing function on the Finance Division's Netware environment.	According to OIG correspondence to the FBI, this recommendation can be closed when annual financial statement audit work verifies that auditing is enabled on all volumes and objects on the Finance Division's LAN.

2001 MW#5	Continue developing the database programmer profile to ensure the database staff are only granted the access needed to perform their job tasks. Additionally, we recommend the systems programmer ACID not access the "PAY.* datasets."	The FBI's September 2002 response to the recommendation stated that the Unit Chiefs of the Systems Programming and Integration Unit (SPIU) and the Data Management Unit had agreed to a restructuring of functions for staff in both units. A transition plan to implement this restructure had been finalized. Additionally, Systems Security and Access Unit staff were in the process of implementing separate security profiles for SPIU and Data Management Unit staff based on the access levels agreed to by the Unit Chiefs of each unit. Further, Systems Security and Access Unit staff had removed access to the "PAY.* datasets" for the systems programmer ACID in question.

Source: OIG analyses of April 2003

Application Software Development and Change Controls: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1996/97 MLC#28	Develop and maintain a configuration management process addressing changes to overall ADPT resources. Configuration changes should be reviewed, approved, tested, evaluated, and documented to show the impact on computer and telecommunications security features.	The FBI's February 1999 response to the recommendation stated that although the FBI had developed the Architecture Change Management Rules, Standards, and Procedures Version 1.0 document, the implementation was still ongoing. The ongoing status was also repeated in the FBI's response dated July 1999. The recommendation was closed by the OIG in October 2002 based on a review of corrective actions taken.
1996/97 MLC#29	Expedite the implementation of the ACM methodology entity-wide. Remove write access privilege from the profile of an individual who does not require that type of access.	The FBI's February 1999 response to the recommendation stated that although the Bureau developed ACM procedures and incorporated the LAN management into the ACM Rules, Standards and Procedures, the status of the corrective action was still ongoing. This recommendation was closed by the OIG in October 2002 based on a review of corrective actions taken.
1996/97 MLC#31	The SPIU should develop and implement procedures to ensure all system problems are entered into NetMan.	The FBI's February 1999 response to the recommendation stated that the SPIU Unit Chief would draft a policy mandating the entering of all system problems into NetMan and that this policy would be effective by March 1999. This recommendation was closed in December 1999 by the OIG based on a review of the corrective actions taken.
2000 MW#17 1999 RC#36 1996/97 RC#17	Ensure the IRD enhances the ACM document to comprehensively address any type of change to the computer based application system and its environment, including changes to hardware, software, and firmware. Once the enhancements are made, ensure the FMS program owners consistently apply the policy to establish a division-wide commitment to software maintenance.	The FBI's September 2001 response to the recommendation stated that FBI management did not totally agree with the recommendation. However, the QCMU had developed an action plan to ensure all IRD software development and maintenance projects complied with change management policies and procedures by an estimated completion date of September 2001. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.

2001 MW#6 2000 MW#19	a. Ensure that the methodology set forth within the ACM is consistently applied to the FMS application. All changes should be documented in the Service Center software. b. Implement the unit test and system plans throughout IRD to standardize, control, and document changes made to the application and system software. The use of the Service Center software to track all change requests, from initiation through final disposition, should be enforced with the planned compliance audits throughout IRD.	The FBI's September 2001 response to the recommendation stated that the QCMU developed an action plan to ensure all IRD software development and maintenance projects complied with change management policies and procedures. The recommendation was closed in October 2002 based on a review of the corrective actions taken.
2000 MW#18 1999 RC#44	Enforce emergency change procedures stated within the ACM for applications. At a minimum, the emergency change procedures should be documented after the fact and should specify: • when emergency software changes are warranted; • who may authorize emergency changes; • how emergency changes are to be documented; and • within what period after implementation the change must be tested and approved.	The FBI's September 2001 response to the FY 2000 recommendation stated that the IRD Payroll Application Project Manager had been advised that he must follow the ACM Procedures defined in the IRD and that all emergency changes need to be entered in the Service Center Management tool. The FY 2000 recommendation was closed by the OIG upon final issuance of the FY 2000 report and the OIG followed-up on this recommendation through its monitoring of the status of the FY 1999 report. The FY 1999 recommendation was subsequently closed by the OIG in October 2002 based on a review of corrective actions taken.

Source: OIG analyses as of April 2003

Application Software Development and Change Controls: Open Recommendations

FY(s)	Recommendation	FBI's Progress
1996/97 MLC#30	Develop and implement a policy requiring periodic independent reviews of all major systems development activities at each major activity milestone. The policy should specify the scope, timing, and format for reporting the results.	The FBI's February 1999 response stated that the QCMU was formed to address this recommendation. The quality control function of QCMU is responsible for performing reviews of all phases of the system development life-cycle. According to FBI correspondence to the OIG (with the most recent dated June 2002), the QCMU is currently in the process of obtaining contract services to assist in the development of a Common Software Process. The QCMU will develop and perform audits to ensure that projects are in compliance with the Project Management Process.
2000 MW#16 1999 RC#35 1998 RC#21 1996/97 RC#18	Implement an automated software management system in order to automate the transfer of all program source code, object code, executable code, interpretable code, control information, and the associated documentation to run a system.	The FBI's September 2001 response to the recommendation stated that a software library management system is needed to control the movement of software components between environments. However, the purchase of the software system was not planned until December 31, 2001. The OIG responded by stating that this recommendation can be closed when it can verify that an automated software management system is implemented.

Source: OIG analyses as of April 2003

System Software Controls: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1996/97 MLC#33	Perform an analysis to determine which libraries and associated members are necessary for proper system performance. A periodic assessment should be performed on the Multiple Virtual Storage operating system to archive and/or delete data sets no longer needed or being used.	The FBI's February 1999 response to the recommendation stated that the Bureau agreed with the recommendation. This recommendation was subsequently closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#34	The SPIU should implement procedures to ensure that all system documentation is current and complete and that changes to documentation are reflected timely and disseminated to applicable individuals.	The FBI's February 1999 response to the recommendation stated that the SPIU has implemented Change Management to comply with the recommendation. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#35	Conduct the following reviews at least quarterly: compare system programmer access privileges per the applicable security software to the employee's current job functions, and adjust accordingly; and, determine system programmer's use of sensitive utilities and reasonableness.	The FBI's February 1999 response to the recommendation stated that the FBI has put an alternate corrective action plan in place because the recommendation was not workable with the current SPIU personnel resources. The recommendation was subsequently closed by the OIG upon the issuance of the final report based on a review of alternative corrective action taken.
1996/97 MLC#36	The SPIU should develop and implement a system software control policy to ensure that system software is current.	The FBI's February 1999 response to the recommendation stated that the FBI would implement the recommended policy regarding system software control by the estimated completion date of March 1999. Additionally, the FBI stated that as of January 1999, all systems executing mission-critical applications had been upgraded. This recommendation was closed by the OIG on issuance of the final report based on a review of the corrective actions taken.

2000 MW#11	Configure the operating system parameters to log all the associated transactions for the respective SMF records.	The FBI's September 2001 response to the recommendation stated that the Bureau employed an alternative method that complied with the applicable regulations. The recommendation was closed in October 2002 by the OIG based on a review of the alternative corrective action taken.
2000 MW#12	Establish and implement a formal change control process for changes to Supervisor Calls and Programs Property Tables programs.	The FBI's September 2001 response to the recommendation stated that the FBI established and implemented an internal change management methodology and process for changes to Supervisor Calls, while a similar process would soon be completed for Programs Property Tables programs. The recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.
1999 RC#35 1998 MLC#21 1996/97 RC#18	Establish and implement a formal change control process for changes to system software. The policies and procedures should include: • documented justification for making the change or utilizing sensitive utilities and management approval; and • periodic inspections, investigations of unusual activities, and recommended actions in the event these activities occur.	The FBI's March 2001 response to the recommendation stated that the SPIU developed an internal change management methodology and process to complement the architecture change management rules, standards, and procedures. In March 2000, this new process was presented to all SPIU personnel. The recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.

Source: OIG analyses as of April 2003

Segregation of Duty Controls: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1996/97 MLC#37	The IRD management should assess the need for additional personnel at the staff level within the data security administrative function.	The FBI's February 1999 response to the recommendation stated that the FBI created a new unit that would address this recommendation. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#38	The IRD should perform an analysis of the potential benefits of applying business process re-engineering and/or activity-based costing processes to current operations in order to enhance effectiveness, efficiency, and productivity.	The FBI's February 1999 response to the recommendation stated that the FBI created a new unit that would address this recommendation. The recommendation was closed by the OIG in December 1999 based on a review of the corrective actions taken.
2001 MW#8 2000 MW#21	Ensure application administrators and programmers do not have direct update access to both test and production application programs.	The FBI's September 2002 response to the recommendation stated that due to the limited resources on projects, application programmers required update access to the production environment. Additionally, as of August 2002, 97 of 152 libraries had been completed. Further, both the PMA and Payroll Applications (addressed in the finding) had been restricted. This recommendation was closed in October 2002 based on a review of the corrective actions taken.

2001 MW#7 2000 MW#20	Establish guidance, policies, procedures, and awareness of segregation of duties within the divisions and units.	The FBI's September 2002 response to the recommendation stated that a goal of the FBI's new Security Division was to develop a professional information security cadre. The role of the Information System Security Officer was under development. A coordinated effort was also underway to define the security knowledge and skills required by the Information System Security Officer role based upon the best practices of Industry and the Intelligence Community. The above-described Security Training, Education and Awareness Program was to assist in ensuring that the appropriate type and level of security knowledge is built into courses and curriculum for the Information System Security Officer as well as each function FBI role. This recommendation was closed during the FY 2002 Financial Statement Audit based on a review of the corrective actions taken.

Source: OIG analyses as of April 2003

Segregation of Duty Controls: Open Recommendations

FY(s)	Recommendation	FBI's Progress
2001 MW#9	Ensure that the administrative process surrounding the payroll-related functions is documented and maintained to ensure the consistent application of the payroll-related administrative process in the Payroll Administration and Processing Unit and Personnel Staffing Unit.	The FBI's September 2002 response to the recommendation stated that the Payroll Administration and Processing Unit, and the Staffing Unit would document payroll related functions and administrative procedures to ensure consistent application by the staff of the two units. The documentation was to include operating manuals setting forth the procedures for processing each of the payroll related functions. The FBI provided an estimated completion date for this recommendation of September 2002.

Source: OIG analyses as of April 2003

Service Continuity Controls: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1996/97 MLC#21	Develop procedures to ensure that daily back-up tapes are stored in a fireproof vault that is secure and not located within the immediate Data Center to prevent the loss of up to nine days of electronic transactions.	The FBI's February 1999 response to the recommendation cited a 3-phase implementation process allowing the FBIHQ Data Center to store the weekly backups from each of its two facilities online. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#22	Keep the daily backup tapes in a fire rated safe if they are located within each division and at the designated off-site location to facilitate recovery in the event of a disaster affecting access to FBIHQ.	The FBI's February 1999 response to the recommendation stated that the Bureau had taken corrective action to ensure LAN server backups were performed on a regular basis and secured accordingly. This recommendation was closed by the OIG upon the final report's issuance based on a review of the corrective actions taken.
1999 MW#20 1998 RC#20b 1996/97 RC#15	Continue plans to develop a comprehensive contingency plan that provides an entity-wide approach for the recovery of mission-critical data processing operation in the event of a disaster, including all FBI resources and business processes. The plan should provide detailed procedures for the recovery of computer operations, including mainframes, microcomputers, workstations, networks and telecommunications, hardware, and facilities.	The FBI's March 2001 response to the recommendations stated that as part of its corrective action, the FBI entered into a contract for the development of a continuity of operations report (COOP) and a concept of operations report (CONOP). The CONOP is for the development of an FBIHQ COOP support system designed to provide critical, uninterrupted FBIHQ support should a terrorist act, natural disaster, or major accident deny use or access to the FBIHQ or its resources. The COOP was scheduled for completion in April 2000. These recommendations were closed upon the issuance of the FY 1999 final report based on a review of the corrective actions taken.
1999 MW#21	Assign responsibility to a team of individuals to ensure full back-up and recovery is performed.	
1999 MW#22 1998 RC#20b 1996/97 RC#16	Periodically test the comprehensive plan, document the test results, and update the plan as necessary.	

1999 MW#25	Design and implement tests of the current disaster recovery plan to ensure that it works and restoration of services occurs in a time frame which is consistent with the expectations of FBI management. Testing should occur not less than annually and include but not be limited to the following components: • supervision by a disaster recovery coordinator; • variation in disaster recovery coordinator; • utilization of multiple teams; • stated objectives; • debriefing sessions; and • retention of adequate documentation.	The FBI's March 2001 response to the recommendation stated that the Data Center Contingency Plan was last updated on February 2001, and is revised semiannually in accordance with Federal Information Processing Standards (FIPS) Publication No. 87, ADP Contingency Planning Guidelines. The OIG responded by stating that the recommendation can be closed when annual financial statement audit test work verifies that management has designed and implemented tests of the current disaster recovery plan. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.
1999 MW#26	Ensure that the FBI or co-located DOJ disaster recovery facility has full back-up capacity.	The FBI's March 2001 response to the recommendation stated that implementation of the IBM Capacity Backup feature ensures that each disaster recovery facility has full backup capacity. The OIG responded by stating that the recommendation can be closed when annual financial statement audit test work verifies that the FBI or co-located DOJ disaster recovery facility has full back-up capacity. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.
1999 MW#32	Ensure all data center personnel are informed when the ADPT contingency plan has been completed and approved and that employees have access to the plan.	The FBI's March 2001 response to the recommendation stated that Data Center Unit employees had been briefed on emergency procedures and responsibilities through hands-on training and by distributing written policies and procedures. The recommendation was closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.

1999 MW#33	Develop entity-wide policies and procedures for performing back-ups, which include: • the required frequency with which files should be backed-up; • off-site rotation policies; • retention policies; • monitoring to ensure that back-ups are complete; and • definition of roles and responsibilities.	The FBI's March 2001 response to the recommendation stated that Application Project Managers are responsible for determining the backup frequency and retention periods as documented in the FBIHQ Computer Center User Reference Manual. This recommendation was closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.
2000 MW#13 1999 MW#28	Include test scenarios and test plans, as suggested by FIPS Publication No. 87, in the FBI's Headquarters Data Center Contingency Plan. Specifically: • identify test scenarios for emergency procedures and disaster recovery, and • establish processing priorities in the event of a disaster.	The FBI's September 2001 response to the recommendation stated that the Data Center Contingency Plan was last updated in February 2001 and that the plan had been finalized and copies were maintained off-site and were disseminated. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.

	Test the contingency plan.	The FY 2000 recommendation was closed by the OIG upon final issuance of the FY 2000 final report.
2000 MW#14a 1999 MW#27	• Prepare and maintain a long-term schedule of the planned semiannual tests to ensure all critical functions covered by the Business Recovery Plan are tested every one to two years, whenever significant changes to the plan have been made, or when there is turnover of key people involved in disaster recovery.	• The OIG followed up on this recommendation through its monitoring of the status of the FY 1999 report. The FY 1999 recommendation was subsequently closed by the OIG in October 2002 based on a review of corrective actions taken.
2000 MW#14b 1999 MW#28	• Test a number of different scenarios while conducting semiannual tests.	• The OIG followed up on this recommendation through its monitoring of the status of the FY 1999 report. The FY 1999 recommendation was subsequently closed by the OIG in October 2002 based on a review of corrective actions taken.
2000 MW#14c 1999 MW#29	• Conduct a full test two to three years to ensure the viability of the disaster recovery plan.	• The OIG followed up on this recommendation through its monitoring of the status of the FY 1999 report. The FY 1999 recommendation was subsequently closed by the OIG in October 2002 based on a review of corrective actions taken.
2000 MW#14d 1999 MW#24	• Finalize the plan and maintain copies at an off-site location.	• This recommendation was closed by the OIG upon final issuance of the FY 2000 report based on a review of corrective actions taken.

2000 MW#15 1999 MW#31	Brief Data Center personnel on emergency procedures and responsibilities through training sessions and by distributing written policies and procedures. Training sessions should be held at least once a year and whenever changes to emergency plans are made.	The FBI's September 2001 response to the recommendation stated that the Data Center Unit employees have been briefed on emergency procedures and responsibilities through hands on training and by distributing written policies and procedures. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.

Source: OIG analyses as of April 2003

Service Continuity Controls: Open Recommendations

FY(s)	Recommendation	FBI's Progress
1999 MW#23	Continue to update the ADPT contingency plan, addressing the weaknesses identified and using FIPS Publication No. 87, ADP Contingency Planning guidelines.	The FBI's March 2001 response to the recommendation stated that the Data Center Contingency Plan was last updated on February 2001, and is revised semiannually in accordance with FIPS Publication No. 87, ADP Contingency Planning Guidelines. The OIG responded by stating that the recommendation can be closed when annual financial statement audit test work verifies that management has acquired the IBM Capacity Backup feature and test plan scenarios have been developed in accordance with FIPS Publication No. 87, Guidelines for ADP Contingency Planning. The FBI's June 2002 response stated that the mainframe was running at 60 percent capacity. The OIG's response dated October 2002 stated that this recommendation can be closed when annual financial statement audit test work verifies that the production test exercise involving transfer of production operations applications to their back-up site has been completed. This exercise was scheduled for November 2002.
2000 MW#14e 1999 MW#30	Ensure the Finance Division has developed and distributed to end-users, a contingency plan covering its information technology applications. The plan should be consistent with the ADPT Contingency Plan maintained by the FBIHQ Data Center.	The FY 2000 recommendation was closed by the OIG upon final issuance of the FY 2000 final report. The OIG followed up on this recommendation through its monitoring of the status of the FY 1999 report. The FBI's September 2001 response to the recommendation stated that the plan has been finalized and that copies are maintained at the off-site location and disseminated to appropriate personnel. The OIG responded by stating that this recommendation can be closed when annual financial statement audit test work verifies that the Finance Division has developed and distributed to end-users a contingency plan covering its information technology applications. The FBI's June 2002 response stated that the completion date for all contingency plans was July 2002.

Source: OIG Analyses as of April 2003

Application Controls: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1998 RC#19	Evaluate FMS security features to determine if control over application transactions can be more effectively managed by CA-Top Secret.	The FBI's June 2000 response to the recommendation stated that that the System Security Access Unit generates a FMS CA-Top Secret profile file on a weekly basis for review by the FMS staff. This recommendation was closed by the OIG in October 2002 based on a review of the corrective actions taken.
1999 MW#34	Review the budgetary module of the FMS, determine the cause of the application security weakness allowing for the transfer of funds beyond the authorized balance, and take the appropriate measures to ensure adequate controls are in place.	The FBI's March 2001 response to the recommendation stated that the FMS software vendor was notified and, after a review of the test data, provided the FBI with a software resolution. The software resolution was successfully tested and implemented into the production FMS in March 2000. This recommendation was closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.
1999 RC#37	Define, document, and communicate the roles and responsibilities for changing code to the Payroll Application.	The FBI's March 2001 response to the recommendations stated that the IRD has limited the number of programmers who can move code to the production environment. Limiting the number of programmers minimizes the risk for unauthorized access to the production environment. These recommendations were closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.
1999 RC#38	Review the list of users having access to the Payroll application code, determine which users should not be making changes in accordance with their duties and responsibilities, and revoke access to users who should not be making changes.	
1999 RC#39	Ensure that user access to payroll code is authorized, documented, and periodically reviewed.	

1999 RC#40	Establish a new Payroll test and development environment.	The FBI's March 2001 response to the recommendations stated that the IRD has created a separate test environment for the Payroll Application. This environment mimics the production environment and permits the programmers to perform complete tests on all changes. When all parties involved are satisfied, the changes are moved to the production environment. These recommendations were closed by the OIG upon issuance of the FY 1999 final report based on a review of the corrective actions taken.
1999 RC#41	Establish a separate test environment for developing and/or modifying application changes.	
1999 RC#42	Periodically review and modify the new test environment.	
1999 RC#43	Adhere to the FBI's change management processes for applications and system software once formal processes have been developed.	
2000 RC#22	Perform an assessment of financial data to ensure the issue has not impacted the FY 2000 Financial Statements.	The FBI's September 2001 response to the recommendation stated that the FMS software vendor was made aware of the problem and provided the FBI a software resolution which was tested and implemented into the production FMS in March 2000. This recommendation was closed by the OIG in October 2002 based on an assessment of the financial data in the FY 2000 financial statements.

Source: OIG analyses as of April 2003

Application Controls: Open Recommendations

FY(s)	Recommendation	FBI's Progress
2000 RC#23	Coordinate with the General Services Administration to synchronize file formats so that data sent via Simplified Intergovernmental Buying and Collection will correctly interface with the FMS application.	The FBI's September 2001 response to the recommendation stated that the Finance Division had not made a request to have the process looked into or to change the file format. The OIG responded by stating that the recommendation could be closed when it verifies that the file formats are synchronized so data can be sent via Simplified Intergovernmental Buying and Collection to correctly interface with the FMS application. Additionally, in October 2002, the OIG's updated response stated that the recommendation could be closed when annual financial statement audit test work verifies that the Intra-governmental Payment and Collection System is in place and manual data entry obligations and expenses are effective.
2000 RC#24	Ensure the FPDS screen is modified to include all the fields required for accurate procurement reporting.	The FBI's September 2001 response to the recommendation stated that the Property Procurement and Management Section was submitting a request detailing the specific fields that need to be added. The OIG responded by stating that this recommendation can be closed when annual financial statement audit test work verifies that the corrective action was completed.
2000 RC#25	Currently there is no restriction in place to prevent operators from selecting any valid field identification or buyer identification. Continue to pursue actions initiated to correct this problem as soon as possible.	The FBI's September 2001 response to the recommendation stated that the software vendor had been requested to make enhancements so that the FMS will subsequently ensure the appropriate enhancements are incorporated. The OIG's most recent response dated October 2002 stated that the recommendation can be closed pending verification of corrective action.
2001 MW#10	Remove the additional access capability from any PMA user not authorized or required to have the additional access to complete their job function.	The FBI's September 2002 response to the recommendation stated that the Financial Systems Unit cost code 0448 is charged with the responsibility of providing technical support for the PMA to include software development and maintenance, quality assurance, ad-hoc reporting, physical inventory support, responsiveness to oversight inquiries, and troubleshooting calls. Due to the nature of PMA activity, Financial Systems Unit management has designated that up to six employees in 0448 should have global access to PMA reporting. In support of this, the Financial Systems Unit will replace 0448 references with software embedded accessor identifications. The OIG responded by stating that this recommendation can be closed upon verification of corrective action.

2001 MW#11	Develop and implement a plan to ensure: a. input control weaknesses identified in the PMA are appropriately addressed, and b. the risk associated with the processing control weaknesses in the PMA are mitigated to ensure that all property is entered, and purchase order and property numbers are accounted for.	The FBI's September 2002 response to the recommendation stated that the Unit Chief of the Property Management Unit will request that the programmers assigned to the Financial Systems Unit modify the PMA to require users to verify the barcode number and the serial number before property is entered into the PMA. In addition, the PMU will contact the Firearms Training Unit and the Firearms-Toolmarks Unit to request that they begin reviewing the firearms and firearm accessories data maintained on the PMA.

Source: OIG analyses as of April 2003

Other Financial-Related IT Areas: Closed Recommendations

FY(s)	Recommendation	FBI's Progress
1996/97 MLC#19	Year 2000: Provide monthly status briefings to the Director of the FBI on the status of the Year 2000 project.	The FBI's February 1999 response to the recommendation stated that the FBI's Senior Official for Year 2000 regularly briefed the Deputy Director and provided monthly progress reports on all Year 2000 efforts. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#20	Strategic Planning: Develop and maintain an IT strategic plan that projects technology spending for a 3 to 5-year period.	The FBI's February 1999 response to the recommendation stated that the FBI completed a strategic plan during 1997 and 1998 and the FBI Strategic Plans will be updated annually. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.
1996/97 MLC#32	Network Encryption: Evaluate encryption alternatives to reduce the risk of compromising sensitive information.	The FBI's February 1999 response to the recommendation stated that the FBI is continuing to evaluate new security technologies as they evolve. This recommendation was closed by the OIG upon issuance of the final report based on a review of the corrective actions taken.

Source: OIG analyses as of April 2003

2. Recommendations on the FBI's FY 2001 GISRA Report

FY 2001 GISRA Report's Management Controls: Closed Recommendation

Recommendation	FBI's Progress
#1. Define and document all criticality levels used to classify applications.	The FBI's April 2002 response to the recommendation stated that all criticality factors had been articulated and documented. However, the OIG stated in the May 2002 GISRA report that the FBI should complete and update the criticality levels within the risk analysis of the System Security Authorization. In June 2002, the FBI provided the OIG's contractor with documentation evidencing the criticality levels of risk analyses within the System Security Authorization documents for the investigative and administrative systems. This documentation resulted in the OIG closing the recommendation in December 2002.
#4. Document a corrective action plan to address the vulnerabilities identified in the risk analysis for the investigative and administrative mainframe systems that describe how each of the recommended actions will be accomplished.	The FBI's April 2002 response to the recommendation stated that a detailed action plan had been created and disseminated to all affected components. The OIG closed this recommendation in April 2003 after receiving documentation from the FBI that demonstrated the corrective action plan to address the vulnerabilities identified in the risk analyses for the investigative and administrative mainframe systems.

Source: OIG analyses as of April 2003

FY 2001 GISRA Report's Management Controls: Open Recommendations

Recommendation	FBI's Progress
#2. Distribute, obtain, and maintain signed statements of end-users' acknowledgement of the Automated Information System Rules of Behavior for the investigative and administrative mainframe systems.	Although the FBI did not initially agree with this recommendation in their April 2002 response to the OIG's recommendation, the subsequent response dated June 2002 concurred with the recommendation and indicated that alternative corrective actions were in place. However, the documentation sent to the OIG in June 2002 did not provide adequate evidence to show employee acknowledgement of the Rules of Behavior. The provided documentation lacks signatures, proof of being an FBI document, and a means to determine that those employees who missed the mandatory training sessions received the Rules of Behavior. The OIG is requesting that all FBI users receive the proper training in regard to the rules of behavior and that it receive documentation demonstrating that FBI users receive training.
#3. Ensure the MIOG and other FBI security policies reflect the evolving systems environment and are enforced.	The FBI reported that a top to bottom review of existing FBI policy is underway and it is anticipated that the current MIOG policies and procedures will be substantially altered to conform to current standards. To close the recommendation, the FBI should provide the OIG with a copy of the updated procedures and evidence that the procedures are being enforced.
#5. Obtain a full accreditation for the investigative and administrative mainframe systems from the FBI's approving authority; a conditional accreditation should be unacceptable.	The FBI's responses to this recommendation stated that the OIG "requirement" for full accreditation of the administrative and investigative mainframes without conditions is not only unachievable in the current FBI environment, but outside of the OIG authority. The FBI further stated that the Designated Approving Authority (DAA) is the only official, besides the Principal Accrediting Authority, with the authority to "formally assume responsibility for operating a system at an acceptable level of risk." According to the FBI, the DAA has made the decision to permit the investigative and administrative mainframe systems to operate at their current level of risk for technical, management, and operational reasons. To resolve and close this recommendation, the FBI should provide the OIG with documentation evidencing that the DAA has accepted the inherent risk by signing the accreditation memorandum granting full accreditation to the investigative and administrative mainframe systems.

#6. Conduct annual refresher computer training for all employees.	The FBI's responses to this recommendation stated that it is working on an initiative that includes developing a variety of training awareness curricula for delivery to every employee. It also stated that the design and development of this effort is expected to continue through the calendar year and be ready for implementation at or near the start of 2003. Because the documentation the FBI submitted to the OIG in June 2002 was not complete with signatures, titles, dates and times, the recommendation remained open as of April 2003.

Source: OIG analyses as April 2003

FY 2001 GISRA Report's Operational Controls: Closed Recommendation

Recommendation	FBI's Progress
#7. Restrict access to all wiring closets.	The FBI's April 2002 and June 2002 responses to the recommendation stated that all wiring closets have appropriate locks in place and employees with access to these restricted areas have been reminded of required security. The OIG closed this recommendation in April 2003 after receiving documentation from the FBI that evidenced its reminder of required security to employees with access to restricted areas.
#10. Establish optimal operating system capacities and implement procedures to alleviate the near capacity usage.	The FBI's April 2002 response to the recommendation stated that in September 2001, a mainframe system update was performed to rectify the issue of system capacity at both Data Centers. Upon verification of the corrective actions by the OIG contractor, the recommendation was closed upon issuance of the final report.

Source: OIG analyses as of April 2003

FY 2001 GISRA Report's Operational Controls: Open Recommendation

Recommendation	FBI's Progress
#8. Document procedures for identifying and restoring mission-critical systems.	The FBI's April 2002 and June 2002 responses to the recommendation stated that the Data Center manuals have been updated as of June 14, 2001, to reflect proper procedures for restoring the FBI mission-critical systems on the investigative and administrative mainframes. In the FBI's response dated June 2002, the FBI included a copy of the updated procedures. However, the documentation does not provide instructions as to the order the in which systems should be restored. Because the documentation the FBI submitted to the OIG in June 2002 was not complete, the recommendation remained open as of April 2003.
#9. Complete the production test exercise involving the transfer of production operations and applications to the backup site and train Data Center staff for this contingency control.	The FBI's April 2002 response to the recommendation stated that backup and recovery procedures were tested for all investigative applications in January 2002 and were scheduled to be tested for administrative applications in October 2002. To close this recommendation, the FBI should provide documentation to the OIG demonstrating the successful completion of the administrative applications transfer test conducted in the spring of 2003.

Source: OIG analyses as of April 2003

FY 2001 GISRA Report's Technical Controls: Closed Recommendations

Recommendation	FBI's Progress
#12. Fully implement and use the System Access Request function to document user logon and verify that user access is commensurate with assigned responsibilities.	The FBI's April 2002 response to the recommendations stated that the Security Access Request function was implemented in April 2001 and that the 12 accounts mentioned in the finding were not processed through the System Access Request. Subsequent to this response, the FBI provided the OIG with documentation evidencing that the System Access Request function was fully implemented and being used to document user logon and verify that user access is commensurate with assigned responsibilities. This documentation resulted in the OIG closing the recommendation in December 2002.
#16. Ensure that the communication carrier signals are not connected to unencrypted network devices.	The FBI's April 2002 response to the recommendation stated that its Inspection Division verified that none of the identified modems were connected to the FBI network in August 2001. Upon verification of the corrective, the recommendation was closed upon issuance of the final report in May 2002.

Source: OIG analyses as of April 2003

FY 2001 GISRA Report's Technical Controls: Open Recommendations

Recommendation	FBI's Progress
#11. Implement and enforce DOJ password policies by re-setting and monitoring operating system settings accordingly.	The FBI's April 2002 response to the recommendation stated that limitations with Novell and Windows NT software prevented full compliance with DOJ directives. The OIG disagreed with the FBI's position and indicated that DOJ policies could be complied with through password masking. FBI officials subsequently stated that they have implemented the DOJ policy with respect to passwords, with the exception of one, password masking, which is not available to ensure a mix of alphabetic, numeric, and special characters. The OIG has obtained information from Novell and found that since 1999, Novell has provided an enhancement to the Novell Client software, which allows enforcement of a password policy using locally stored data to ensure a mix of alphabetic, numeric, and special characters. To close this recommendation, the FBI should implement a password policy to ensure a mix of alphabetic, numeric, and special characters and provide the OIG with a screen shot demonstrating that password setting have been implemented according to DOJ policy.
#13. Enforce DOJ security policies and ensure sufficient controls for FBI systems to operate so that authorized users have access to only the information they are entitled to.	The FBI's April 2002 response to the recommendation stated that controls are in place to limit a user's access to only the information he/she needs to perform his/her job and requested more information to further respond. The OIG stated in December 2002 that the FBI continued to disagree with this recommendation. However, the FBI has subsequently agreed that there were deficiencies with network accounts, and consequently initiated and completed a major effort to correct password deficiencies and ensure that password control options are set properly and enforced. In April 2003, the OIG stated that to close the recommendation, the FBI should provide documentation that identifies users with access to administrative and investigative systems as well as their roles and responsibilities. After reviewing this documentation, the OIG can determine if users have proper access to the systems and satisfy the terms to this recommendation.

#14. Require that system administrators periodically review and delete all system accounts that have been unused for more than 90 days.	The FBI's April 2002 response to the recommendation stated that no automated process existed on its local networks to assist system administrators with the function of periodically reviewing and deleting system accounts that have been unused for more than 90 days, but the process would be automated and centrally administered by the Enterprise Operations Center when Trilogy upgrades are completed in October 2002. In order to close this recommendation, the OIG requested the FBI to provide them with documentation evidencing that it is requiring system administrators to periodically review and delete all system accounts that have not been used for more than 90 days. In April 2003, the OIG informed the FBI that the updated status of this recommendation was pending and would be provided based upon the results of the FY 2003 financial statement audit of the FBI.
#15. Enable account lockout on all systems so that it occurs after three unsuccessful logon attempts.	The FBI's April 2002 response to the recommendation stated that account lockout settings have been set to comply with the DOJ's standards. In order to close this recommendation, the OIG requested the FBI to provide them with documentation (screen shots) evidencing that account lockout has been enabled on all systems so that it occurs after three unsuccessful logon attempts. Because the FBI's responses have not provided the OIG with appropriate documentation, the recommendation remained open as of April 2003.
#17. Enforce the use of the FBI's Service Center as a centralized approval point to track all change requests from initiation through final disposition.	The FBI's April 2002 response to the recommendation stated that the Service Center application is now the only approved method for recording system changes as a result of its February 2002 system upgrades. Subsequently, the FBI provided the OIG with documentation supporting that policies and procedures existed for the centralized approved change management process. However, the OIG stated in December 2002 that these polices were not being enforced. Although the OIG closed the recommendation in December 2002, in order to track its status with the GISRA FY 2002 review of the FBI's ACS system, we considered the recommendation to be open since the FBI could not demonstrate that policies were being enforced.
#18. Implement the format and content standards for information technology development and maintenance support test plans.	The FBI's April 2002 response to the recommendation stated that it created and implemented format and content standards for application development and modification by FY 2002. However, in the FBI's memorandum dated March 11, 2003, the FBI stated that it anticipates completion for the implementation of the format and content standards for information technology development and maintenance support test plans to be December 2003. In order to close this recommendation, the OIG requested the FBI to provide them with documentation evidencing that the format and content standards for IT development and maintenance support test plans are fully implemented.

#19. Update the Architecture Change Management Policy to reflect the FBI's current information application and system software environment.	The FBI's April 2002 response to the recommendation stated that the FBI did not concur with the recommendation as it was written. As a result, the recommendation was considered unresolved upon final report issuance in May 2002. The FBI's next response dated June 2002 stated that a FBI-wide Configuration Management (CM) policy was created and approved by the Chief Information Officer on October 1, 2001. The FBI has since acquired a contractor to assist them in complying with the FBI-wide Configuration Management (CM) policy. The new CM procedures have been developed and were to be validated in March 2003. Once validated, the FBI will develop a plan for implementing the procedures through the IRD. To close this recommendation, the FBI should provide the OIG with documentation demonstrating that the CM procedures as well as a copy of the developed plan for implementing the CM procedures.
#20. Document procedures to establish the supervisory review process of software change when deviations from normal procedures occur.	The FBI's April 2002 response to the recommendation stated that as of March 2002, a review board now meets every two weeks to ensure supervisory review and determine procedures for any deviations that may occur. In order to close this recommendation, the OIG requested the FBI to provide a copy of documented procedures for that process.
#21. Enable auditing to capture the necessary system information to comply with DOJ policy.	The FBI's April 2002 response to the recommendation stated that the auditing functions were enabled only on servers that met required processing and storage capacity to support those functions. The response further stated that as obsolete servers are being replaced, auditing functions are enabled on replacement servers and estimates a complete phase out of obsolete servers by July 2003. In order to close this recommendation, the OIG requested the FBI to provide documentation evidencing that auditing (or some other compensating control) is enabled on all servers to capture the necessary system information in order to comply with DOJ policy.

#22. Require that audit trail activity be reviewed regularly.	The FBI's April 2002 response to the recommendation stated that it is impractical to conduct regular reviews of audit trail activity for either all personnel or all information systems. As a result, the recommendation was considered unresolved upon final report issuance in May 2002. In December 2002, the OIG stated that FBI continued to indicate that it is impractical to conduct regular reviews of audit trail activity for either all personnel or all information systems. However, the FBI has since agreed that security audit is an essential part of system security. The Security Division is systematically addressing audit requirements for each FBI information system in the ongoing Certification and Accreditation effort. The Information Assurance Section has also begun the build-out of the Enterprise Security Operations Center (ESOC) that will have multiple security capabilities. To close this recommendation, the FBI should provide the OIG with documentation demonstrating that the initial and full operating capability of the ESOC upon completion.
#23. Apply manufacturer patches in a timely manner to prevent system compromise to all network operating systems.	The FBI's April 2002 response to the recommendation stated that in March 2002, manufacturer's patches were implemented as a required part of the change management process to ensure that changes do not result in negative impacts to applications and/or users. In order to close this recommendation, the OIG requested that the FBI provide documentation evidencing the corrective action taken. Because the FBI's responses have not provided the OIG with appropriate documentation, the recommendation remained open as of April 2003.

Source: OIG analyses as of April 2003

3. Recommendations on the FBI's Special Investigation Reports

Campaign Finance Investigation Report: Open Recommendations

Recommendation	FBI's Progress
IV.A (#9) The Manual of Administrative Operations and Procedures should be revised to require more comprehensive mandatory indexing of names appearing in an FBI document, and entry practices should be changed accordingly. Additionally, FBI policies should be changed to require that all documents be uploaded into the Electronic Case File database.	The FBI's July 1999 response to this recommendation stated that the FBI would establish a working group to revise the procedures governing the uploading of documents and indexing of names in the ACS system. However, the FBI's response dated August 2001, stated that the FBI did not establish a formal working group as originally intended but instead relied upon the Information Resources Division to work with other FBI divisions to improve the ACS system's procedures. The FBI's May 2003 response to this recommendation stated that the not all documents can be uploaded (into the Electronic Case File) due to certain sensitivities and restrictions. However, the FBI issued ECs in July 2000 and June 2002 that required ECs and e-mails to be uploaded into the ACS system, unless otherwise prohibited. Regarding the mandatory indexing of names, the FBI stated that the VCF will facilitate indexing on various web-based documents by providing data fields in searchable database tables. The index is created once the document is approved and serialized into the VCF. The index data can be searched using search screens or viewing the serialized document. Because the first release of the VCF is not scheduled for completion until December 2003, this recommendation remains open.

IV.B (#10) Supplementary training for agents who are principally responsible for the information that is entered into the ACS system should be performed.	The FBI's July 1999 response to this recommendation stated that the FBI was developing a program to provide agents with additional training on the ACS system once the new ACS system procedures are adopted. The FBI's August 2001 response stated that the IRD provided basic ACS system training in 1999 and 2000 to over 200 special agents and close to 1,000 new special agents, while close to 200 special agents received basic ACS system training in 2001. The FBI's May 2003 response stated that 43 veteran agents and 1,374 new agents were trained on the ACS system between August 2001 and May 2003. Additionally, the FBI's response stated web-based VCF training would be conducted between October 2003 and November 2003. To prepare for the VCF training, the FBI is assessing its employees' basic computer literacy skills. This assessment identifies employees in need of additional computer skills so that appropriate training can be taken prior to the VCF training. Because it is not clear whether the ACS training provided to veteran agents has been adequate and we were unable to assess the FBI's web-based training for the VCF (since it will not occur until October and November 2003), this recommendation remains open.
IV.C (#11) Agents should be made responsible for determining what information is entered into the IIIA system or for reviewing entries made by analysts to ensure their accuracy and completeness. Additionally, the FBI should consider increasing the number of IIIA system analysts, particularly in those field offices that generate significant amounts of foreign counter-intelligence information. Finally, when IIIA searches are performed, original IIIA system reports should be provided to the parties who requested the searches, rather than summary electronic communications.	The FBI's July 1999 response to this recommendation stated that the working group addressing the issues concerning ACS would also review the problems with the IIIA system identified by the recommendation. However, the FBI's response dated August 2001 stated that while the FBI did not establish a formal working group as originally intended, it did advise users of the IIIA system of new system enhancements, policies, and procedures through a newsletter. The response further stated that in 1999 and 2000: (1) additional training was provided to users of the IIIA system, and (2) several initiatives were undertaken to improve the accuracy of information in the IIIA system. Additionally, the response stated that Trilogy's new enterprise solution (VCF) would ultimately absorb the IIIA system (scheduled for deployment in June 2004. The FBI's May 2003 response to this recommendation stated that significant changes are planned for the IIIA system since the VCF development is not based on a system-by-system replacement, but rather a re-engineering of business practices and policies. The FBI is continuing to schedule and prioritize the functional components that must be integrated into the VCF for each delivery through June 2004. Because replacement of the IIIA system is planned as part of releases two and three of the VCF scheduled for June 2004, this recommendation remains open.

IV.D (#12) Any task force that is using the FBI's databases should obtain at least a fundamental appreciation for their operation.	The FBI's July 1999 response to this recommendation stated that appropriate training would be conducted whenever a relevant task force is created. The FBI's May 2003 response to this recommendation stated that the VCF training plan includes all Bureau task force members who will have access to the VCF application. Because the VCF training has not yet been completed, this recommendation remains open.

IV.E (#13) Ensure that the FBI's database operators are conversant with the format of Chinese and other foreign names. Additionally, database operators should inquire about whether the requesting party has in fact determined the order of such names, and if in doubt, should always perform an "around the clock" search.	The FBI's July 1999 response to this recommendation stated that the working group addressing the issues concerning the ACS system would also review ways of improving the process of entering and retrieving foreign names in FBI databases. However, the FBI's response dated August 2001, stated that while the FBI did not establish a formal working group as originally intended, it did make enhancements to the IIIA system in July 2000 so that variations of a name are identified during a search. The FBI's May 2003 response to this recommendation stated that on May 3, 2002, the LTAU announced in an EC a project to adopt and implement standards for the uniform "Romanization" of foreign personal and place names. Additionally, in an EC dated May 8, 2002, the LTAU began work on implementing standardization systems for "Romanizing" Arabic by offering training to all applicable FBI employees. According to the FBI, by the end of the second quarter of FY 2003, 371 FBI employees had received training in Arabic "Romanization," while classes continue to be held. Regarding Chinese "Romanization," the LTAU announced in an EC dated September 12, 2002, that training on Chinese "Romanization" was being offered to all applicable FBI employees. As of June 9, 2003, a total of 80 FBI employees had been trained in Chinese "Romanization" while classed continue to be held. The FBI's May 2003 response to this recommendation also stated that the FBI selected a commercial-off-the-shelf application for searching names. The software will search names entered in any order and will create different permutations of ordering. The software will not only search the different orders of names, but also will have algorithms to detect common or likely misspellings, sound-a-likes, and cultural differences. Additionally, the LTAU worked with the VCF project management team to create a keyboard for the "Romanization" of names in accordance with the U.S. Board on Geographic Names. In addition to training, the FBI expects the VCF to help database operators apply foreign names to searches within databases. For example, the VCF will allow the addition of STC for Asian names, Unicoded for other foreign names, and it will deploy a name search engine that incorporates variations on names. Because the first release of the VCF is not scheduled for completion until December 2003, this recommendation remains open.

Source: OIG analyses as of May 2003

McVeigh Report: Closed Recommendations

#8. The FBI should evaluate its computer training in order to develop a clear understanding of what agents need to perform their jobs effectively.	The FBI's September 2002 response to this recommendation stated that training was being assessed by a curriculum review committee. The FBI's April 2003 response to this recommendation stated that the Training Division completed the design of instruments currently being used by new agents and managers to assess what computer skills agents need to perform their jobs and to determine the need for additional improvements to the new agents' computer training curriculum. These instruments, which will evaluate whether the Training Division's computer training program is meeting the needs of field offices and investigators, are in the process of being tested. Based on a review of supporting documentation provided by the FBI, we believe that the FBI has adequately addressed this recommendation.
#9. The FBI should consider whether computer usage should be a part of the core skills needed to graduate from the new agents training academy.	The FBI's September 2002 response to this recommendation stated that the Training Division intends to implement policy requiring all new agents to possess core computer competency skills prior to graduation. The FBI's April 2003 response to this recommendation stated that the Training Division determined that computer training should be a core requirement for graduation from the FBI Academy. Accordingly, the Training Division has implemented a policy requiring all new agents to pass an exam on core computer competency skills prior to graduation. Based on a review of supporting documentation provided by the FBI, we believe that the FBI has adequately addressed this recommendation.
#10. The FBI should consider mandatory refresher training for veteran agents.	The FBI's September 2002 response to this recommendation stated that the Training Division works to encourage the use of investigative computer training for veteran agents. The FBI's April 2003 response to this recommendation stated that the FBI has recently implemented a program of continual mandatory training for veteran agents, and all employees (including the FBI's cadre of intelligence analysts). This mandatory training will include investigative computer training. Based on a review of supporting documentation provided by the FBI, we believe that the FBI has adequately addressed this recommendation.

#13. The FBI should ensure that deadlines for the completion of leads is clear and not undermined by the automated system, such as the ACS system's setting of a 60-day deadline for "immediate" leads.	The FBI's September 2002 response to this recommendation stated that the deadlines set within the ACS system for completing "Immediate" and "Priority" leads would be changed to one day by December 31, 2002. The current procedures for specifying deadlines for routine matters will remain unchanged. The FBI's April 2003 response to this recommendation stated these changes to the ACS system were completed by August 26, 2002. Based on a review of supporting documentation provided by the FBI, we believe that the FBI has adequately addressed this recommendation.

Source: OIG analyses as of April 2003

McVeigh Report: Open Recommendations

Recommendation	FBI's Progress
#1. The FBI should foster an attitude among all employees that information management is an essential part of the FBI's mission and that automation is a key tool in managing the storage, analysis, and retrieval of information.	The FBI's September 2002 response to this recommendation stated that the FBI was engaging in programs to improve all of its records management capabilities through its restructuring and creation of the RMD. The FBI undertook training of all employees in the areas of information management requirements, procedures, and responsibilities during a 1-day stand down in 2001. Further, the FBI's response stated that future training in records management was being planned. The FBI's April 2003 response to this recommendation stated that the RMD was actively promoting effective information management within the Bureau and was encouraging acceptance of new automation plans by Bureau employees. Since 2002, RMD staff has worked closely with the VCF and SCOPE data warehouse program teams to ensure close coordination of records and information management activities. Additionally, the response stated that the RMD has begun to identify, develop, and implement the quality control mechanisms to ensure that record systems' problems are quickly detected. Also, the RMD is investigating the possibility of establishing an annual awareness campaign. Further, the RMD will establish a Records Management publicity team. Because the RMD's activities are ongoing and the first release of the VCF – which will significantly change the FBI's information and workflow process – is not scheduled for completion until December 2003, this recommendation remains open.
#2. As part of its development of Trilogy, the FBI should consider whether its document management systems can be simplified, such as by having supervisors review electronic copies of documents, and whether its record keeping formats can be reduced in number.	The FBI's September 2002 response to this recommendation stated that the FBI was pursuing the simplification of its document management systems through the development of Trilogy and the VCF. The FBI's April 2003 response to this recommendation stated that the RMD has taken part in the process to simplify the FBI's document information systems through the implementation of the new electronic record keeping system. The VCF system is designed to develop a workflow process that will allow for electronic signatures. The response further stated that it is the responsibility of the VCF to work with the FBI Public Key Infrastructure Team to implement electronic signatures for the approval process. Because the first release of the VCF is not scheduled for completion until December 2003, this recommendation remains open.

#3. The FBI should evaluate whether inserts should be eliminated.	The FBI's September 2002 response to this recommendation stated that inserts would be eliminated with the deployment of the VCF. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.
#4. The FBI should evaluate its practices regarding "originals" of FBI created documents (such as FD-302s). If originals continue to be needed, the FBI should develop a system that more clearly identifies an original.	The FBI's September 2002 response to this recommendation stated that the FBI was examining how "originals" would be managed in the future, within the VCF applications. The FBI's April 2003 response to this recommendation stated the FBI has determined that electronic versions of records in VCF are the "record copies" as part of the Public Key Infrastructure/VCF – Record Management Application (RMA) development. Approval of the requirements for a Public Key Infrastructure was obtained in February 2003. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.
#5. Any new automation system should be user friendly, meaning that the steps required to obtain information should be few in number and intuitive. Information should be provided to the user quickly.	The FBI's September 2002 response to this recommendation stated that the VCF will be in a web-environment, familiar to computer users with simplified workflow processes for document storage and retrieval. In the VCF, basic workflow processes will be accomplished through point and click capabilities. The submission of a document or package to a case file for routing and approval will be accomplished through a single "submit action." Once properly stored, every case and document will be immediately available to all persons who have proper security access through a web-based point and click environment. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.
#6. Any new automation system should include an effective document tracking system. The FBI should consider whether a system that integrates the creation of documents into the tracking system is feasible and appropriate.	The FBI's September 2002 response to this recommendation stated that the development (through Trilogy) of comprehensive automated document creation, receipt, and management systems will eliminate much of the need for traditional document tracking systems. FBI employees will be able to access documents directly from their desktop computers, whether those documents were created by the FBI or received from external sources and scanned into the Trilogy systems. The FBI's April 2003 response to this recommendation stated that with the implementation of VCF, systems and processes will be established to effectively track documents and materials contained in the FBI records systems. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.

#7. The FBI should work toward eliminating crisis management software and other independent systems. The FBI should consider the feasibility of developing an automation system that expands to meet situations rather than developing new software that is compatible with other programs.	The FBI's September 2002 response to this recommendation stated that the focus of the VCF project has been to develop a user-friendly case management and program management tool that attempts to integrate the workflow involved in the recording of events and data with the natural flow of the investigation. The response further states that the information intake process for a crisis response should be the same as intake for routine matters. The VCF project has defined the FBI's case and program management needs and requirements to include crisis management as a component of the workflow and case management. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.
#11. The FBI should ensure that leads cannot be "covered" without an explanation of what has been done to the task assigned.	The FBI's September 2002 response to this recommendation stated that the VCF is being designed so as to permit leads to be "covered" as a separate function from the documentation of the lead being covered. The FBI's April 2003 response to this recommendation stated that in January 2002, the process to identify the VCF program requirements to ensure that leads cannot be "marked covered without an explanation of the action taken" was begun. That phase of the process was completed on November 22, 2002, with the delivery of the program requirements to the VCF contractor. The contractor is to complete the design and implementation phase of the process by July 17, 2003. Upon completion of the design and implementation phase, testing of the VCF system, including the "lead coverage requirement" will begin and is to be completed on October 27, 2003. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.
#12. Future automation systems should incorporate a system to allow supervisors to easily track the status of leads. The FBI should evaluate whether a lead tickler system is appropriate and feasible.	The FBI's September 2002 response to this recommendation stated that VCF will assign unique lead "counters" to each lead in a single case. Split leads or leads created from an original lead will reflect lead counters with a derivative or "parent-child relationship" which will facilitate the tracing of all leads to their origin. The response further states that leads will be capable of being viewed from the desktop computer by the lead originating office and by all receiving offices to determine to whom the leads are assigned or whether action on the lead has occurred. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.

#14. The FBI should evaluate the feasibility of developing a system of universal lead numbers to eliminate the use of local lead numbers as a tracking mechanism.	The FBI's September 2002 response to this recommendation stated that the VCF system of universal lead counters unique to each case will facilitate lead creation, tracking, and action. The system for lead control will provide case agents and managers with a user-friendly tool to ensure lead accountability. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.
#15. The FBI should evaluate the use of lead numbers on leads and responding reports and determine whether new policies, better enforcement of existing policies, improved training, or better automation is the best method of fixing the problem.	The FBI's September 2002 response to this recommendation stated that the VCF system of universal lead counters unique to each case will facilitate lead creation, tracking, and action. The system for lead control will provide case agents and managers with a user-friendly tool to ensure lead accountability. Because the first release of the VCF is not scheduled for delivery until December 2003, this recommendation remains open.

Source: OIG analyses as of April 2003

OTHER REPORTS RELATING TO THE FBI'S IT PROGRAM

1. GAO Reports

The GAO is the investigative arm of Congress. The GAO examines the use of public funds, evaluates federal programs and activities, and provides analyses, options, recommendations, and other assistance to help Congress make effective oversight, policy, and funding decisions. Since 1998, the GAO has issued several reports and related testimony that highlight deficiencies with the FBI's IT, including one report that provides an IT recommendation.

According to the "GAO's Agency Protocols," issued in December 2002, the GAO's recommendations are intended to improve the economy, efficiency, and effectiveness of an agency's operations and to improve the accountability of the federal government for the benefit of the American people. Consequently, the GAO monitors agencies' progress in implementing these recommendations. To accomplish this monitoring, the GAO maintains a database of open recommendations. As new reports with recommendations are issued, their recommendations are incorporated into the database. This database serves both the GAO and the agencies by helping them meet their record maintenance and monitoring responsibilities.

The GAO's goal is to remove all closed recommendations from the database on an ongoing basis. However, toward the end of each fiscal year, special attention is directed to this effort. The GAO removes a recommendation from its database after determining that (1) the agency has implemented the recommendation or has taken action that in substance meets the intent of the recommendation, or (2) circumstances have changed and the recommendation is no longer relevant. The open recommendation database is available to the public on the GAO's website (www.gao.gov). Specific recommendations can be identified because the database is searchable by agency, Congressional committee, and key words. Congressional oversight and authorization committees, as well as the Appropriations Committees, can use the database to prepare for hearings and budget deliberations.

Additionally, when the GAO issues a report containing recommendations to the head of an agency, 31 U.S.C. Section 720 requires that the agency head submit a written statement of the actions taken by the agency on the GAO's recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Reform no later than 60 days after the date of the report. The agency's statement of action is also to be submitted to the House and Senate Committees on

Appropriations with the first request for appropriations that is submitted more than 60 days after the date of the report. If the Congressional requestor has asked that the distribution of the report be restricted, as provided by the "GAO's Congressional Protocols," the 60-day period will begin on the date the report is released.

Because agency personnel serve as the primary source of information on the status of recommendations, the GAO requests that the agency also provide it with a copy of the agency's statement of action to serve as preliminary information on the status of recommendations. The GAO will follow up by discussing the status of recommendations with cognizant agency officials; obtaining copies of agency documents supporting the recommendations' implementation; and performing sufficient work to verify that the recommended actions are being taken and, to the extent possible, that the desired results are being achieved.

While conducting an audit on the FBI's counterterrorism program,[54] the OIG found that the FBI had not implemented a GAO recommendation in its report entitled, "Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks." Among the reasons identified by the OIG was that the FBI does not have a system of management controls to ensure timely implementation of GAO, OIG, or other agency issued recommendations. Because of the FBI's non-compliance with this GAO recommendation, we examined whether the FBI has implemented recommendations relating to IT that have been issued by the GAO in the last five years.

To assess the FBI's progress in implementing recommendations directed toward improving its information technology, we examined the following GAO reports that discussed the FBI's use and management of information technology:

- the 2000 report on the FBI's National Instant Criminal Background Check System (NICS);
- the 2000 report on the DOJ's Campaign Finance Task Force; and
- the 2002 Enterprise Architecture Report.

[54] The OIG report, entitled "A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management," was issued in September 2002.

Based on our review of these reports, only the report on the NICS had a recommendation that related to IT. We found that the FBI timely implemented this recommendation. Because the remaining two reports included some discussion of the FBI's IT program, we summarized the reports' findings to supplement our analyses of the FBI's progress in improving its IT.

A. Report on the FBI's National Instant Criminal Background Check System

In February 2000 GAO issued "Gun Control: Implementation of the National Instant Criminal Background Check System." The National Instant Criminal Background Check System is a computer system maintained by the FBI that is designed to provide background screening for all types of firearms bought from federal firearms licensees. In this report, the GAO:

- provided statistics on background checks, denials, and appeals;
- described enforcement actions taken against persons who allegedly falsify their status on firearm-purchase applications;
- discussed the NICS's computer system architecture, capacity management system availability, transaction response time, retention of records, monitoring activities, and the prospect of making the NICS a fingerprint-based system rather than a name-based system; and
- discussed pawnshop issues.

The report stated that the FBI did not authorize NICS before it began operations on November 30, 1998. System authorization was not obtained, according to FBI officials, due to insufficient time and resources to formally test security controls between the date that the FBI received the system from the contractor and the Congressionally-mandated date for system operation. However, while a formal test of security controls was not conducted, the security officer responsible for NICS' authorization stated that a subset of NICS' security requirements was assessed and a number of vulnerabilities were disclosed. The FBI requested an interim approval to operate NICS from the FBI's National Security Division, which is the FBI's authorization authority. According to an FBI National Security Division representative, the interim approval was granted for one year beginning November 30, 1998.

However, the GAO's report stated that, according to the security officer responsible for NICS authorization, all authorization requirements — such as certification testing — were not completed during the interim period because of competing priorities, such as the authorization of NCIC 2000 and the Integrated Automated Fingerprint Identification System. Additionally, the GAO's report stated that according to the DOJ, the completion of security testing was overshadowed by more urgent issues directly impacting NICS' ability to function; therefore, security testing was delayed. On December 2, 1999, the National Security Division extended the interim approval to operate NICS through April 2000. Further, the GAO's report stated that according to the security officer, security testing for NICS was completed on December 21, 1999. The FBI planned to obtain full authorization by March 31, 2000.

The report further stated that because of the system vulnerabilities that were identified before NICS went operational and the delays experienced in authorizing the system, the FBI continued to lack an adequate basis for knowing whether NICS assets (hardware, software, and data) were sufficiently secure and were not vulnerable to corruption and unauthorized access. Additionally, it had not yet been authorized as secure in accordance with the DOJ's own requirements, and attempts to do so had been delayed. The report also stated that further delays in authorizing NICS would expose the system and the data it processes about individuals to unnecessary risk. Therefore, it was extremely important that the FBI fulfill its commitment to authorize NICS by March 31, 2000.

We determined that the FBI timely implemented the report's one IT-related recommendation. This recommendation pertained to the certification and accreditation of the NICS by March 31, 2000. According to the GAO's website, the recommendation's status was closed.

To confirm that the status of this recommendation was closed, we interviewed FBI officials and reviewed documentation supporting the authorization and accreditation of the NICS as of March 31, 2000.

B. Report on the DOJ's Campaign Finance Task Force

In May 2000, the GAO issued a report entitled, "Campaign Finance Task Force: Problems and Disagreements Initially Hampered Justice's Investigation." The objective of this review was to examine the management and oversight, operations, and results of the Campaign Finance Task Force from its inception through December 31, 1999.

Among its findings, the report stated that the FBI lacked an adequate information system that could manage and interrelate the evidence that had been gathered in relation to the Campaign Task Force's investigations. Specifically, the Campaign Finance Task Force was overwhelmed with documents and other evidence and lacked sufficient staff and electronic system resources to input and organize the information being gathered. The report also stated that the lead investigator noted that after several months, the large volume of documents obtained overwhelmed the Campaign Finance Task Force's electronic data management system and a new system had to be purchased.

This report did not contain any FBI IT-related recommendations. However, the deficiencies described in this report are consistent with ones reported by the OIG. The more recently issued McVeigh and ITIM reports stated that similar vulnerabilities with the FBI's information management systems have continued, demonstrating that additional corrective actions are necessary.

C. Report on the FBI's Enterprise Architecture

In February 2002, the GAO issued a report entitled, "Enterprise Architecture Use Across the Federal Government Can Be Improved." The objectives of the report were to determine (1) the status of federal agencies' efforts to develop, implement, and maintain enterprise architectures; and (2) OMB's actions to oversee these efforts.

The report stated 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.

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.

This report did not contain any FBI IT-related recommendations. However, the recently issued ITIM report stated that the FBI still has not

fully established an enterprise architecture, although progress is being made. Specifically, a baseline architecture was being developed in a data repository, which ultimately will be maintained in the FBI's intranet. This data repository, when complete, is intended to describe how all of the FBI's IT systems align with the business processes of the Bureau. Additionally, the enterprise architecture office was developing a technical reference model that will outline the technical architecture of the Bureau's IT systems. Also, the FBI was 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 progress being made, the ITIM report ultimately concluded that the FBI's enterprise architecture development was not far enough along to adequately support the FBI's IT investment management activities.

D. Summary of GAO Reports

The three GAO reports we examined noted deficiencies with certain aspects of the FBI's IT program. The Gun Control report stated that the FBI did not properly authorize an IT system (NICS) through accreditation and certification. However, we found that the system was subsequently certified and accredited as of March 31, 2000. Additionally, the report on the FBI's Campaign Finance Task Force stated that the FBI lacked an adequate information system that could manage and interrelate the evidence that had been gathered in relation to the Campaign Task Force's investigations. These deficiencies were similar to those reported by the OIG Campaign Finance report. Further, the report on the FBI's enterprise architecture stated that the Bureau lacked a foundation for managing enterprise architecture. The recently released ITIM report reiterated the importance of having an established enterprise architecture when developing an IT investment management process.

2. Other Reports on the FBI's IT

In addition to the OIG and the GAO, other entities have issued reports in recent years that included analyses of the FBI's IT management. One report of particular relevance to IT security was issued by the Webster Commission. This report entitled, "A Review of FBI Security Programs" was issued in March 2002. This Commission, chaired by former FBI Director William H. Webster, was established to investigate the espionage of FBI Supervisory Special Agent Robert Hanssen.

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 protection of classified information.

- 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 had been deficient. It had 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 Webster Commission's report, these findings resulted from the FBI's lack of attention to IT security in developing and managing computer systems. The report highlights the importance of computer security as it shows how breaches, such as those that GISRA audits continue to identify, present national security risks.

APPENDIX 4

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

ACID	Top Secret Accessor Identification
ACM	Architecture Change Management
ACS	Automated Case Support
ADP	Automated Data Processing
ADPT	Automated Data Processing and Telecommunications
ARCS	Automated Response and Compliance System
BPMS	Bureau Personnel Management System
C&A	Certification and Accreditation
CM	Configuration Management
CONOP	Concept of Operations Report
COOP	Continuity of Operations Report
DAA	Designated Approving Authority
DOJ	Department of Justice
EC	Electronic Communication
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FMS	Financial Management System
FPDS	Federal Procurement Data Statistics
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
IIIA	Integrated Intelligence Information Application
IPC	Information Presentation Component
IRD	Information Resources Division
IT	Information Technology
ITIM	Information Technology Investment Management
LAN	Local Area Network
LTAU	Language Training and Assessment Unit
MAOP	Manual of Administrative Operations and Procedures
MIOG	Manual of Investigative Operations and Guidelines
MLC	Management Letter Comment
MW	Material Weakness
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General

OMB	Office of Management and Budget
PMA	Property Management Application
QCMU	Quality Configuration and Methods Unit
RC	Reportable Condition
RMA	Record Management Application
RMD	Records Management Division
SCI	Sensitive Compartmented Information
SMF	System Management Facility
SPIU	Systems Programming and Integration Unit
STC	Standard Telegraphic Code
Task Force	Campaign Finance Task Force
TNC	Transportation Network Component
UAC	User Application Component
VCF	Virtual Case File
WAN	Wide Area Network

FBI'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

September 22, 2003

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 August 21, 2003, 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 Implementation of Information Technology Recommendations." This memorandum requested that the FBI review and provide written comments regarding report recommendations. Specifically, you requested that the FBI comment on its agreement or disagreement with each of the recommendations. You also requested that the FBI identify steps taken or are planned to achieve corrective action and to include the dates of implementation.

Attached is the FBI's written response. Please note that the format of the document identifies the specific DOJ recommendations followed by the responses of the FBI Executive Management. Additionally, a sensitivity review is being conducted per your request and the results will be forwarded to you under separate cover.

The responses set forth in the attached were coordinated through the FBI's Inspection Division. If you have any questions, please contact either me, on 202-324-2901, or Kevin L. Perkins on 202-324-2903.

Sincerely yours,

S C McCraw

Steven C. McCraw
Assistant Director
Inspection Division

Enclosure

FBI Response
to
DOJ OIG Draft Audit Report
Federal Bureau of Investigations's
Implementation of Information Technology Recommendations

Recommendation Number 1, Page 74: We recommend that the Director of the FBI: Develop, document, and implement Bureau-wide procedures to follow-up and close audit and investigative recommendations, in accordance with OMB Circular A-50 and DOJ Order 2900.6A. This process should include the tracking and resolution of system audit recommendations.

Response: The FBI agrees with this recommendation. On 07/11/2003, OIG and GAO guidance was promulgated Bureau-wide. See attached Electronic Communications entitled "DOJ OIG Financial and Non-Financial Audits" and "General Accounting Office," Tabs A and B. These documents have also been posted on the Inspection Division website. Additionally, the MPMOU has spoken with the FBIHQ Manuals Desk on the feasibility of including these guidance documents into a planned centralized database of FBI policies, procedures, and processes. These documents will be reviewed on a semiannual basis and updated accordingly to accommodate any changes. The next review is scheduled for December 2003.

Recommendation Number 2, Page 74: We recommend that the Director of the FBI: Ensure that the ARCS database is complete and includes recommendations from all sources of OIG audits and reviews.

Response: The FBI agrees with this recommendation. The transition strategy for migrating audit information into ARCS addresses both new as well as prior year audits. All new (FY 2003 and subsequent) audits will be entered into ARCS. The strategy for entering open prior year audits is twofold. Known prior year open audits will be entered into ARCS immediately while unknown open prior year audits, those that may have slipped through the cracks due to inefficiencies in prior methods used to track audit compliance, will be entered when a formal response request is received from the OIG. Prior year closed audits will not be entered into ARCS. Since implementation of this strategy, 113 audits have been entered into and are being or have been tracked/monitored using ARCS.

The FBI has taken and will continue to take proactive steps to ensure the ARCS database is accurate and complete. First, all INSD Audit Liaison POC's were requested to search their records to identify open prior year audits. Audits that were identified but not in ARCS were immediately entered into ARCS. Also, the FBI recently performed a reconciliation of the ARCS database with the audit/inspection activities identified in the "Audit Highlights for the U.S. Department of Justice" Newsletter, dated May-June 2003 (Tabs C). The newsletter is published by the DOJ, Justice Management Division (JMD), Audit Liaison Office (ALO). The reconciliation was conducted to assess whether or not the ARCS database was current, accurate, and complete. The DOJ "Status of Current General Account Office Activities" and "Status of

Current Office of Inspector General Internal Activities" listed in the newsletter were matched to the ARCS database. The reconciliation identified only two findings. First, all of the OIG and with the exception of two GAO audits/reviews listed in the newsletter were in ARCS. In regards to the two GAO audits that were not in ARCS, further investigation determined that DOJ initially identified the FBI as a component in which the audits were applicable, then DOJ verbally informed the FBI that they were not. Regardless, they have since been entered into ARCS, documenting the initial identification of the FBI as a component and the subsequent rescissions. The reconciliation also noted that the audit status reporting in the newsletter did not account for audits that are resolved but have open recommendations. However, with the recent dissemination of DOJ, JMD, ALO guidance entitled "Process to Monitor and Oversee the Implementation of Audit Recommendations," we believe this finding will ultimately be resolved.

With the exception of one report (Campaign Finance), all of the OIG audits/investigations identified in Appendix 2 of the draft audit report are being monitored and tracked using ARCS. In regards to the report that is not in ARCS, the FBI has contacted the report issuing entity to request a copy of the audit report and associated correspondence. Upon receipt of the report, it will be entered into ARCS and tracked accordingly. The GAO reports sited in Appendix 3 of the draft audit report are not in ARCS due to their closure prior to the implementation of ARCS.

In regards to the statement that ARCS "does not include vulnerabilities generated by system audits required by GISRA," ARCS was not designed to track these types of internal audits. Systems audits, referred to as certification and accreditation (C&A), fall under the purview of the FBI's Information Assurance Section (IAS) (Tab D). ISA is mandated by policy to maintain all C&A information. IAS is in the process of establishing a database to maintain all information associated with the outcome of the C&A process of which system deficiencies/vulnerabilities would be a subset of the information collected. An award of a contract to develop the IAS database is imminent. Initial operational capability is anticipated within 3-4 months after the contract is awarded. It should be noted that IAS's action to establish and implement a C&A database is being tracked in ARCS in response to a recommendation contained in OIG Audit Report 03-06 (ARCS 03-03). ARCS will document and track all OIG GISRA audit findings and recommendations until closure. The three reports issued for FYs 2001 and 2002 specific to the FBI compliance with GISRA mentioned in the draft audit report have been entered into and are being tracked/monitored using ARCS.

Recommendation Number 3, Page 74: We recommend that the Director of the FBI: Ensure that managers are held accountable for the tracking, resolution, and timely implementation of OIG recommendations.

Response: The FBI agrees with this recommendation. In accordance with FBI guidance (see response to recommendation number 1), various individuals (i.e., managers and non-managers) are held accountable for the tracking, resolution, and timely implementation of OIG recommendations. An executive owner, a recommendation contact lead as well as compliance action/task points of contact is identified for each audit recommendation. Each have varying

degrees of accountability for the tracking, resolution, and timely implementation of OIG recommendations. Executive owners have overall accountability for the timely implementation of audit recommendations. They must review, approve, and oversee the corrective action plan associated with each audit recommendation as well as allocate the necessary resources to execute the corrective action plans. The recommendation contact lead must develop, manage, and execute the corrective action plan associated with a specific recommendation. The action/task point of contact is responsible for the execution of a specific action or task associated with a recommendation corrective action plan. ARCS is designed to record, track, and monitor audit information including management accountability for the tracking, resolution, and timely implementation of OIG recommendations. As noted in the draft audit report, weekly email notifications are issued when tasks are past due or approaching their due date. This control mechanism ensures that the appropriate individual is held accountable for the timely execution of recommendation corrective action plans.

OIG, AUDIT DIVISION ANALYSES AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

In its response to the draft report, the FBI agreed with all of our audit recommendations and provided over 25 pages of additional support to address the recommendations. Because of the length of the additional support provided, we include as Appendix 5 of this final report only the FBI's summary response.

Recommendation number:

1. Resolved. This recommendation is resolved based on the FBI's agreement to develop, document, and implement Bureau-wide procedures to follow-up and close audit and investigative recommendations. The documentation provided by the FBI included two electronic communications that provided guidance for the follow-up of OIG and GAO audits. However, it is not clear as to whether this guidance has been institutionalized as policy through inclusion within the FBI's formal policy manuals. This recommendation can be closed when we receive documentation demonstrating that the guidance documents provided, "DOJ OIG Financial and Non-Financial Audits" and "General Accounting Office," or other specific audit follow-up procedures are institutionalized as policy within the FBI's formal policy manuals.

2. Resolved. This recommendation is resolved based on the FBI's agreement to ensure that the ARCS database is complete. This recommendation can be closed when we receive documentation demonstrating that the Campaign Finance report has been entered into ARCS, and that vulnerabilities generated by system audits required by GISRA are being tracked.

3. Resolved. This recommendation is resolved based on the FBI's agreement to ensure that managers are held accountable for the tracking, resolution, and timely implementation of OIG recommendations. As stated for recommendation 1, the documentation provided does not appear to be institutional policy. This recommendation can be closed when we receive documentation demonstrating that the guidance documents provided, or other specific audit follow-up procedures, are institutionalized as policy within the FBI's formal policy manuals, and that the ARCS database is complete.