

1. Counterterrorism: The highest priority of the Department of Justice (Department) continues to be its efforts to deter, prevent, and detect future terrorist acts. Given the importance of this ongoing challenge, a significant amount of the Office of the Inspector General's (OIG) oversight efforts in the 4 years since September 11, 2001, have focused on Department programs and operations related to counterterrorism and national security issues. While a series of OIG reviews issued during the past year identified areas in need of improvement, we believe the Department continues to make progress in addressing this preeminent challenge.

Much of the OIG's oversight work related to counterterrorism involves the Federal Bureau of Investigation (FBI). Since the September 11 terrorist attacks, the FBI has made a concerted effort to transform itself from a traditional law enforcement agency that investigates crimes after they have been committed to a more proactive agency that seeks to prevent terrorist acts. To gauge the FBI's success at making this transition, the OIG has completed three reviews over the past 2 years that have examined the FBI's reallocation of resources from traditional criminal investigations to counterterrorism and counterintelligence matters.

The most recent OIG report on this subject, completed in late September 2005, showed that between fiscal years (FY) 2000 and 2004 the FBI formally reallocated 1,143 field agent positions away from investigating traditional criminal matters and placed these resources primarily in terrorism-related programs. In addition to the formal reallocation of positions, we found that the FBI actually utilized almost 2,200 fewer field agents to investigate traditional criminal matters, such as bank robbery and drug crimes, in FY 2004 than it had in FY 2000. According to senior FBI officials, the additional agents were diverted from criminal investigative areas to terrorism-related matters as needs arose. For example, FBI field offices were directed to ensure that no terrorism-related matter went unaddressed, which primarily contributed to the significant gap in the utilization and allocation figures in FBI criminal investigations.

Also during the past year, the OIG examined the work of the Department's counterterrorism task forces; the FBI's recruitment and training of intelligence analysts; the FBI's information technology (IT) initiatives such as the Trilogy Project, its failed Virtual Case File effort, and its ongoing effort on a replacement case management system called Sentinel; the FBI's management of the Terrorist Screening Center (TSC); and the TSC's efforts to support the Transportation Security Administration's Secure Flight program. We discuss several of these reviews in this section, as well as in other sections of this document where they relate to different management challenges.

In June 2005, the OIG released a report that evaluated the operations of five Department counterterrorism task forces and advisory councils that were either created or expanded after the September 11 terrorist attacks. The OIG review assessed the role and operations of these task forces and councils – whether they were achieving their purposes, and whether gaps, duplication, or overlap existed in the groups' counterterrorism coverage. The five groups examined in the OIG review were the Joint Terrorism Task Forces (led by FBI field offices with participation by other Department of Justice, federal, State, and local law enforcement agencies) which seek to prevent terrorist incidents and investigate terrorism threats); National Joint Terrorism Task Force (led by the FBI) which provides administrative, logistical, and training support to the Joint Terrorism Task Forces; Anti-Terrorism Advisory Councils (led by U.S. Attorneys) which aid the exchange of terrorism-related information among federal, State, and local organizations in the public and private sectors; National Security Coordination Council (led by the Deputy Attorney General and composed of senior Department officials) which defines and coordinates the Department's counterterrorism strategy; and the Foreign Terrorist Tracking Task Force (led by the FBI) which provides data to task forces and other government agencies to help prevent terrorists from entering the United States, locates terrorists who have entered the country, and assists in terrorism investigations.

In sum, the OIG review concluded that the terrorism task forces and advisory councils generally function as intended, without significant duplication of effort, and that they contribute significantly to the Department's counterterrorism efforts. Specifically, we found that the Department's terrorism task forces and advisory councils improved information sharing among law enforcement agencies, the intelligence community, and private industry by broadening the pool of individuals with security clearances and providing forums for information exchange about terrorism matters.

However, the OIG review also identified a series of management and resource issues affecting the operation of the task forces and advisory councils. Those problems included the need for more stable leadership among the task forces and councils, better training for participants, increased attention to the Foreign Terrorist Tracking Task Force, greater involvement in the task forces by the Drug Enforcement Administration (DEA), additional resources, and increased coverage of remote areas. The OIG report provided 28 recommendations to help the Department improve the operations of its various counterterrorism task forces and councils. The Department concurred with all 28 recommendations.

Other OIG reviews have identified additional areas in need of significant improvement in order for the Department to most effectively meet its counterterrorism responsibilities. For example, in several reviews, the OIG has reported on the urgent need to upgrade the FBI's IT systems. In essence, the FBI is in the business of uncovering, analyzing, sharing, and acting on information. To do so effectively and fully, it must have state-of-the-art IT and case management systems. But the FBI's current IT systems fall far short of what is needed, and its efforts to create a modern case management system to catalogue, retrieve, and share case information have not succeeded. The successful upgrade of the FBI's IT systems – as well as the development and integration of other important IT systems throughout the Department – remains one of the top challenges facing the Department in the years ahead. This issue is discussed in more detail in this document under Challenge 4.

In addition, to effectively meet its counterterrorism mission the FBI must value and support to a greater degree staff with technical skills. For example, until recently the FBI did not adequately value the contributions of intelligence analysts. The FBI's historic view was that its special agents performed the key work of the agency while intelligence analysts (and other non-agent support personnel such as scientists and linguists) primarily were viewed in a less important support role for ongoing cases.

A May 2005 OIG audit examined the FBI's efforts to hire, train, and retain its intelligence analysts. Since the September 11 terrorist attacks, the FBI has emphasized the development of its intelligence analysis capabilities to help meet its highest priority of preventing future terrorist attacks. In the three years since the September 11 terrorist attacks, the FBI's analytical corps has grown from 1,023 analysts in October 2001 to 1,403 analysts in October 2004 – a net increase of 380 intelligence analysts or 37 percent.

The OIG audit found that the FBI has made progress in hiring and training intelligence analysts. However, the OIG found several areas in need of improvement. For example, the FBI fell short of its FY 2004 hiring goals and ended the fiscal year with a vacancy rate of 32 percent. In addition, the FBI has made slow progress toward developing a quality training curriculum for new analysts. The initial basic training course offered from 2002 to 2004 was not well attended and received negative evaluations. Furthermore, an OIG survey of FBI intelligence analysts found that work requiring analytical skills accounted for about 50 percent of the analysts' time, and many analysts reported performing administrative or other non-analytical tasks. In addition, some analysts said that not all FBI special agents, who often supervise the analysts, understand the capabilities and functions of intelligence analysts. Finally, our survey found that 22 percent of the FBI's current intelligence analysts said they plan to leave the FBI within 5 years. Among analysts hired since FY 2002, 35 percent said they do not plan to remain with the FBI for 5 years.

The OIG report made 15 recommendations to help the FBI improve its efforts to hire, train, and retain intelligence analysts. These include recommending that the FBI develop and implement a threat-based or risk-based methodology for determining the number of intelligence analysts required and for allocating the positions among FBI offices; assess the work done by intelligence analysts to determine what is analytical in nature and what general administrative support of investigations can more effectively be performed by other support or administrative personnel; and develop retention and succession strategies for intelligence analysts. The FBI agreed with all of the recommendations. To date, the FBI has fully addressed 4 of our 15 recommendations, including improving its applicant processing and training programs, and establishing a funded staffing level for analysts.

In a report issued in March 2005, the OIG examined the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) implementation of the Safe Explosives Act, implemented as part of the Homeland Security Act of 2002 to expand the ATF's licensing authority over the manufacture, purchase, and use of explosives. This issue can affect the ability of individuals to obtain and use explosives in terrorist acts.

The OIG found critical deficiencies in the ATF's implementation of the Act, including that the ATF did not effectively identify and prevent potentially dangerous individuals from having access to explosives. According to ATF records, the ATF failed to request an FBI background check on 9 percent of the more than 38,000 individuals who had applied for permission to work with explosives. In addition, in cases where the ATF had requested an FBI background check, the OIG found that in many cases the ATF failed to complete the clearance process. As a result, 31 percent of the applicants remained in a "pending" status in the ATF's Federal Licensing System. Until the ATF completes the clearance process, applicants can continue to work with explosives. The OIG found that, on average, these applicants had remained in a pending status for 299 days. A finding of particular concern was that the individuals who remained in a pending status included some who have extensive criminal records.

The OIG found other problems with the ATF's explosive licensing program, including incomplete and error-filled records in the ATF's licensing database, and inadequate training in explosives products provided to ATF inspectors who oversee explosives licensees. In addition, the OIG found that the ATF only recently began to make plans for implementing the authority granted by the Safe Explosives Act in November 2002 to collect and catalog samples of explosives at the ATF National Laboratory. The OIG report made ten recommendations to help improve the ATF's implementation of the Safe Explosives Act and more effectively regulate explosives within the United States.

In sum, the Department's counterterrorism challenge is varied and unceasing. While the Department has made progress in its counterterrorism efforts, continuing improvements are needed because of the importance of and difficulties associated with the Department's top challenge of detecting and deterring terrorism.

2. Sharing of Law Enforcement and Intelligence Information: The Department has made strides this past year to improve its sharing of law enforcement and intelligence information with federal, State, and local officials. The ability to share such information timely and effectively is critical to the Department's success in preventing violent crime and acts of terrorism.

As part of the OIG's September 2005 review of the FBI's reallocation of resources from traditional crime areas to terrorism-related matters (discussed in Challenge 1), the OIG interviewed FBI managers, other federal law enforcement officials, and numerous state and local law enforcement personnel in 12 major cities to assess their perspectives on the FBI's shift in priorities. The majority of FBI managers and other law enforcement officials we interviewed at both the headquarters and field office levels stated that the overall relationships between the FBI and other law enforcement agencies have improved over the last few years. State and local law enforcement officials also indicated that the FBI has shared more terrorism-related information with them since the September 11 attacks. However, while they welcome this intelligence information, many of the

state and local officials we spoke with said they would like the FBI to share more information related to traditional crime areas, such as gangs.

Similarly, a June 2005 OIG review of the Department's counterterrorism task forces and councils, which are responsible for coordinating and integrating intelligence and law enforcement activities related to terrorism prevention and prosecution, found that information sharing improved as a result of the task forces and councils. The majority of state, local, and federal law enforcement officials interviewed by the OIG stated that they were more satisfied with the exchange of terrorism information since September 11, 2001.

In the past year, the OIG has reviewed several other Department programs and operations related to the sharing of law enforcement and intelligence information, including the integration of the FBI's and the Department of Homeland Security's (DHS) automated fingerprint identification databases, the FBI-run Terrorism Screening Center, the ATF's National Integrated Ballistic Information Network (NIBIN), and the Department's Joint Automated Booking System. In these and other reports, the OIG found that the Department has made progress in improving its sharing of law enforcement and intelligence information, but it continues to face significant challenges in this area, both within the Department and with its law enforcement and intelligence agency partners.

For example, in June 2005 the OIG publicly released an unclassified, redacted version of its report that examined the FBI's handling of intelligence information in its possession prior to the September 11 attacks. The OIG review reported on significant deficiencies in the FBI's handling of this intelligence information and concluded that the FBI had failed to fully evaluate, investigate, exploit, and disseminate information related to an Electronic Communication written by an FBI agent in Phoenix, Arizona, that raised concerns about efforts by Usama Bin Laden to send students to attend United States civil aviation schools to conduct terrorist activities, and intelligence information available to the FBI regarding two of the September 11 hijackers – Nawaf al Hazmi and Khalid al Mihdhar.

The causes for these failures were widespread and varied, ranging from poor individual performance to more substantial systemic deficiencies that undermined the FBI's efforts to detect and prevent terrorism. Among other things, the OIG review described the systemic impediments that had hindered the sharing of information between the FBI and the Central Intelligence Agency.

In its response to the OIG's report, the FBI described changes it has made related to these issues since the September 11 attacks, including upgrading the physical infrastructure in FBI field offices to handle classified information, establishing centralized intelligence components in each field office, and training initiatives on subjects such as disseminating threat-related information and the Foreign Intelligence Surveillance Act. In addition, the FBI created a panel to assess whether any action should be taken with regard to the performance of FBI employees described in the OIG report.

As discussed in more detail elsewhere in this document, one of the biggest obstacles hindering the FBI's ability to rapidly and fully share information are problems associated with its Information Technology (IT) systems, particularly the FBI's failure to upgrade its automated case management system. The FBI believes that Sentinel, the successor to the aborted Virtual Case File effort, will result in a case management system that provides an automated workflow process, search capabilities, and effective records and case management.

In this regard, the FBI is also the lead agency for developing an interagency Federal Investigative Case Management System, with Sentinel serving as the application of that framework for eventual adoption by other federal investigative agencies. The DEA, ATF, DHS, and other participating agencies are relying on the FBI's successful development of Sentinel to meet their own case management needs and enhance information sharing within the federal law enforcement community. In an ongoing review, we have found that the FBI allowed these agencies to review its

completed requirements for Sentinel, including the information-sharing requirements that need to be incorporated into the system's design by the contractor. However, the FBI has not yet asked the agencies to provide input in developing these requirements.

A separate OIG review examined another aspect of the Department's efforts to share critical terrorism-related information with other federal, state, and local law enforcement agencies. In June 2005, the OIG issued a report that assessed the operations of the FBI's Terrorist Screening Center (TSC), a multi-agency effort led by the FBI to consolidate the federal government's terrorist watch lists and provide 24-hour, 7-day-a-week responses for screening individuals against the consolidated watch list. Prior to establishment of the TSC, the federal government relied on multiple separate watch lists maintained by a variety of agencies to search for terrorist-related information about individuals who apply for a visa, attempt to enter the United States through a port of entry, travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation.

The OIG found that the TSC made significant achievements in developing and creating a consolidated terrorist watch list in a short period of time. However, the report identified several areas of the TSC's operations that need improvement, including database improvements, data accuracy and completeness, call center management, operational planning, and coordination between participating agencies. In addition, the OIG found that the TSC had not ensured that the information in its terrorist screening database was complete and accurate. For example, the OIG found instances where the consolidated database did not contain names that should have been included on the watch list and inaccurate or inconsistent information related to persons included in the database. The report made 40 recommendations to the TSC to address areas such as database improvements, data accuracy and completeness, call center management, and staffing, and the TSC generally agreed with the recommendations. The TSC also stated that it implemented many of the OIG recommendations and was conducting a record-by-record review of the watch list database to ensure that the inaccuracies are fixed.

In a separate OIG review that examined the treatment of the September 11 detainees, one issue related to our finding of weaknesses in Department information sharing remains unresolved more than 2 years after the report's issuance. In response to our recommendation that federal immigration authorities work closely with the Department and the FBI to develop a more effective process for sharing information during future national emergencies that involve alien detainees, the Department said that it was still working with the DHS to develop a memorandum of understanding that would govern the detention of aliens of national security interest. However, the memorandum of understanding had not yet been finalized.

Another aspect related to this challenge that the Department continues to address is improving its ability to share fingerprint information with other federal agencies. In December 2004, the OIG completed its fourth report in 4 years examining ongoing efforts to integrate the FBI's automated fingerprint identification database (IAFIS) with the DHS's automated fingerprint identification database (IDENT). Full integration of IDENT and IAFIS will assist law enforcement and immigration officers in identifying known criminals and known or suspected terrorists.

The December 2004 OIG report found that full integration of IDENT and IAFIS had yet to be realized and that the Department and DHS still had not entered into a memorandum of understanding to guide the integration of IAFIS and IDENT. In response to the OIG's report, the FBI is now making weekly transmissions of the fingerprints of known or suspected terrorists to the DHS, and the FBI has initiated actions to improve the availability of its IAFIS fingerprint system. In addition, in April 2005 the federal government agreed on a common fingerprint enrollment standard of 10 flat fingerprints for an integrated interoperable biometric fingerprint system. In July 2005, the DHS Secretary announced that US-VISIT, the DHS entry-exit system, would be modified to collect 10 fingerprints for enrollment. We believe this is a significant step towards fully integrating law enforcement fingerprint identification systems, and the OIG intends to initiate a follow-up review in FY 2006 to assess the status of IDENT/IAFIS integration.

During the past year, the OIG examined several other Department systems intended to enhance sharing of law enforcement information. For example, in June 2005, the OIG issued a review of the NIBIN, a national ballistic imaging system designed to assist federal, state, and local law enforcement agencies in solving gun-related crimes by identifying potential matches between crime-scene bullets and shell casings collected at other crime scenes. The OIG found that while the NIBIN program had been fully deployed with the capability to compare ballistic images on a national level, the necessary equipment had not been deployed to the sites that could best utilize it, and the nationwide search capability of NIBIN was rarely used. The OIG also found that the ATF had not taken steps to maximize the entry of firearms evidence into NIBIN.

The OIG also reviewed the Department's Joint Automated Booking System (JABS), a computer system that helps federal law enforcement agencies book, identify, and share information electronically about persons in federal custody. This May 2005 OIG report found that JABS has made important progress by automating the booking process in the Department's law enforcement components, providing an automated interface with the FBI's fingerprint system, and providing basic data sharing between components. However, the audit determined that JABS does not fully reduce booking steps through data sharing as envisioned, resulting in component redundancy and duplication of effort. The audit also found that the offender tracking system was incomplete, which reduced agencies' ability to track offenders. The OIG made six recommendations to improve JABS, and the Justice Management Division concurred with the recommendations.

In sum, the Department continues to make improvements in the way it shares intelligence and law enforcement information with other federal, state, and local agencies. However, the Department must continue to focus on ensuring the effective, secure, and timely sharing of intelligence and law enforcement information.

3. Department and FBI Intelligence-Related Reorganizations: As discussed in the first two Challenges, the Department's ability to effectively gather, analyze, share, and use intelligence information is critical to its success in meeting its counterterrorism and counterintelligence challenges. Both the Department of Justice and the FBI are reorganizing their national security elements into new structures, and this presents significant management challenges. Part of this restructuring is in response to the recommendations made by the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). In addition, creation of the Office of the Director of National Intelligence (DNI) may have an impact on the activities, personnel, and budget in counterterrorism and counterintelligence.

With regard to the reorganizations within the Department, the Department's national security elements – the Office of Intelligence Policy Review, and the Criminal Division's Counterterrorism and Counterespionage Sections – will be consolidated under a new Assistant Attorney General for National Security. In addition, in September 2005 the FBI created a new National Security Branch that combines the FBI's Counterterrorism Division, Counterintelligence Division, and Directorate of Intelligence. Both the Department's new division and the FBI's National Security Branch will be subject to the coordination and budget authorities of the DNI. According to the WMD Commission, the goal of this restructuring is to create a stronger and more centralized management of the intelligence community.

The segments of the FBI affected by the creation of the National Security Branch have been the subject of several major personnel increases and a series of major and minor restructurings since the September 11 terrorist attacks. When the FBI first attempted to bolster its intelligence capability in 2002 by creating an Office of Intelligence within its Counterterrorism Division, the Counterterrorism Division had approximately 200 agents. Today it has approximately 1,300 agents. In 2003, intelligence authorities across all FBI programs (Criminal, Cyber, Counterterrorism, and Counterintelligence) were unified under a new Office of Intelligence led by an Executive Assistant Director, and the FBI began a major initiative to hire additional intelligence

analysts. More recently, a Directorate of Intelligence was established within the FBI, comprised of a headquarters element as well as intelligence entities in each FBI field office called Field Intelligence Groups. Under the September 2005 reorganization, the work of this Directorate must now be integrated with the intelligence work of other federal agencies through the DNI.

For the FBI, one of the challenges is to successfully manage the strain placed upon an organization when it undergoes repeated changes to its organizational structure. As OIG audits have shown, the FBI already has undergone a major reprioritization of resources since the September 11 terrorist attacks. To gauge the effects of this shift in priorities, in September 2005 and September 2004 the OIG issued reviews that examined the changes in the FBI's allocation of its personnel resources. In the 2004 review, the OIG determined that the FBI had reallocated resources in accord with its shift in priorities from traditional criminal investigative work to counterterrorism and counterintelligence matters. The OIG also found that the FBI reorganized itself with the intent of creating a more proactive, intelligence-driven agency. The OIG report recommended that the FBI regularly conduct similar detailed analyses of its agent usage and case openings to provide a data-based view of the status of FBI operations and to assist managers in evaluating the FBI's progress in meeting its goals.

The Department's restructuring of its national security elements under a new Assistant Attorney General for National Security similarly presents challenges for the Department. This new structure will require creating new relationships with other federal, state, and local agencies and new reporting structures. The restructuring also will require the Department to make important decisions with respect to the allocation of its limited resources. Accomplishing each of these tasks effectively and efficiently, without any diminution in the Department's counterterrorism and counterintelligence efforts, presents an important challenge for the Department.

Another major challenge facing the FBI as it focuses on restructuring its intelligence division is improving its foreign language translation program. This program is critical to national security because it supports the FBI's counterterrorism and counterintelligence programs, as well as criminal and cyber-crimes investigations.

In July 2004, the OIG issued an audit that found that the FBI's collection of material requiring translation had outpaced its translation capabilities and the FBI could not translate all the foreign language counterterrorism and counterintelligence material it collected. In addition, the OIG audit found that the FBI had difficulty in filling its critical need for additional contract linguists and was not in full compliance with the quality control standards it had adopted for reviews of the work of FBI linguists.

A follow-up review in July 2005 concluded that the FBI had taken steps to address the OIG's recommendations from a year earlier and had made progress in improving the operations of its foreign language translation program. However, the OIG found that key deficiencies remain in the FBI's foreign language translation program, including 1) a continuing backlog of unreviewed counterterrorism and counterintelligence material; 2) some instances where high-priority material had not been reviewed within 24 hours counter to FBI policy; and 3) continued challenges in meeting linguist hiring goals and target staffing levels. In addition, implementation of the FBI's quality control program has been slow, although the FBI had made improvements in this area.

In August 2003, the OIG issued a report entitled, "A Review of the FBI's Performance in Detering, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." Hanssen's espionage began in November 1979 – 3 years after he joined the FBI as a special agent – and continued intermittently until his arrest in February 2001. The OIG concluded that Hanssen escaped detection not because he was extraordinarily clever and crafty, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. The OIG's report made 21 recommendations to help the FBI improve its internal security and enhance its ability to deter and detect espionage.

The OIG has initiated a review of the FBI's progress in implementing the recommendations contained in its August 2003 report. The follow-up review will assess the FBI's response in the following five areas: 1) improving the FBI's performance in detecting an FBI penetration; 2) improving coordination with the Justice Department; 3) improving source recruitment, security, and handling; 4) security improvements; and 5) management and administrative improvements.

In sum, the restructuring of the intelligence functions of the Department and the FBI that is currently under way creates significant challenges. The effectiveness of critical national security operations must be maintained and enhanced while the new organizational structures are created and solidified. Additionally, the development of a single and flexible intelligence community across multiple federal Departments is an enormous undertaking. In the coming years, the OIG will continue to examine how the Department and the FBI meet this multifaceted challenge.

4. Information Technology Systems Planning and Implementation: 2005 was a critical year in IT systems development in the Department. The FBI acknowledged that it would have to abandon its long-planned Virtual Case File system. The failure to timely develop this system, and the FBI's stated loss of more than \$100 million of the \$170 million invested in the project during its 3 years of development, were major setbacks to the FBI's efforts to reshape itself technologically and provide its employees with a modern, efficient case management system.

Congress has expressed its concerns about the Department's development of IT systems, most recently in separate House- and Senate-passed appropriation bills funding the Department in FY 2006. Both versions of the legislation would create a new account, the Justice Information Sharing Technology account, to fund cross-cutting Department IT initiatives and centralize control over information-sharing systems within the Department and its components under the Department's Chief Information Officer. According to the Senate report, the account is an effort to provide "more control to the Department Chief Information Officer to ensure that investments in information technology are well planned and aligned with the Department's overall IT strategy and enterprise architecture." The Senate report stated that the account would help ensure that Department components "build systems that are interoperable with shared components and not stove piped systems that become obsolete once operational."

Because the Department continues to face significant challenges in ensuring that its IT systems are developed and deployed in a timely and cost-effective manner, the OIG has undertaken a series of reviews examining key aspects of the Department's IT development and implementation efforts. Specifically, a variety of OIG reviews has assessed the Department's progress in Enterprise Architecture, project management, business process re-engineering, and E-government.

One ongoing OIG review is examining whether the Department is effectively managing its IT investments and developing an appropriate Enterprise Architecture. Preliminary audit results indicate that although the Department has not yet established Enterprise Architecture or IT Investment Management processes, it is actively developing and implementing new frameworks designed to establish these necessary architecture and processes in the future. The audit noted, however, that these frameworks are limited because the Department is relying on component Enterprise Architectures and IT Investment Management processes to support the overall Department-wide frameworks without ensuring the adequacy of the component-level frameworks. To do this, the Department must take a greater role in overseeing the completion of component Enterprise Architectures and IT Investment Management processes.

These efforts are important in avoiding the well-known problems the FBI has had in replacing its case management system. The FBI's efforts to develop a new electronic case management system called the Virtual Case File have been unsuccessful, and in early 2005 the FBI announced that it was terminating the Virtual Case File and replacing it with a new information technology effort called Sentinel. The FBI expects Sentinel to replace its antiquated paper-based case management system and enable the FBI to more efficiently manage its criminal cases and more effectively share information agency-wide and with other law enforcement and intelligence agencies.

A February 2005 OIG audit analyzed the problems with the FBI's IT modernization effort. The report found that the FBI had successfully completed the first two components of its IT modernization project, previously called Trilogy, which provided the hardware and communications infrastructure needed to run the FBI's various user applications, including its planned Virtual Case File. However, completion of this portion of Trilogy was significantly delayed and more expensive than anticipated – full deployment was completed 22 months later than expected, despite an additional \$78 million provided by Congress after the September 11 terrorist attacks to accelerate deployment of Trilogy's infrastructure components. In addition, the total costs for the infrastructure components of Trilogy increased from \$238 million to \$337 million over the course of the project.

The OIG audit identified a variety of causes for the problems in the Trilogy project, including poorly defined and slowly evolving design requirements, weak information technology investment management practices, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on the Trilogy project, unrealistic scheduling of tasks, and inadequate resolution of issues that warned of problems in Trilogy's development. The OIG report also faulted the FBI for moving forward with contracting for the Trilogy project without providing or insisting upon defined requirements, specific milestones, critical decision review points, and penalties for poor contractor performance.

At the request of the FBI Director and Congress, the OIG has initiated a long-term audit of Sentinel, the FBI's successor system to the failed Virtual Case File, to closely monitor its development and implementation. Initially, this audit is focusing on the FBI's planning for the project, including its approach to developing the system, management controls over the project, information technology management processes, project baselines, contracting processes, and funding sources. Rather than issue a single audit report, the OIG plans to issue a series of reports examining discrete aspects of the Sentinel project, such as the FBI's monitoring of the contractor's performance against established baselines and the progress of the project.

As of October 2005, our preliminary assessment is that the FBI has instituted important improvements in its IT management controls and practices that it did not have when it attempted to develop the Virtual Case File. As our February 2005 audit reported, the FBI's Virtual Case File effort suffered from poorly defined and slowly evolving design requirements, IT Investment Management weaknesses, lack of an Enterprise Architecture, and lack of management continuity and oversight. Our preliminary review of Sentinel indicates that, for the most part, the FBI is attempting to address these weaknesses in preparing for the Sentinel project.

However, despite these apparent improvements, our preliminary work has identified several issues of concern that the FBI will need to focus on in order to successfully develop and deploy the Sentinel case management project. For example, the FBI's Sentinel Program Management Office is not yet fully organized and staffed with systems engineers, contracting officers, and budget personnel. Further, the Sentinel Program Manager, on loan from another agency, has committed to 2 years with an option for a third year. Given the anticipated time frame for developing this project, the Program Manager may have to be replaced before Sentinel is completed and deployed. As noted in OIG audits, turnover of key personnel during the Trilogy effort undermined that project.

In addition, the FBI's internal review process has identified a number of risks in the Sentinel development process, risks that the OIG will review and monitor throughout its audit. These risks include: 1) the program award schedule is very aggressive; 2) Sentinel phases must interface with numerous legacy systems operated outside the FBI's Office of the Chief Information Officer; 3) parallel FBI initiatives could result in scope creep for the Sentinel project; 4) FBI mission or user requirements could change and also result in scope creep; 5) evolving Enterprise Architecture standards could present new design problems; and 6) total project costs are unknown.

As part of our ongoing audit, we also plan to review the FBI's plans to fund the Sentinel project. In late September 2005, the FBI requested congressional approval to reprogram \$97 million from its current funds to pay for the first of Sentinel's four development phases. As part of our ongoing Sentinel review, we plan to examine the amount of funding required, the source of funding to bring the project to completion, and the effect of FBI reprogrammings to fund Sentinel on other critical FBI operations.

Other OIG IT-related reviews in the FBI have found that the FBI has made progress by reorganizing its IT function and creating the Office of the Chief Information Officer to manage centrally all IT responsibilities, activities, policies, and employees across the FBI. The FBI has issued a Life Cycle Management Directive that now applies to its IT projects a structured investment management process, including decision gate reviews of proposed projects by an Investment Management Product Review Board. Also, the FBI has made progress toward developing a mature Enterprise Architecture. However, the FBI must ensure that it follows its IT investment management processes and that its projects are consistent with the FBI's Enterprise Architecture. In addition, the FBI must fully staff a professional Program Management Office to ensure that approved IT projects meet cost, schedule, performance, and technical benchmarks.

The OIG's IT reviews extend beyond the FBI. For example, in September 2004, the OIG issued a review that found the DEA is making solid progress towards developing Enterprise Architecture and IT investment management processes. The DEA had completed much of its Enterprise Architecture, with the exception of developing a target architecture and a transition plan to accomplish the target architecture. The DEA had also improved the effectiveness of its IT investment management (ITIM) by creating an IT investment awareness, characterizing its IT investment process through structured processes, and building the foundation for current and future investment success by establishing basic IT selection and control processes. By taking steps to improve its ITIM processes, the DEA has begun to mitigate the risk of basing its IT decisions on judgment, intuition, and partial data rather than on objective, systematic, IT-related information that is routinely collected and analyzed within the ITIM process. Institutionalizing the entire ITIM process will further reduce such risks to the DEA.

However, the DEA had not yet established measures of Enterprise Architecture progress, quality, compliance, and return on investment that are necessary to ensure that the Enterprise Architecture meets the targeted milestones and complies with the necessary regulatory requirements. In addition, the DEA had not established a schedule for fully developing all IT investment management practices.

Since issuance of our report, the DEA has: 1) established configuration management procedures for the completed Enterprise Architecture components; 2) outlined the process to be used to integrate and document security and privacy requirements in the target Enterprise Architecture; 3) created a schedule for completing Stages 3 through 5 of the IT investment management process; and 4) initiated the development of a project management plan to include metrics for measuring Enterprise Architecture progress, quality, compliance, and return on investment.

Another issue the OIG plans to track in the coming year is the Department's efforts to upgrade its Internet protocol. An Internet protocol provides the addressing mechanism that defines how and where information such as text, voice, and video move across interconnected networks. According to IT experts, Internet protocol version 4 (IPv4), which is widely used today, may not be able to accommodate the increasing number of global users and devices that are connecting to the Internet. Consequently, Internet protocol version 6 (IPv6) was developed to increase the amount of available space, promote flexibility and functionality, and enhance security.

The Office of Management and Budget has established June 2008 as the date by which all federal agencies' infrastructure must use IPv6. However, a May 2005 audit by the General Accountability Office (GAO) found that the majority of federal agencies, including the Justice Department, had not yet initiated key planning considerations for transitioning to IPv6. In particular, the GAO found

that the Department did not: 1) develop a business case, 2) have a transition plan, 3) inventory their IPv6-capable equipment; and 4) estimate transition costs.

In sum, the Department's complex and interrelated IT systems play a vital role in helping the Department meet its top priorities. Consequently, Department managers and IT specialists need to commit to a sustained oversight effort to ensure that the Department's IT systems are developed and managed effectively.

5. Information Technology Security: In addition to developing effective IT systems, the Department is faced with the significant challenge of ensuring the security of its critical IT systems and information. The OIG annually performs security assessments and penetration testing of Department computer systems, as mandated by the Federal Information Security Management Act (FISMA). Under FISMA, the OIG performs an independent evaluation of the Department's information security program and practices.

Our reviews have found that the Department continues to make progress in improving its IT security and, based on our system testing, the components have improved their adherence to IT security policies and procedures. Although the Department has made improvements with respect to its IT security, our FY 2004 testing found that the Department did not always perform verification of component data collected for FISMA reports. In addition, we found that the FBI, the DEA, and the U.S. Marshals Service (USMS) did not have a proper tracking system in place to ensure that all of their employees received computer security awareness training and education. The OIG also found that these components had not ensured that contingency plans for all certified and accredited systems were tested. In addition, the components insufficiently tracked vulnerabilities previously identified and corrective actions already taken for their information technology systems. Moreover, the OIG found that the FBI had not certified and accredited 6 of its 15 systems (40 percent) as reported in the OIG's FY 2004 FISMA review. As a result of our findings, we provided the Department with recommendations for improving its IT security oversight program.

In our FY 2005 FISMA reviews, we examined the security programs of the Justice Management Division, FBI, Federal Bureau of Prisons (BOP), and the DEA. As part of our review, we also selected two classified systems (the FBI's Automated Case Support System and the DEA's El Paso Intelligence Center Information System) and two sensitive but unclassified systems (BOP's Inmate Telephone System II and DEA's El Paso Intelligence Center Seizure System). We plan to issue separate reports in December 2005 for each of these components and the four mission-critical systems evaluated.

In addition, in July 2005 the OIG issued an audit that examined the policies and practices in the Department regarding handling classified information on portable computers. Our audit found that the current policies contain inappropriate and confusing references and do not provide complete guidance and instructions. Further, the OIG identified several innovative practices used by other agencies to help improve the use of portable computers for processing classified information while adequately safeguarding classified information. The report included 12 recommendations to assist the Department in improving the storing, processing, and transmitting of classified information on portable computers. The Department concurred with all 12 recommendations.

In sum, the Department's networks and databases are at continual risk from unauthorized access as hackers and potential terrorists develop new techniques to breach government computer systems. Ensuring the systems are secure is an important and continuing challenge for the Department and its components.

6. Financial Management and Systems: The Department was successful in obtaining unqualified opinions on each of the components' financial statements for both FYs 2005 and 2004, resulting in unqualified opinions on the Department's financial statements for both years. This past year involved significant efforts on the part of Department management to correct a series of deficiencies

in its financial management and systems that led to a disclaimer of opinion for FY 2004 on its consolidated financial statements. The reason for the disclaimer was that the Office of Justice Programs (OJP) received a disclaimer of opinion on its financial statements for FY 2004, and this disclaimer was significant enough to affect the Department's overall consolidated opinion. A second component, the ATF, received a qualified opinion for FY 2004 while all other Department components received unqualified opinions.

The Department proactively addressed these issues in preparing for the FY 2005 audit. It restated and re-audited the OJP financial statements for FY 2003 and FY 2004, resulting in the re-issuance of unqualified opinions for both years. OJP took action to address the problems identified during the FY 2004 audit, including improving its data, refining its grant accrual methodology, improving financial reporting, and addressing the significant information systems environment control weaknesses previously identified by the OIG. The ATF also was able to provide sufficient supporting documentation for its FY 2004 accounts payable accrual to enable an unqualified opinion on its FY 2004 financial statements.

The Department continues to face significant challenges because of the need to correct long-standing financial and accounting control issues. While the Department was successful in achieving unqualified opinions on its FY 2005 and 2004 financial statements, it still has two material weaknesses at the consolidated level and ten at the component level. For FY 2004, the consolidated report included two material weaknesses and one reportable condition. The total number of material weaknesses at the component level for FY 2005 remains unchanged from FY 2004, although the components affected are somewhat different. For FY 2005, the Department was able to eliminate one consolidated material weakness because of improvements in grant accounting at OJP, but the previously cited consolidated reportable condition related to information systems was elevated to a material weakness. At the component level, the Department was successful in reducing the number of reportable conditions from 13 in FY 2004 to 8 in FY 2005.

Even taking into account the significant progress made in correcting past years' deficiencies, the Department's financial controls remain a serious management challenge. To move forward, the Department must concentrate on standardizing and integrating financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes. In an effort to address these and other deficiencies, the Department has pursued the Unified Financial Management System project to replace the seven major accounting systems currently used throughout the Department. While the Department selected the vendor for the unified system in FY 2004, its progress in implementing the new system has been slower than planned.

Currently, none of the Department's accounting systems are integrated with each other. Consequently, Department-wide accounting information is produced manually, which is costly and compromises the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles.

Beginning in FY 2004, audits of the Department's components must be completed within approximately 30 days of the end of the fiscal year for the Department to successfully meet the accelerated reporting deadlines. The key to success in meeting the expedited time lines is the quality of accounting records throughout the year. Effective controls must be enforced to ensure accurate, timely financial information is available throughout the year, not solely after the fiscal year ends.

For FY 2004, the Department was able to meet the new reporting deadlines, but at the expense of an unqualified opinion. While the Department was able to regain its unqualified opinions for FY 2005, it still faces significant challenges as evidenced by the two consolidated and ten component material weaknesses. Because of the Department's reliance on manual processes and multiple, ineffective financial systems, its capability to provide managers with current and accurate financial information also remains limited. For FY 2005, the Department's primary challenge was to

successfully address the known issues at OJP, ATF, and other components while continuing to meet the reporting deadline. However, challenges involving the USMS's internal control framework and management and recording of real property were added this year and must be addressed by the Department in FY 2006.

7. Grant Management: Grant management remains a long-standing challenge in light of the more than \$3.5 billion appropriated to Department grant programs in FY 2005.

OIG audits have shown that grant awarding agencies, such as OJP and the Office of Community Oriented Policing Services (COPS), need to ensure that grantees receive clear, timely, and unambiguous guidance on the specific criteria under which grantees will be held accountable. The myriad of policy guidance cited in "boilerplate" application and award documents (OJP Financial Guide and COPS User Manuals) can often be confusing and contradictory, increasing the risk that grantees will be less likely to satisfy their fiduciary responsibility to safeguard grant funds and ensure funds are used solely for the purposes for which they were awarded.

On a positive note, at the end of FY 2005 OJP had fully automated its request for funding and financial reporting processes. However, the OIG has identified areas related to the Department's management of grant programs that need further improvement.

In March 2005, the OIG issued an audit report on the administration of tribal-specific Department grant programs. We found that COPS, OJP, and the Office on Violence Against Women were not effectively monitoring the tribal grant programs. These components did not ensure that tribal grantees submitted information necessary to assess grant implementation and achievement of grant objectives and did not effectively monitor utilization of grant funds. We also found that the Department did not have a formal process for coordination, information sharing, and training staff responsible for monitoring and administering grants awarded to tribal governments. Our report contained 53 recommendations that focus on the need to adequately monitor grants, require financial and progress reports to be submitted in a timely manner, and ensure that funds drawn down by grantees do not exceed immediate needs for active grants and excess funds are not drawn down for expired grants.

As a result of the significant findings in the tribal grant audit, the OIG conducted a follow-up review to evaluate the effectiveness of the Office for Victims of Crime tribal victim assistance program. The OIG found a wide range in the effectiveness of four individual grantee tribal victim assistance programs.

In November 2004, the OIG issued an audit of the OJP's No Suspect Casework DNA Backlog Reduction Program, a grant program that provides funding to states for the identification, collection, and analysis of DNA samples from evidence collected in cases where no suspect was developed or in which the original suspect was eliminated. Our audit found that OJP failed to closely monitor grantee progress in using funds before awarding additional funds, implemented inconsistent program requirements, and failed to ensure that program funds benefited the national DNA database. We also determined that four grantee laboratories did not maintain adequate documentation to substantiate that their oversight of contractor laboratories met certain quality assurance requirements, and that some costs charged to program awards were unallowable or unsupported. OJP agreed with our recommendations and plans to correct the deficiencies we identified.

In a September 2004 audit, the OIG found that two OJP organizations that awarded the majority of technical assistance grants did not consistently conduct program and financial monitoring. In addition, we found little coordination between the program offices and OJP's Office of the Comptroller. The OIG recommended that grant managers receive annual training to ensure that they are knowledgeable about OJP's requirements for submission of timely and accurate reports, grant monitoring, and grant closeout procedures. We also recommended that OJP bureaus work

with grantees to develop performance or outcome measures to assess the effectiveness of technical assistance and training grants. OJP agreed to take corrective actions in response to the report's recommendations and by the end of FY 2005 it was in the process of redesigning several business processes, updating the grant manager's manual, and training grant managers. In response to another OIG recommendation, several months earlier OJP had begun to require all technical assistance and training grants to include performance and outcome measures.

Finally, the Department is facing the challenge to ensure that grants related to Hurricanes Katrina and Rita are properly awarded and monitored. The OIG has initiated a review of these grants and other grants related to hurricane reconstruction and response.

8. Detention and Incarceration: The Department's significant responsibilities to detain and incarcerate individuals held in the custody of the BOP and the USMS safely, humanely, and at a reasonable cost remains a top Department challenge. Aspects of this challenge include managing overcrowding in federal prisons, deterring staff sexual abuse of inmates, providing adequate medical care, preventing the introduction of contraband into the facilities, and housing detainees and inmates incarcerated on terrorism-related charges.

With rising prison populations come many difficulties and expenses. One is the need to provide cost effective medical care to inmates and detainees. A February 2004 OIG review examined the USMS's provision of medical care to prisoners in its custody and concluded that the USMS was not effectively managing this program. We identified deficiencies in how USMS was providing medical care, including a failure to adequately track and monitor communicable diseases and a failure to provide adequate emergency response to prisoners. We also found that by failing to comply fully with statutory cost saving measures, the USMS was paying approximately \$7 million more annually than necessary for prisoner medical care. Since issuance of the OIG audit, the USMS has secured funding through the Office of Detention Trustee and as of August 2005 it was in the process of negotiating the national managed health care contract.

We also are completing an audit of the BOP Pharmacy Services program. In this audit, we found that the BOP spent approximately \$51 million on pharmacy services in 2004. We concluded that the BOP needs to assess its new initiatives that are designed to reduce the cost of pharmacy services. In addition, BOP needs to improve accountability and safeguarding of prescription medication and ensure its pharmacies comply with existing policies for administration of prescription medication. Given the growth in medical costs and the increasing size of the federal prisoner population, the effectiveness with which the Department meets the medical needs of individuals in its custody remains a top management challenge for the Department.

Another challenge presented by rising prison populations is the Department's ability to obtain affordable detention space for individuals not housed in federal facilities. A June 2005 audit examined the USMS's ability to obtain detention space for its inmates and detainees in local facilities. Historically, the USMS used its Cooperative Agreement Program to provide money to local jails for fund expansion in return for guaranteed jail space for federal detainees. However, because funding for the Cooperative Agreement Program was eliminated in FY 2005, the USMS expects to lose more than 11,000 guaranteed bed spaces between FYs 2005 and 2029. In addition, the USMS has identified 47 cities in which detention space is a serious or emergency problem. The OIG review found that even though the USMS faces a critical challenge to house its prisoners and detainees, it had not developed specific plans for securing detention space, at a reasonable cost, once Cooperative Agreement Program funding expires.

The Department faces different challenges in detaining terrorism suspects. For example, the OIG currently is assessing whether the BOP has implemented adequate controls over inmates' mail to protect the security of institutions and the public. This review arose in response to concerns that 3 convicted terrorists incarcerated at the U.S. Penitentiary in Florence, Colorado, wrote approximately 90 letters to individuals outside prison, including Islamic extremists who are members of a Spanish terror cell tied to the March 2004 terrorist train bombings in Madrid.

The OIG also plans to evaluate how well the BOP is regulating inmate use of telephones. In October 2005, the OIG initiated a follow-up review to assess the BOP's implementation of 17 recommendations from a 1999 OIG report that evaluated the BOP's management of inmate telephone privileges. The initial review was prompted in part by several prosecutions of high-profile inmates who were convicted of committing crimes from inside a BOP facility. The review determined that inmate abuse of prison telephones is a significant problem and that the BOP had failed to institute measures to adequately control the abuse. The OIG found that the BOP monitored only a small percentage of telephone calls and failed to target inmates who posed a high risk of committing crimes using prison telephones. The OIG recommendations focused on improving telephone monitoring, imposing proactive restrictions on telephone privileges, and making the discipline of telephone abusers more consistent. The follow-up review will evaluate the current status of the BOP's management of inmate telephone privileges.

In response to an April 2004 OIG review of the BOP's recruitment, endorsement, selection, and supervision of Muslim religious services providers, the BOP has taken steps to implement the OIG's recommendations. For example, the OIG review found that the BOP and the FBI did not adequately exchange information on the organizations the BOP relies on to endorse candidates who provide religious services to Muslims. We also found that inmates often led Islamic services subject only to intermittent supervision from BOP staff members.

Since issuance of this report, the BOP has developed enhanced screening criteria for religious services providers, and it has recruited an additional staff member to serve as a liaison with the FBI. With respect to supervision practices, the BOP has accepted the report's conclusions that inmate-led services should be reduced, that supervision in the chapel areas should be enhanced, and that reading materials should be screened more effectively.

The OIG's June 2003 Detainee Report and our December 2003 supplemental report on the treatment of detainees at the Metropolitan Detention Center (MDC) in Brooklyn, New York, made a series of recommendations to help improve procedures for handling aliens arrested in connection with terrorism investigations. We also recommended discipline for several MDC staff members who we found had physically abused some of the detainees. The BOP has taken actions to address the systemic recommendations, including: 1) modifying its training to address the appropriateness of specific inmate escort techniques; 2) providing guidance to prison staff on the prohibition of recording communications between inmates and their attorneys; and 3) implementing policies on videotaping incoming high-security inmates and documenting injuries to inmates. In addition, in July 2005 the OIA completed its review and sustained many of the OIG's findings. The BOP has initiated the disciplinary process, and is still in the process of deciding the appropriate discipline. The OIG continues to monitor the BOP's actions with regard to disciplinary action.

In April 2005, the OIG completed a review examining staff sexual abuse of federal inmates. The report discussed the number of sexual abuse cases investigated by the OIG in federal prisons and highlighted the shortcomings of current federal law in deterring staff sexual abuse. The OIG found that current federal penalties making it a misdemeanor to engage in unforced sexual abuse or sexual contact with an inmate are out-of-step with similar state laws. In fact, the OIG found that unlike federal laws, 43 of the 50 states make unforced sexual relations with inmates a felony. The OIG also noted that current federal laws covering sexual abuse of inmates do not apply when federal inmates are held in facilities under contract to the federal government rather than in BOP facilities. The OIG's report recommended that the Department seek passage of legislation: 1) to increase the statutory maximum penalties for sexual abuse of an inmate and sexual contact with an inmate to a felony, and 2) to extend federal criminal jurisdiction to individuals who engage in a sexual act or sexual contact with a federal prisoner housed in a detention facility under contract to the Department. House and Senate versions of legislation to reauthorize the Department for FY 2006-2009 both contain language that would address these shortcomings.

Historically, the confinement of individuals awaiting trial in federal court or immigration proceedings was the responsibility of the USMS and the former Immigration and Naturalization Service (INS). However, long-standing concerns about the cost and efficiency of federal detention efforts by two separate Department components resulted in a fragmented approach to detention management. Because of the magnitude of these issues, the Department concluded that a central command structure was key to realizing cost savings and improving efficiency in managing detention activities. Consequently, in FY 2001 Congress created the Office of the Federal Detention Trustee (OFDT) to centralize responsibility for detention and to better plan for needed detention resources without unwanted duplication of effort or competition with other Department components.

In a December 2004 audit, the OIG examined the funding and the accomplishments of the OFDT since its inception, assessed how the OFDT coordinates and oversees detention activities within the Department, and reviewed the office's plans for managing detention needs. The OIG review found that the OFDT had not yet been able to complete the goal of centralizing and overseeing Department detention activities. The former INS's transfer to the Department of Homeland Security in March 2003, leadership vacancies, and other obstacles have complicated the OFDT's ability to build a firm foundation with a clearly defined organizational purpose. In addition, the report found that recent funding shortages for detention issues have necessitated the transfer of funds to the OFDT from other Department initiatives.

We recommended that the Department and the OFDT address the continued lack of accuracy in estimating the cost of detention activities that has caused budgetary shortfalls to occur and take steps to help contain the continually rising costs of detention. In addition, we recommended that the Department take action to establish the role and functions of the OFDT.

9. Judicial Security: Two OIG reports identified significant deficiencies in the USMS's effort to ensure the security of the federal judiciary. The issue of judicial security received national prominence in early March 2005 when two members of a federal district court judge's family were murdered by a disgruntled litigant in Chicago, Illinois, and a state judge, a court reporter, a deputy sheriff, and a federal agent were killed by an escaped prisoner in Atlanta, Georgia.

In March 2004, the OIG issued a report on the USMS's efforts to improve its protection of the federal judiciary. The review examined the USMS's ability to assess threats and determine appropriate measures to protect members of the federal judiciary during high-threat trials and while they are away from courthouses.

The OIG report found that after September 11, 2001, the USMS had placed greater emphasis on judicial security by hiring 106 court security inspectors and improving the physical security of courthouses. However, the OIG also found that the USMS's threat assessments were often untimely and of questionable validity. Further, we found that the USMS had only a limited capability to collect and share intelligence on potential threats to the judiciary with USMS districts, the FBI's Joint Terrorism Task Forces, and other law enforcement entities. Moreover, the USMS lacked adequate standards for determining the appropriate protective measures that should be applied to protect the judiciary against identified potential risks.

For example, the OIG found that the USMS failed in 73 percent of the cases to meet its internal standard that requires threats against judges to be assessed within a specific time period. In addition, the OIG review found that USMS failed to improve the timeliness of its threat assessments despite a 30 percent decrease in the number of reported threats since FY 2000. Furthermore, the OIG report found that the USMS database used to assess threats has not been updated since 1996. The database contained no information on the more than 4,900 threats made since that time, including threats related to terrorism cases that have occurred since September 11, 2001.

The OIG review concluded that the USMS must improve its ability to assess threats against the federal judiciary in an accurate and timely manner, and develop a proactive approach to collecting

and sharing the information necessary to this security challenge. We made six recommendations to improve the USMS's judicial security efforts.

Since issuance of our report, the USMS has reported that it instituted rating criteria to identify, assess, and prioritize all threats and to ensure that all threats are assessed within established time frames. However, the USMS's revised threat assessment policies have not been formalized because, according to the USMS, other revisions may result from the ongoing Attorney General's review of judicial security.

In response to another finding in the OIG report, the USMS said it had merged the historical threat database into the Justice Detainee Information System which: (1) allows additional data from closed cases with known outcomes to be utilized in the comparative analysis of new threats, (2) allows the program to be used with greater ease by analysts, and (3) improves the accuracy of the comparative analysis process. In addition, data on approximately 4,900 threats that had not been entered into the USMS's previous threat database have been entered into the new system. The database now includes data on about 7,000 threats from 1980 to the present.

Moreover, the USMS appears to have made some progress in revising its policies to establish risk-based standards and require after-action reports for high-threat trials and protective details. The USMS has drafted a new protocol for conducting judicial threat assessments, but USMS officials said the protocol will not be finalized until the USMS receives recommendations from the ongoing Attorney General's judicial security working group.

While the USMS has taken several significant steps to respond to the report's recommendations, we believe it must make further action to improve its protection of the federal judiciary. The USMS indicated in its response to our report that it would assign full-time representatives to all 56 FBI Joint Terrorism Task Forces and ensure effective liaison with intelligence agencies. However, it appears that overall the USMS has reduced rather than increased its full-time representation on the Joint Terrorism Task Forces. When our report was issued in March 2004, the USMS had 50 representatives assigned to Joint Terrorism Task Forces, 25 of whom were full-time and 25 who were part-time. As of September 2005, the USMS had 58 representatives assigned to the Joint Terrorism Task Forces, but only 20 were full-time and 38 were part-time. We believe that the continuing lack of full-time representation on the task forces presents a potential intelligence vulnerability, not only to the USMS's judicial security responsibilities but to all USMS missions.

In addition, our report recommended that the USMS create a capability to collect and share intelligence. In response, the USMS established an Office of Protective Intelligence to oversee the handling of judicial threat information. According to the USMS, the Office of Protective Intelligence is responsible for the collection, analysis, and dissemination of all intelligence relating to the safety of USMS protectees, employees, facilities, and missions. However, it has been staffed with only five positions since its creation in June 2004. While the USMS stated in May 2004 that additional analysts would be reassigned to the office, those positions have not materialized and, as of April 2005, the USMS had offered no timetable for the transfer. We believe it is essential that the Office of Protective Intelligence be staffed appropriately to effectively carry out its critical mission.

In another audit issued in May 2005, the OIG examined another aspect of judicial security – the USMS's use of the more than 2,700 contract guards hired annually to transport federal prisoners to and from court facilities and to guard federal prisoners in courtrooms or cellblocks. The audit identified a number of serious deficiencies, such as internal control weaknesses that allowed for the hiring of unqualified individuals for guard service.

For example, the OIG review found that some of the independent contract guards hired by the USMS lacked the experience required to qualify as contract guards. The OIG audit also found that 30 percent of the armed contract guards did not always receive their firearms refresher training every 6 months, as required by USMS policy. In fact, 13 percent of the armed independent

contractors had gone a year or longer without re-qualifying with their firearms. Furthermore, due to lack of documentation in USMS files the audit also could not verify that applicable background investigations were performed on contract guards prior to their employment.

The OIG will continue to monitor the USMS's implementation of the recommendations in both of these OIG reviews. While the USMS has begun to take steps to respond to our recommendations, concerted, sustained action is needed to protect the safety and security of federal judges and federal courthouses throughout the country.

10. Supply and Demand for Drugs: An ongoing challenge for the Department is to reduce both the supply of and demand for drugs. Law enforcement efforts to reduce the supply of illegal drugs in the United States are an integral part of a comprehensive drug strategy. However, enforcement alone is not sufficient to reduce illegal drug use, and the Department faces a continuing challenge to find ways to reduce both the supply of and the demand for illegal drugs.

The federal government has funded programs on drug abuse education, prevention, treatment, research, rehabilitation, drug-free workplaces, and drug testing in an effort to reduce the demand for illegal drugs. On the supply reduction side, the President's National Drug Control Strategy and the Department's FY 2003-FY 2008 Strategic Plan include strategies to reduce the drug supply in the United States by 10 percent by the end of FY 2008.

However, one of the growing challenges for the Department is reducing the illegal diversion of prescription drugs for non-medical purposes. Diversion occurs when legally produced pharmaceuticals are illegally obtained for non-medical use. According to the Substance Abuse and Mental Health Services Agency, controlled pharmaceutical diversion accounts for 30 percent of all reported deaths and injuries associated with drug abuse.

A September 2002 OIG report found that the DEA did not adequately address the problem of controlled pharmaceutical diversion, and that the DEA did not allocate sufficient diversion investigators and special agents to its diversion efforts. We found that the DEA focused the majority of its resources on dismantling drug trafficking operations, despite alarming trends in the diversion of controlled pharmaceuticals.

Since our report, the DEA has allocated 158 new positions to diversion control; requested permission from the Department to convert its diversion investigators to special agents, thus expanding their investigative authority; and completed a review of intelligence capabilities to provide improved support for diversion control. The DEA also has developed a toll-free international hotline for people to report the illegal sale and abuse of pharmaceutical drugs.

The OIG recently initiated a follow-up review of the DEA's Diversion Control Program, including an in-depth look at the actions that DEA has taken in response to our previous report on the diversion of controlled pharmaceuticals. Diversion has become an increasingly widespread and serious problem in the United States. The reasons for this increase include the recent availability of higher potency products and the use of the Internet to facilitate diversion. The OIG's follow-up review will examine the DEA's response to the growing problem of Internet diversion, as well as the amount of law enforcement and intelligence support provided for diversion investigations.

Another significant challenge for the Department is addressing the supply and demand for methamphetamines. In August 2005, the DEA announced that the first nationally coordinated methamphetamine investigation resulted in more than 400 arrests and the dismantling of 56 clandestine drug laboratories nationwide.

Since 1998, the COPS Office has distributed more than \$218 million under the congressionally created methamphetamine initiative. Generally the purpose of these COPS grants is to assist state and local law enforcement agencies in reducing the production, distribution, and use of methamphetamine. In December 2004, the OIG initiated a review to examine the adequacy of

COPS' management of this initiative as well as its administration and monitoring of grantee activities. We also are evaluating the extent to which the grantees have administered grants in accordance with applicable laws, regulations, guidelines, and terms and conditions of the grant awards.

Another continuing challenge for the Department is keeping drugs out of federal prisons and rehabilitating drug-addicted inmates. In January 2003, the OIG issued an evaluation that found that the BOP did not search visitors or monitor visiting rooms adequately, did not search staff or take sufficient measures to prevent drug smuggling by BOP staff, or provide adequate non-residential drug treatment to inmates. In response to our recommendations in that report, the BOP has proposed or implemented revisions to strengthen visitor searches, improve surveillance of visiting rooms, to expand the use of non-contact visits, to expand drug interdiction training to staff, to limit the size and content of staff's property entering the prisons, to limit unsolicited mail received by inmates, to expand the non-residential drug treatment program, and to provide incentives to inmates to participate in non-residential drug treatment.

The BOP has not agreed with the OIG recommendation to search staff and their property upon entry and has asked for additional time to study the results of other actions it intends to take before making a final decision on searching staff. The OIG plans to conduct a follow-up review in FY 2006 to evaluate the BOP's actions in responding to the OIG's recommendations.

In sum, reducing the supply of illegal drugs, the diversion of legal prescription drugs for illegal use, and the demand for illegal drugs remains a critical, ongoing challenge for the Department.

**THE DEPARTMENT OF JUSTICE MANAGEMENT'S RESPONSE TO
THE OFFICE OF INSPECTOR GENERAL'S TOP
MANAGEMENT AND PERFORMANCE CHALLENGES-2005**

1. COUNTERTERRORISM

The Department must deter, prevent, and detect future terrorist acts.

Issue: *There is a need for more stable leadership among the Department's task forces and councils, better training for participants, increased attention to the Foreign Terrorist Tracking Task Force (FTTTF), greater involvement in the task forces by the DEA, additional resources, and increased coverage of remote areas.*

Action: The FBI is committed to having experienced supervisors leading its task forces. However, due to their seniority, the Senior Special Agents (SSAs) are also in line for promotions to higher level positions and consequently, the turnover rate is somewhat of a double edged sword; to get experienced SSAs to lead the task forces, there is the potential of losing the candidate to a promotion. The FBI Counter-terrorism Division (CTD) has undertaken a project to establish a structured orientation and training program for the Joint Terrorism Task Force participants, to be implemented in FY 2006. The FBI is focused on ensuring long-term, stable leadership; organizational structure; and sufficient resources for the FTTTF. The FBI uses the annual budget process to request enhancements for its task forces. As part of our current strategy for addressing the law enforcement community in remote areas, the CTD is coordinating with the Directorate of Intelligence (DI) to produce an FBI National Report on a weekly basis, which will be the primary terrorism threat outreach bulletin for the nationwide national law enforcement community at the for official use only/law enforcement sensitive classification level. DEA and FBI are currently in discussion for increasing DEA's membership in Joint Terrorism Task Forces and developing a joint plan.

Issue: *The FBI needs to upgrade its information technology systems (IT). The FBI's current IT systems fall far short of what is needed, and its efforts to create a modern case management system to catalogue, retrieve, and share case information have not succeeded.*

Action: SENTINEL is the FBI's current acquisition program for obtaining an electronic information system that provides case management, intelligence analysis, and field administration capabilities. SENTINEL will deploy a Service Oriented Architecture (SOA) in accordance with the FBI Enterprise Architecture and develop a baseline for the Department of Justice Federal Investigative Case Management System. FBI developed an acquisition strategy for SENTINEL in February 2005. SENTINEL will be deployed in four phases, with each phase delivering a stand-alone capability, during an approximate 39-month total development life cycle. The delivery of the first phase of SENTINEL will occur approximately 12 months after contract award.

Issue: *The FBI must value and support to a greater degree staff with technical skills. The FBI fell short of its FY 2004 hiring goals and ended the fiscal year with a vacancy rate of 32 percent. In addition, the FBI has made slow progress toward developing a quality-training curriculum for new analysts. An OIG survey of FBI intelligence analysts found that work requiring analytical skills accounted for about 50 percent of the analysts' time, and many analysts reported performing administrative or other non-analytical tasks. In addition, some analysts said that not all FBI special agents, who often supervise the analysts, understand the capabilities and functions of intelligence analysts. The OIG recommended that the FBI develop and implement a threat-based or risk-based methodology for determining the number of intelligence analysts required and for allocating the positions among FBI offices; assess the work done by intelligence analysts to determine what is analytical in nature and what general administrative support of investigations can more effectively be performed by other support or administrative personnel; and develop retention and succession strategies for intelligence analysts.*

Action: The FBI has established new policies and systems to ensure they hire and retain the highest quality Intelligence Analysts (IAs). A key component of these policy changes is the creation of an Intelligence Career Service (ICS), which acknowledges the importance of its intelligence mission and elevates the stature of its intelligence professionals by using a competency-based approach. This approach drives all aspects of the human resource continuum for ICS (e.g., selection and hiring, training and development, performance management,

retention, and Intelligence Officer Certification). With these new policies and systems, the FBI is hiring more applicants possessing one or more critical skills. In 2005 alone, the FBI hired an average of 60 new analysts each month, a 91% increase over the total number of IAs hired in FY 2004. They also lowered the attrition rate to approximately 6% for FY 2005, with more than 50% of the departures resulting from retirement or internal transfers.

To inform the hiring and allocation decisions, the FBI continues to develop and make plans to implement a threat-based methodology.

The FBI also ensures that it is developing a high-quality cadre of intelligence professional by implementing changes to its training program. They improved existing basic intelligence training by instituting their Analytic Cadre Education Strategy (ACES) course, and trained more than 1,000 onboard analysts in FY 2005. By the end of FY 2006, the FBI plans to train all analysts in ACES. In October 2005, they also launched the Cohort Training Program where new IAs, Language Analysts, and Physical Surveillance Specialists enter on duty to the FBI together as a class to receive 5 weeks of basic intelligence training and orientation. The ICS Cohort curriculum reinforces the key roles and contributions of ICS members in carrying out the FBI's intelligence mission starting with their first day at the FBI. Providing a common foundation for understanding analytic tradecraft and tools, the Cohort class is a key element in the FBI's strategy for developing an intelligence culture throughout the Bureau.

Along with other Intelligence Community agencies, the FBI recognizes the need to provide more training on the role of IAs and more administrative support to IAs. The Directorate of Intelligence established a working group to identify administrative or non-intelligence duties and has begun implementing recommendations that focus the FBI's Operations Specialists on intelligence analytic work. The FBI incorporated intelligence into its investigative training and created several joint-training opportunities between agents and analysts to foster greater understanding of these interrelated roles.

Issue: The OIG found critical deficiencies in ATF's implementation of the Safe Explosives Act (SEA). In particular, ATF did not effectively identify and prevent potentially dangerous individuals from having access to explosives. According to ATF records, the ATF failed to request an FBI background check on 9 percent of the more than 38,000 individuals who had applied for permission to work with explosives. In addition, in cases where the ATF had requested an FBI background check, the OIG found that in many cases the ATF failed to complete the clearance process. As a result, 31 percent of the applicants remained in a "pending" status in the ATF's Federal Licensing System (FLS). Until the ATF completes the clearance process, applicants can continue to work with explosives. The OIG found that, on average, these applicants had remained in a pending status for 299 days. A finding of particular concern was that the individuals who remained in a pending status included some who have extensive criminal records.

Action: The SEA enacted the most significant changes to federal explosives laws in over 30 years, requiring all persons receiving explosives to acquire a permit from ATF. ATF had 6 months to implement the SEA with limited resources in fiscal year 2003. ATF redirected firearms resources in fiscal year 2003 to issue approximately 4,000 explosives licenses/permits in order to implement the SEA by May 24, 2004. This included the conduct of background checks on all persons responsible for explosives-related operations. ATF has since conducted a 100 percent cross-match between data contained in the FLS and the FBI National Instant Criminal Background Check System (NICS E-Check) and found that these differences were due mainly to typographical errors made by data entry clerks. ATF is in the process of updating this information in the FLS system and NICS E-check as appropriate. Also, ATF has implemented new data entry procedures and quality control measures to ensure data accuracy and that all persons associated with explosives licenses and permits receive a background check. In response to the OIG's findings that individuals are remaining in a pending status for long periods of time, ATF has implemented new procedures that include timelier follow-up with employee possessors who do not respond to ATF requests for additional information. Information on non-responders is forwarded to ATF field offices for follow-up action. In response to the OIG's finding relating to individuals who remained in a pending status who had extensive criminal records, some of these instances were a result of typographical data-entry errors and untimely FLS updates. In no instance did ATF knowingly allow anyone with a criminal record to possess explosives. All individuals in question have been issued letters of denial. In addition to the new data quality control measures, ATF now has data entry procedures that include the immediate update of FLS with a denied status for all individuals that have been identified by FBI NICS as being prohibited. By statute, ATF

cannot prevent an individual from possessing explosives until such time as a record of disposition is found stating the specific prohibition. The mere evidence of an arrest is not enough to deny an individual the right to possess explosives in conjunction with a federally licensed/permitted explosives operation.

Issue: The OIG found problems with the ATF's explosive licensing program, including incomplete and error-filled records in the ATF's licensing database, and inadequate training in explosives products provided to ATF inspectors who oversee explosives licensees.

Action: ATF has implemented new data entry procedures that will help ensure information entered into the FLS accurately reflects what was submitted by the explosive licensee/permittee. In addition, ATF has implemented new data quality internal control procedures that include a daily random sample of application data entered into FLS to ensure it is accurate and a cross check of information entered into FBI's E-Check system against what was entered into FLS. All discrepancies found are corrected. This ensures that the data used to run a background check accurately reflects what was submitted by the applicant.

2. SHARING OF LAW ENFORCEMENT AND INTELLIGENCE INFORMATION

The Department has a critical, but paradoxical, need to disseminate information that exposes credible threats to the national security interests of the United States among appropriate federal, state, and local officials, while maintaining appropriate security of that information, much of which is sensitive.

Issue: In September 2005, the OIG reviewed the FBI's reallocation of resources from traditional crime areas to terrorism-related matters to assess the perspectives of FBI managers, other federal law enforcement officials, and state and local law enforcement personnel on the FBI's shift in priorities. The majority of FBI managers and other law enforcement officials interviewed at both the headquarters and field office levels stated that the overall relationships between the FBI and other law enforcement agencies have improved over the last few years. State and local law enforcement officials also indicated that the FBI has shared more terrorism-related information with them since the September 11, 2001 attacks. However, while they welcome this intelligence information, many of the state and local officials said they would like the FBI to share more information related to traditional crime areas, such as gangs.

Action: The FBI has acted decisively to address and minimize any effect that its shift of resources from traditional crime areas to terrorism-related matters might have on relationships with law enforcement partners. As part of the strategy, the FBI has concentrated criminal investigative resources on the most critical federal crime problems: public corruption, civil rights, international organized crime, and major gangs. They also have leveraged resources by increasing the use of task forces with local, state, and federal law enforcement partners, particularly in anti-gang efforts. For example, the FBI increased the number of Safe Streets Gang Task Forces from 104 in FY 2004 to 125 during FY 2005, established a Mara Salvatrucha (MS-13) National Gang Task Force, and launched a National Gang Intelligence Center (NGIC). The NGIC will enable the FBI and its law enforcement partners to centralize and coordinate the national collection of intelligence on gangs in the United States and then analyze, share, and disseminate this intelligence with law enforcement authorities throughout the country. The FBI has undertaken similar efforts to expand its interagency task forces in white-collar crime and other traditional crime areas.

In addition, the FBI has created an intelligence dissemination site on Law Enforcement Online (LEO) on which they have posted hundreds of unclassified intelligence reports on a wide range of criminal issues. Approximately 45,000 state and local police officers hold LEO accounts.

Because terrorists use criminal enterprises and criminal activities to further their interests, criminal investigations develop invaluable intelligence on terrorists. This intelligence helps identify U.S. vulnerability to attack and directly supports the FBI and the Intelligence Community missions in the counterterrorism, counterintelligence, and cyber crime arenas.

Issue: In June 2005, the OIG issued a report that assessed the operations of the FBI's Terrorist Screening Center (TSC). The report identified several areas of the TSC's operations that need improvement, including database improvements, data accuracy and completeness, call center management, operational planning, and coordination between participating agencies. In addition, the OIG found that the TSC had not ensured that the information in its terrorist screening database was complete and accurate. For example, the OIG found

instances where the consolidated database did not contain names that should have been included on the watch list and inaccurate or inconsistent information related to persons included in the database.

Action: The TSC has taken vigorous action to address and satisfy all 40 recommendations raised in the June 2005 OIG Report. Five of these recommendations were closed in the initial report issued by the OIG in June 2005. In July 2005, the TSC submitted a response to the OIG that resolved the only unresolved recommendation, and in September 2005, the TSC submitted to the Inspection Division information to close 33 of the 35 remaining recommendations. The TSC aggressively worked to satisfy or exceed the OIG recommendations. With respect to database improvements, the process from the National Counterterrorism Center to the TSC has migrated to the use of Terrorist Identities Datamart Environment, a more robust and accurate data system. The TSC also has implemented a continuous automated update system to the National Crime Information Center's Violent Gang and Terrorist Organization File. With respect to data quality, not only have the previous database enhancements improved the data quality of its imports and exports, the TSC is constantly working with its partners to establish and maintain a thorough data integrity process through rigid quality assurance protocols and procedures to maintain a thorough, accurate, and current Terrorist Screening Database (TSDB). Furthermore, the TSC launched an exhaustive record-by-record review of the TSDB to ensure the highest quality of data possible. With respect to call center management, the TSC has implemented a highly effective organizational structure in its Terrorist Screening Tactical Operations Center to address the call center management findings. In summary, the TSC identified, prior to the OIG report, a predominant amount of the findings and took immediate steps to address them. The TSC maintains a proactive stance toward identifying and correcting all potential concerns with the ability of the United States Government to consolidate its approach to terrorism screening using the most accurate, current, and thorough data available, as well as the most effective and efficient methods.

Issue: *In an OIG review that examined the treatment of persons detained as a result of September 11, 2001, one issue related to weaknesses in Department information sharing remains unresolved more than two years after the report's issuance. In response to the OIG's recommendation that federal immigration authorities work closely with the Department and the FBI to develop a more effective process for sharing information during future national emergencies that involve alien detainees, the Department said that it was still working with the Department of Homeland Security (DHS) to develop a memorandum of understanding that would govern the detention of aliens of national security interest. However, the memorandum of understanding has not yet been finalized.*

Action: A working group comprised of representatives of DOJ (including FBI) and DHS was formed to complete the draft of a Memorandum of Agreement (MOA), which has been prepared in response to the recommendations of the OIG. The working group completed the revised draft MOA in April 2005, and the draft was then widely circulated at both DOJ and DHS. Personnel within DOJ and DHS made additional revisions to the MOA as a result of review. In the wake of Hurricanes Katrina and Rita, senior DHS officials requested additional time to complete DHS's requested revisions to the MOA. FBI has been informed that DHS will soon complete its final revisions and FBI stands ready to promptly review the revisions when they are received. It is anticipated that the MOA will be finalized and executed shortly thereafter.

Issue: *A June 2005 OIG review of the ATF's NIBIN, a national ballistic imaging system, found that, while the NIBIN program had been fully deployed with the capability to compare ballistic images on a national level, the necessary equipment had not been deployed to the sites that could best utilize it, and the nationwide search capability of NIBIN was rarely used. The OIG also found that the ATF had not taken steps to maximize the entry of firearms evidence into NIBIN.*

Action: The NIBIN Branch has developed milestones addressing deployment of equipment, use of NIBIN throughout the nation, and entry of firearms evidence into the system.

NIBIN continues to train users to perform nationwide searches at the Interagency Border Inspection System training in Largo, Florida. During the Fall 2005 Users Congress meeting in Tucson, Arizona, NIBIN distributed instructions on performing nationwide searches and requested that the attendees provide them to the users in their region. NIBIN also will post the instructions to the Users Area of its website.

The NIBIN Branch, contractors, coordinators and partner agencies have been working together to promote the program through increased presence in the press and other outreach programs. The NIBIN Branch is currently

working with ATF's Office of Public Affairs to garner media press emphasizing the successes achieved throughout the United States in areas utilizing the ballistic imaging system to solve crimes. NIBIN Program staff continues to provide a presence at major law enforcement and forensic conferences, including the International Association of Chiefs of Police, the American Society of Crime Lab Directors, and the Association of Firearms and Toolmark Examiners. Additionally, ATF Special Agents in Charge regularly meet with local law enforcement and NIBIN coordinators and contractors provide roll call training to state and local law enforcement personnel to continue outreach programs. The NIBIN Branch is currently updating the website to provide the most up-to-date information on the program and NIBIN contractors are formulating "storyboards" to promote the significant successes achieved by agencies in their areas.

Issue: A May 2005 OIG report found that the Joint Automated Booking System (JABS) has made important progress by automating the booking process in the Department's law enforcement components, providing an automated interface with the FBI's fingerprint system, and providing basic data sharing between components. However, the audit determined that JABS does not fully reduce booking steps through data sharing as envisioned, resulting in component redundancy and duplication of effort. The audit also found that the offender tracking system was incomplete, which reduced agencies' ability to track offenders.

Action: The JABS Program Management Office (PMO) has initiated the USMS Data Integration Project and the Strategic Maturity Project to begin addressing the data sharing and federal offender tracking program goals. The development contracts for both projects will be awarded in the first quarter of FY 2006. Additionally, during the third quarter of FY 2006, the PMO will initiate the concept and requirements phase of the BOP Data Integration Project to further address these goals.

3. DEPARTMENT AND FBI INTELLIGENCE-RELATED REORGANIZATIONS

The Department's ability to effectively gather, analyze, share, and use intelligence information is critical to its success in meeting its counterterrorism and counterintelligence challenges. To better facilitate managing intelligence information, both the Department and the FBI are reorganizing their national security elements into new structures. This presents significant management challenges, including coordinating budget issues with the Director of National Intelligence, and new relationships with other federal, state, and local agencies.

Issue: A July 2004 OIG audit found that the FBI's collection of material requiring translation had outpaced its translation capabilities. In addition, the audit found that the FBI had difficulty filling its critical need for additional contract linguists and was not in full compliance with the quality control standards it had adopted for reviews of the work of FBI linguists. A July 2005 follow-up concluded that the FBI had taken steps to address the OIG's recommendations and had made progress in improving the operations of its foreign language translation program. However, key deficiencies remain in the FBI's foreign language translation program, including 1) a continuing backlog of unreviewed counterterrorism and counterintelligence material; 2) some instances where high-priority material has not been reviewed within 24 hours counter to FBI policy; and 3) continued challenges in meeting linguist hiring goals and target staffing levels.

Action: The OIG's July follow-up report is better understood in the context of the FBI's increased workload and prioritization of that workload. As noted in the report, the increase in the counterterrorism Financial Institution Supervisory Act (FISA) backlog represented a scant 1.5% of all counterterrorism audio collected. By contrast, the FBI's counterterrorism workload during the same time period increased by 52%. The sheer volume of information collected requires that the FBI manage language processing to ensure that the highest national security priorities are met. A five-tier prioritization system was created by a panel of representatives from the FBI, the Central Intelligence Agency, the National Security Agency, and the Department of Justice Office of Intelligence Policy and Review for managing and processing the collection of foreign language FISA material. This system ensures that the FBI manages its workload and the enormous volume of material collected against nationally determined priorities. As the OIG also noted, none of the FBI's counterterrorism audio backlog includes Tier 1, or highest-level priority cases. Additionally, the FBI analyzes all counterterrorism backlog identified in the monthly surveys to determine (1) whether the backlog is an issue of concern (or is empty microphones and white noise), or (2) whether the backlog is due to a lack of linguist resources (as in rare languages). This process has allowed the FBI to determine that more than half of the negligible counterterrorism backlog is likely white noise.

Regarding the issue of the FBI's review of high priority material within 24 hours, the FBI has been very successful in staying within those guidelines for its Tier 1 counterterrorism and other high priority cases. The OIG did note some randomly sampled cases that were not reviewed within 24 hours. However, as the FBI noted in its response, the material in both cases was fully reviewed in slightly more than 24 hours, and although the cases were denoted as Tier 1, they were also designated as medium priority within that tier. The FBI is committed to addressing its highest priority cases as quickly as possible and is making great strides as it continues to increase its linguist base.

The FBI is not alone in facing the difficult challenge of hiring sufficient numbers of qualified and clearable linguists. Even so, the FBI has been on track in meeting its hiring goals, having cleared 316 new linguists in FY 2005 and another 12 so far in FY06. Even with these successes, the greatest challenge lies in the fact that the FBI may only hire as many linguists as funding will allow. The FBI's ability to fully use its cleared linguist workforce and hire the additional linguists needed will depend in part on passage of the President 2006 budget request, which includes an additional 274 Language Specialist work years and \$5,000,000 in additional contract linguist funding. This funding is crucial if the FBI is to address all of its counterintelligence and criminal workload (in addition to counterterrorism), and also to dedicate sufficient resources toward quality control.

The FBI has successfully developed and expanded its Quality Control (QC) Program, particularly during and after the OIG follow-up audit. The FBI has made great strides in clarifying QC policies and procedures and training field offices, which have resulted in near universal compliance field-wide. In addition, the FBI has been conducting monthly QC training workshops, resulting so far in the training and recertification of 62 out of 200 designated QC reviewers.

4. INFORMATION TECHNOLOGY (IT) SYSTEMS PLANNING AND IMPLEMENTATION

The Department must ensure that investments in IT are well planned and aligned with the Department's overall IT strategy and enterprise architecture, and that components build systems that are interoperable with other component systems.

Issue: An ongoing OIG review is examining whether the Department is effectively managing its IT investments and developing an appropriate Enterprise Architecture (EA). Preliminary audit results indicate that, although the Department has not yet established processes for IT investment management or EA, it is actively developing and implementing new frameworks designed to support them. The audit noted, however, that these frameworks are limited because the Department is relying on component IT investment management and EA processes to support the overall Department-wide frameworks without ensuring the adequacy of the component-level frameworks. To do this, the Department must take a greater role in overseeing the completion of component IT investment management and EA processes.

Action: In August 2005, a new Deputy Chief Information Officer for the Policy and Planning Staff was hired to oversee the IT Investment Management (ITIM) program and the EA program. Furthermore, in September 2005, a Chief Enterprise Architect was hired to lead the Department's EA Program Management Office (EAPMO).

Under the leadership of these two individuals, the Department is expanding and enhancing the activities associated with these programs, with the goals of: better leverage of established Government-wide best practices and lessons learned; increased levels of guidance and coordination with DOJ component organizations; and greater maturity with EA efforts, as assessed within the GAO's Enterprise Architecture Management Maturity Framework (EAMMF) and OMB Effectiveness Assessment.

The EAPMO is developing a Program Management Plan (PMP) to ensure the EA Program is Department-wide and will leverage existing component EAs. The PMP will: identify milestones towards its implementation and completion; provide for explicit mechanisms to coordinate with and provide guidance to components for the development and maintenance of their EAs; use established Government-wide best practices such as use of federal EA Framework, GAO's EAMMF, and OMB's EA Effectiveness Assessment; and provide mechanisms for tracking and reviewing the planning, development, completion, and updating of component-level EAs.

The Department is continuing to refine and implement the IT Strategic Management Framework to ensure that all Department IT investments are covered by an ITIM process. The Department will define the need for component

ITIM processes based on criteria such as size, mission need, and percent of enterprise investment dollars. By the end of the third quarter of FY06, the Department will select components deemed necessary to have their own ITIM process, establish a working committee with Component representation, develop and provide guidance documentation for implementation, and implement a mechanism for measuring process maturity over time.

Issue: A February 2005 OIG audit identified a variety of causes for the problems in the FBI's IT modernization project, formerly known as Trilogy. These included poorly defined and slowly evolving design requirements, weak IT investment management practices, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on the project, unrealistic scheduling of tasks, and inadequate resolution of issues that warned of problems in Trilogy's development. The OIG report also faulted the FBI for moving forward with contracting for the Trilogy project without providing or insisting upon defined requirements, specific milestones, critical decision review points, and penalties for poor contractor performance.

Action: The FBI has established strong managerial and contractual mechanisms to define design requirements and identify poor contractor performance. As an example, the FBI has structured the SENTINEL Program in accordance with its Life Cycle Management Directive (LCMD) and structured the SENTINEL contract so that all or portions of the effort can be terminated upon identification of poor performance. Managerial and contractual mechanisms have been established to identify if the prime contractor is not performing. These mechanisms, strictly adhered to by the SENTINEL Program Management Office, include:

- A disciplined, stable, and well-conceived program management system that includes strict and full adherence to the FBI's new Information Technology LCMD and a best-of-breed PMO structure modeled on the program management system successfully used by the Central Intelligence Agency's Chief Information Officer organization.
- A risk management system that will identify contract performance risks and the status of steps being taken to mitigate them on a weekly basis.
- A schedule control and monitoring system that will identify variances in the contractor's schedule every two weeks.
- Requirements on both the prime contractor and the SENTINEL PMO to use a certified Earned Value Management (EVM) System, as well as the requirement to report on EVM status on a monthly basis which will identify variances in cost, schedule, and technical performance from the approved EVM baseline.
- Certification of these EVM Systems includes Independent Validation and Verification (IV&V) by an independent entity that the EVM systems are set up and performing in accordance with the United States national EVM standard.
- A rigorous Quality Assurance program, which includes IV&V of the quality control systems of both the prime contractor and the SENTINEL PMO.
- A rigorous configuration and change control system that is designed to control increases in the scope of technical requirements.

From an Investment Management perspective, significant progress has been made in the post Trilogy/VCF environment. The FBI has implemented the Clinger-Cohen Act requirements for establishing a Capital Planning and Investment Control process through its IT Investment Management Policy, signed by the Director in June 2005. This process for selecting, controlling, and evaluating IT Investments is now tightly integrated with the FBI's budget formulation and project management process and will ensure early identification of investments not meeting its cost, schedule, or performance goals.

Issue: The OIG has initiated an audit of Sentinel, the FBI's successor system to Trilogy's Virtual Case File. Preliminary work has identified several issues of concern that the FBI will need to focus on in order to successfully develop and deploy the Sentinel case management project. For example, the FBI's Sentinel Program Management Office is not yet fully organized and staffed with systems engineers, contracting officers, and budget personnel. Further, the Sentinel Program Manager, on loan from another agency, has committed to

two years with an option for a third year. Given the anticipated time frame for developing this project, the Program Manager may have to be replaced before Sentinel is completed and deployed.

Action: The FBI recognized and addressed the criticality of a properly staffed SENTINEL PMO by taking significant actions to properly formulate, establish, and staff the PMO. PMO roles and responsibilities are clearly articulated within the SENTINEL Program's Staffing Plan, providing organizational definition and focus for each staff member. The SENTINEL PMO is being established as a discrete section with lower level units within the Office of IT Program Management. The PMO Staffing Plan also defines the staff skill requirements, associated government and contractor PMO staffing levels, and actions for filling the PMO positions.

To execute the Staffing Plan, the FBI is mitigating risk to the program by forming an integrated team of subject matter experts from government, federally funded research and development centers, and systems engineering and technical assistance contractors. This approach maximizes program expertise, eases staffing burden for any one contractor, and affords the greatest flexibility in addressing known and unforeseen staffing requirements.

Regarding the SENTINEL program manager tenure, he is committed to serving three years on this program. The FBI also is building management depth in the program organization to ensure each part of the PMO has a trained backup to ensure continuity of the program.

Issue: In general, the FBI must ensure that it follows its IT investment management (ITIM) processes and that its projects are consistent with their EA. In addition, the FBI must fully staff a professional Program Management Office to ensure that approved IT projects meet cost, schedule, performance, and technical benchmarks.

Action: In accordance with the FBI's ITIM process, all investments are required to develop a full business case which includes an alternative analysis, life cycle cost estimate, baseline schedule, performance goals, and alignment with FBI/DOJ strategic goals and objectives, among others prior to becoming eligible to compete for IT funding. Once an IT concept is approved and funded it is subjected to the ITIM control process. On a monthly basis each major and non-major IT investment is required to submit actual cost, schedule, and performance data used by the OIPP/Project Assurance Unit to assess the health of the project. Those investments that are not achieving 90% of its cost, schedule, or performance goals, are reviewed by FBI Assistant Directors at the Investment Management Project Review Board. This early identification of underperforming investments ensures that appropriate management attention is given to t-risk projects in time to affect positive change or de-select the investment. Through adherence to this process the FBI is successfully mitigating the risk that another VCF project will be allowed to progress to completion.

The Office of IT Program Management (OIPM) is the organization within the Bureau responsible for managing approved IT projects. This office is staffed with a cadre of qualified program management professionals (assisted by OIPM Contracting Officer Technical Representatives) who are responsible for leading all the activities required to ensure successful program execution. These activities include program planning, management, control, reporting, and systems development and deployment and are conducted under the framework of the LCMD.

Issue: The Office of Management and Budget (OMB) has established June 2008 as the date by which all federal agencies' infrastructures must use the IPv6 Internet protocol. However, a May 2005 audit by the General Accountability Office (GAO) found that the Department had not yet initiated key planning considerations for transitioning to IPv6. In particular, the GAO found that the Department did not: 1) develop a business case, 2) have a transition plan, 3) inventory their IPv6-capable equipment; or 4) estimate transition costs.

Action: OMB issued policy memorandum M-05-22, dated August 2, 2005, regarding agency transition planning for IPv6. In response to this guidance, the DOJ OCIO initiated proactive measures to ensure DOJ compliance. Specifically, the OCIO has assigned an official lead to coordinate agency IPv6 planning and has issued a data call to all DOJ component CIOs in order to complete the required initial inventory of network backbone routers, switches, and hardware firewalls by November 15, 2005. Simultaneously, the OCIO has begun efforts to compile a detailed inventory of all IP-aware devices, develop a formal IPv6 transition plan, and perform an impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6. Additionally, the OCIO has proactively reached out to OMB, Department of Education, Department of Commerce, Department of Defense and Central Intelligence Agency IPv6 transition offices in order to facilitate interagency coordination,

collaboration, and cooperation in meeting this OMB mandate. IPv6 will remain a key priority for the OCIO and every effort will be made to ensure compliance with the OMB mandated June 30, 2008, transition objective.

5. INFORMATION TECHNOLOGY SECURITY

The Department must ensure that its systems are secure, even though its networks and databases are at continual risk from unauthorized access as hackers and potential terrorists develop new techniques to breach government computer systems.

Issue: *OIG FY 2004 testing found that the Department did not always perform verification of component data collected for Federal Information Security Management Act (FISMA) reports. In addition, the OIG found that the FBI, the DEA, and the U.S. Marshals Service did not have proper tracking systems in place to ensure that all of their employees received computer security awareness training and education. The OIG also found that these components had not ensured that contingency plans for all certified and accredited systems were tested. In addition, the components insufficiently tracked vulnerabilities previously identified and corrective actions already taken for their IT systems. Moreover, the OIG found that the FBI had not certified and accredited 6 of its 15 systems (40 percent) as reported in the OIG's FY 2004 FISMA review.*

Action: Coordination with Department components has been enhanced through the application of an automated Report Card, grading all activities against a common norm stated in the DOJ Program Management Plan and in support of the President's Management Agenda. The process has been simplified through the implementation of automated tools for improving the visibility of accomplishments, areas needing additional efforts, and for the gathering of reportable data. These results were reflected in the Department's Congressional Report Card Grade issued in February 2005, which was a B-.

The IT Security Staff continues to refine its program and staff to include DOJ component client representatives who serve as both liaisons with the component IT staffs and as validations of information and actions completed by the components. In FY 2005, the Department CIO reported 97% of DOJ's 215 systems were independently validated and 99% of the Department systems were certified and accredited in the annual FISMA Report. The OIG further validated the Department's program by identifying the Department does have an agency-wide security configuration policy and the Department's certification and accreditation process is "Good."

The IT Security Staff and component IT security personnel were diligent in overseeing the enterprise-wide computer security awareness training course for all participating components, which included DEA and U.S. Marshals Service for the first time in FY 2005. That effort, accompanied by the strengthening of FBI's awareness program execution, brought improved control to the process and a completion rate of over 96% in security awareness training. Several training workshops, departmental exercises, and contingency plan reviews resulted in over 99% of contingency plans tested.

The IT Security Staff evaluated, procured, and implemented an enterprise-wide-scanning tool. The Program Management Plan now requires weekly vulnerability scanning and monthly reporting to the Department. Corrective action planning/execution for all resulting "high risk" findings over 30 days old, must be identified in a Plan of Action and Milestones (POA&M). The IT Security Staff closely monitors these results and provides immediate feedback to components via the Report Card.

In FY 2006, continued emphasis will be placed on implementing corrective action on identified weaknesses, increasing vulnerability scanning and mitigation of high vulnerabilities, implementing the National Institute of Standards and Technology (NIST) 800-53, Recommended Security Controls for Federal Information Systems, and ensuring 90% of the Department's IT assets have secure configuration.

DEA uses a Computer Based Training (CBT) application, which was provided by DOJ, to meet the DOJ Program Management Plan's (PMP) standard of providing the requisite computer security training to 96% of the DEA work force, including DEA government, contract, task force officer, Department of Defense and other federal law enforcement or intelligence counterparts as assigned. At the end of FY2005, 98% of the DEA work force successfully completed the security CBT.

All DEA certified and accredited systems have contingency plans and were tested during FY2005. Contingency

