Top Management Challenges in the Department of Justice 2004

November 22, 2004

The Honorable James Sensenbrenner
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable John Conyers
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman and Congressman Conyers:

Enclosed is the Office of the Inspector General's (OIG) 2004 list of top management challenges facing the Department of Justice (Department). The challenges are not presented in order of priority - we believe that all are critical management issues facing the Department. However, similar to recent years' lists, it is clear to us that the top challenge facing the Department is its ongoing response to the threat of terrorism. Several other top challenges are closely related to and impact directly on the Department's counterterrorism efforts.

Eight of the challenges from last year's list remain. They are long-standing, difficult challenges that will not be solved quickly or easily. However, we note in the accompanying analysis that the Department is making progress on many of these complex issues. Two challenges from last year's list have been replaced by two other challenges. We removed "Performance Based Management" and "Protecting the Security of Department Information and Infrastructure" this year and added two new challenges - "Detention and Incarceration" and "Forensic Laboratories."

We hope that this list and the accompanying analysis will assist your Committee in its oversight responsibilities. We look forward to continuing to work with the Committee to address these important issues.

Sincerely,

Glenn A. Fine
Inspector General

Enclosure

(similar letter sent to the Chairman and Ranking Member of the Senate Committee on the Judiciary)

---

1. Counterterrorism: The Department of Justice's (Department) clear and consistent highest priority this year - as it has been since the terrorist attacks of September 11, 2001 - is to deter, prevent, and detect future terrorist acts. The Department's Strategic Plan for fiscal years (FY) 2003-2008 notes the challenges facing the Department as it seeks to effectively manage its varied counterterrorism programs while coordinating its efforts with other intelligence and law enforcement agencies. To accomplish this mission, the Department receives billions of dollars in

appropriated funds, creating a challenge for Department managers to ensure that these funds are spent in an effective manner. As the OIG issues this list of Top Management Challenges in October 2004, Congress is debating far-reaching proposals to restructure the United States Intelligence Community that would significantly impact programs and personnel in the Department, particularly in the Federal Bureau of Investigation (FBI).

Because of the importance of this challenge, the Office of the Inspector General (OIG) continues to examine Department programs and operations related to counterterrorism. We also attempt to follow-up on previously issued reviews to determine whether Department components have taken action in response to the recommendations. During the past year, the OIG reviewed counter-terrorism-related issues in a variety of Department components, including the FBI's handling of certain intelligence information prior to the September 11 terrorist attacks, the FBI's foreign language translation program, the FBI's reassignment of staff since the September 11 terrorist attacks to counter-terrorism matters, and the readiness of United States Attorneys' Offices (USAO) to mount an effective response to terrorist attacks or other critical incidents in their districts.

A July 2004 OIG audit examined the FBI's progress in translating critical foreign language material, its success at meeting its linguist hiring goals, its procedures for prioritizing translation work, and its efforts to ensure quality translations and appropriate security screening of FBI linguists. The OIG found that since September 11, 2001, funding for the FBI's foreign language program has increased from $21.5 million in FY 2001 to nearly $70 million in FY 2004, and the number of linguists has grown from 883 to 1,214. At the same time, the FBI's electronic surveillance collection in languages primarily related to counterterrorism activities (such as Arabic, Farsi, Urdu, and Pashto) has increased by 45 percent and is expected to increase by at least 15 percent annually.

Our audit found that the FBI's collection of material requiring translation outpaced its translation capabilities and the FBI did not translate all the foreign language counterterrorism and counterintelligence material it collected. We attributed the FBI's backlog of unreviewed material to its insufficient number of linguists as well as limitations in the FBI's translation information technology (IT) systems. For example, the FBI's digital collection systems have limited storage capacity and consequently unreviewed audio sessions are sometimes deleted automatically to make room for incoming audio sessions. With respect to quality control, we found that the FBI generally did not complete required reviews for newly hired linguists and annual reviews for its on-board linguists.

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

Following up on a September 2003 audit of the FBI's Casework and Human Resource Allocation, the OIG took a closer look at the FBI's efforts to reprioritize and refocus its investigative resources in the aftermath of the September 11 terrorist attacks. This follow-up review, issued in September 2004, describes the changes in the FBI's reassignment of staff to counter-terrorism and counterintelligence matters from investigations of traditional criminal matters. The OIG report provides detailed statistical information regarding investigative areas that gained or lost personnel from FYs 2000 to 2003. In addition, the OIG review identifies field offices most affected by changes in FBI priorities within these investigative areas, such as shifting agent resources from organized crime or health care fraud cases to terrorism investigations.

The report showed that since the September 11 terrorist attacks, the FBI has reprioritized its mission and shifted substantial resources from investigating traditional crimes to matters related to terrorism. The report's detailed statistical review showed that FBI investigative activities were in line with its post September 11 priorities.

The OIG report recommends 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.

In another OIG review, initiated at the FBI Director's request, the OIG reviewed the FBI's handling of intelligence information prior to the September 11 terrorist attacks. This review concentrated on analyzing the FBI's handling of: 1) a July 2001 memorandum from the FBI's Phoenix field office expressing concerns about persons of interest in terrorism investigations who were enrolled in aviation-related training; 2) the Zacarias Moussaoui investigation; and 3) information about two of the September 11 terrorists - Nawaf al-Hazmi and Khalid al-Mihdhar.

The OIG issued a 421-page report in July 2004, classified at the Top Secret/SCI level, which was provided to the FBI, the National Commission on Terrorist Attacks Upon the United States, and congressional oversight committees. The OIG report made several recommendations about the process the FBI uses to obtain wiretap and search authority pursuant to the Foreign Intelligence Surveillance Act (FISA). The FBI responded by outlining training efforts related to the FISA process, such as training in field offices, conferences, and "distance learning courses." The FBI also stated that it has significantly increased the number of attorneys working on FISA-related matters and reorganized the unit within its Office of General Counsel that handles counterterrorism to ensure routine contact between agents, analysts, and attorneys.

Also in response to the OIG report, the FBI noted that it is in the process of revamping its analytical program by creating its Office of Intelligence, which will be responsible for recruiting, hiring, developing, and training intelligence analysts. The FBI also created the College of Analytic Studies to provide basic training for newly hired analysts and specialized training for experienced analysts. In addition, the FBI reported that it is working to improve coordination and consultation between operational and analytical units within the FBI. The OIG currently is reviewing the FBI's efforts to hire and train analysts.

The Department's response to terrorism requires the resources of many Department components, not solely the FBI. An OIG review issued in December 2003 underscored the need for the entire Department to be prepared to respond to a terrorist incident or other emergencies, should it occur. The OIG reviewed the USAO's implementation of the Crisis Management Coordinator Program (CMC Program). This review assessed the training provided to USAO staff, exercises conducted to respond to critical incidents, and critical incident response plans developed by the USAOs. In addition, the review examined the administration and support provided to the CMC Program by the Criminal Division's Counterterrorism Section (CTS) and the Executive Office for United States Attorneys (EOUSA). The OIG review found that the CMC Program had not been adequately implemented to ensure that USAOs are prepared fully to respond quickly and appropriately to terrorist attacks or other critical incidents, such as large-scale crimes or natural disasters. We found that although the CTS, EOUSA, and the USAOs have taken significant steps to improve the Department's ability to prevent terrorist attacks, a commensurate need existed to be prepared to respond effectively to terrorist attacks and other critical incidents should prevention efforts fail. We concluded that these deficiencies left the Department less prepared than it could be - and should be - to respond when terrorist attacks or other critical incidents occur.

However, during the review and since issuance of our report, the Department has made significant progress in addressing the problems described. For example, as of July 14, 2004, 88 of the 93 USAOs had submitted revised critical incident response plans to the EOUSA and the remaining USAOs were to have submitted their plans by the end of August 2004. In addition, the Department formed a Critical Incident Working Group to review these revised crisis response plans and provide USAOs with individualized feedback.

A continuing challenge for the Department in responding to the heightened terrorism threat is to

use its varied law enforcement and intelligence-gathering authorities in a manner that respects the civil rights and civil liberties of potential subjects or witnesses. In September 2004, the OIG issued its fifth report to Congress as required under Section 1001 of the USA PATRIOT ACT. The report described the status of OIG and Department investigations of alleged civil rights and civil liberties abuses by Department employees. During the most recent reporting period, the OIG identified 13 new matters of varying seriousness that warranted opening an investigation or conducting a closer review. The OIG opened three new Section 1001-related investigations based on these complaints and forwarded ten allegations to Department internal affairs offices for their review.

In addition, the report highlighted several OIG reviews that have been completed or undertaken in furtherance of our Section 1001 responsibilities, including a review of the Federal Bureau of Prisons' (BOP) process for selecting Muslim religious services providers and an ongoing review of the FBI's implementation of Attorney General Guidelines that govern general crimes and criminal intelligence investigations.

With regard to past reviews concerning civil rights and civil liberties issues, the Department continues to take positive steps to implement recommendations from the OIG's June 2003 report that examined how the Department treated certain aliens arrested in connection with its September 11 terrorism investigation. Specifically, the Department has implemented changes to increase the sharing of information among law enforcement agencies about individuals arrested in connection with terrorism investigations. The Department also has developed new procedures relating to the handling of these individuals in federal detention facilities. In addition, the Department continues to negotiate a Memorandum of Understanding (MOU) with the Department of Homeland Security (DHS) regarding policies and procedures for managing a national emergency that involves alien detainees.

The OIG currently is reviewing several other critical counterterrorism-related Department programs, including the progress of the FBI's Terrorist Screening Center, an entity charged with consolidating various terrorist watch lists and providing support to thousands of federal screeners across the country and around the world. In addition, the OIG is assessing how well the ATF has implemented provisions of the Safe Explosives Act (part of the Homeland Security Act of 2002) that require it to implement expanded licensing and inspection requirements for individuals who manufacture, sell, or use explosives.

In a follow-up audit examining the Department's Counter-terrorism Fund (Fund), we found that the Department's Justice Management Division had made improvements in its administration of the Fund. Our testing of expenditures for reasonableness, appropriateness, compliance with legislation, and adequacy of supporting documentation revealed a reduction in the error rate of Fund usage and payment compared to our previous audit.

In sum, the counterterrorism challenge is great and the task is continual. Due to the importance of and difficulties associated with detecting and deterring terrorism, and the large amounts of money committed to the Department's anti-terrorism efforts, counterterrorism remains a top Department management challenge.

2. Sharing of Intelligence and Law Enforcement Information: In response to the September 11 terrorist attacks, the Department has sought to ensure that information exposing a credible threat to the national security interests of the United States should be shared with appropriate federal, state, and local officials. The Department has focused resources and attention on enhancing its ability to share information. This remains a difficult challenge, however, given the multitude of federal and state entities that seek access to intelligence and law enforcement information as well as the sensitive nature of much of the information. Nevertheless, the ability to share intelligence and law enforcement information timely and effectively is critical to the Department's success in preventing future acts of terrorism.

   The OIG reported on the FBI's efforts to improve the sharing of intelligence and other information in December 2003. We found that among the FBI's main obstacles to effective information sharing were the need to improve its IT systems, enhance its ability to analyze intelligence, overcome security clearance and other security issues concerning the sharing of information with state and

local law enforcement agencies, and develop policies and procedures for managing the flow of information.

Since the report's issuance, the FBI has taken action to address the report's recommendations. The FBI has drafted an Intelligence Dissemination Policy Manual to provide consistent procedures for information sharing, including what types of information should be shared with what parties under what circumstances; completed a blueprint and process map for intelligence and information sharing; and revised its policy for Urgent Reports which are submitted by field offices to the FBI Director regarding critical matters requiring immediate attention. We believe the FBI still needs to develop implementation plans for its Intelligence Concept of Operations Plans that include budgets, time schedules, and designation of responsible officials. These Concept of Operations Plans provide a framework and vision for improving each of nine core intelligence functions defined by the FBI.

As noted above, the OIG recently completed an examination of the FBI's handling of intelligence information in its possession prior to the September 11 terrorist attacks. Several recommendations in the OIG's report addressed information sharing between the FBI and the Intelligence Community. In response to these recommendations, the FBI provided information about specific steps it has taken to: 1) improve the management of FBI employees detailed to other agencies; 2) ensure that FBI employees who interact with other intelligence agencies better understand those agencies' intelligence-reporting processes; and 3) improve its technological capabilities as they relate to information sharing. The FBI also reported that it has begun to develop intelligence collection and reporting guidance for field agents and has developed a training course dedicated to reporting and disseminating raw intelligence.

The OIG continues to examine the status of efforts to integrate the DHS's automated fingerprint identification database (IDENT) with the FBI's automated fingerprint identification database (IAFIS). In a report issued in March 2004, the OIG examined the actions of immigration employees in a case that reinforced the need to integrate the IDENT and IAFIS databases as expeditiously as possible in order to enable sharing of critical information. The report examined the case of Victor Manual Batres and the impact of the failure to fully integrate IDENT and IAFIS. In January 2002, the Border Patrol apprehended Victor Manual Batres twice in two days after he attempted to illegally enter the United States. Instead of being detained because of his extensive criminal record, he was returned to Mexico and subsequently succeeded in illegally crossing the border. In September 2002, he brutally raped two Catholic nuns in Oregon, killing one of them. Although we found that some of the agents and supervisors who apprehended Batres failed to follow Border Patrol policies, we concluded that individual agents will not be able to determine consistently the full criminal histories and prior deportations of all aliens they apprehend until they can query simultaneously both IDENT's immigration records and IAFIS's FBI fingerprint records.

Our report found that integration of these databases has been advancing slowly, in part because of uncertainty over who is responsible for managing the project now that the former Immigration and Naturalization Service (INS) has transferred to the DHS. According to the agencies' own projections, full integration of IDENT and IAFIS was not scheduled to occur for several years. Moreover, the Department and the DHS had not entered into an MOU on the specific roles, responsibilities, and funding to complete the integration project.

Since issuance of our report, the Department and the DHS have made some progress towards full integration. For example, the FBI began providing daily wants and warrants extracts from IAFIS in May 2004 rather than the prior bi-weekly extracts. In addition, as of September 2004 the Department was seeking a contractor to develop technology to capture more quickly and accurately ten rolled fingerprints or palm prints. However, an MOU between the Department and the DHS still has not been developed, and significant outstanding issues remain regarding who should be subjected to fingerprint searches, the standard fingerprint collection procedures to use, the databases to query, who will have access to the information collected and how the information will be used, and who will maintain the databases.

In another review, the OIG examined the ATF's and FBI's arson and explosives intelligence databases used to collect and disseminate intelligence about arson and explosives cases. We found that state and local bomb squads, fire departments, and law enforcement agencies do not

report arson and explosives incidents consistently to the FBI or the ATF. Further, we found that the Department had not efficiently and effectively collected information relating to arson and the criminal misuse of explosives and did not make it available to the federal, state, and local law enforcement community. The similar responsibilities of the ATF and the FBI in compiling data resulted in duplication of effort, confusion, and duplicate reporting by state and local agencies. As a result, customers do not have a single, comprehensive source for obtaining intelligence information on arson and explosives matters to assist in their investigations. On August 11, 2004, the Attorney General directed the ATF and the FBI to consolidate the Department's databases on arson and explosives incidents into databases that will be maintained by the ATF.

The OIG's review of the treatment of the September 11 detainees also identified certain weaknesses in Department information sharing. 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 is working with the DHS to develop an MOU that would govern the detention of aliens of national security interest. As of October 2004, the MOU had not been finalized.

Several ongoing OIG reviews examine other aspects of the Department's critical information-sharing challenge. For example, as noted above, the OIG is reviewing the FBI's Terrorist Screening Center (TSC) that was established in September 2003 to consolidate various agencies' separate "watch lists." The OIG is examining the TSC's coordination with participating agencies and determining if the TSC is appropriately managing the terrorist-related information to ensure that a complete, accurate, and current watch list is developed and maintained.

Another OIG ongoing review is assessing the implementation of the Department's Joint Automated Booking System, an information-sharing system and a conduit for sending standard booking data directly to the FBI's IAFIS system. We also recently began an audit of the ATF's National Integrated Ballistic Information Network Program, which is 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.

Overall, the Department continues to make improvements in the way it shares intelligence with other federal, state, and local law enforcement entities. However, the critical but paradoxical need to disseminate information more widely while maintaining appropriate security makes this issue a continuing top management challenge. The Department needs to commit sustained effort to ensure the progress of its efforts to effectively, securely, and timely share appropriate intelligence and law enforcement information.

3. Information Technology Systems Planning and Implementation: The Department continues to face significant challenges in ensuring its IT systems are developed and deployed in a timely and cost-effective manner. These complex and often-interrelated IT systems play a vital role, for example, in consolidating and maintaining terrorist watch lists, sifting through thousands of leads in terrorism and criminal investigations, and developing annual financial statements. The Attorney General recognized the importance of IT planning and implementation by citing utilization of technology to improve government as one of the Department's ten management goals. Management of Department IT investments has been a Department material weakness since FY 2002.

   In April 2002, the Department selected a new Chief Information Officer (CIO) responsible for leading and implementing effective acquisition and management of IT across the Department. The CIO manages the Department's $2.1 billion IT program, overseeing management, acquisition, and integration of the Department's information resources. His oversight includes strategic planning, policy, capital planning, systems development, telecommunications, information security data management, enterprise architecture, e-government, and user computing.

   Over the past two years, the CIO has completed a major reorganization of his office intended to align the Department's IT strategy with its counterterrorism and information sharing strategic plans. He also has sought to upgrade skills to ensure that the Department can effectively manage major IT areas, such as enterprise architecture, security, project management, business process

re-engineering, and e-government. To assess the Department's progress in these areas, the OIG plans to examine the Department's centralized efforts related to enterprise architecture and IT investment management in FY 2005.

During that same two-year period, the OIG issued reviews of IT planning and implementation in two major Department components - the Drug Enforcement Administration (DEA) and the FBI. In a September 2004 review, we found the DEA is making solid progress towards developing Enterprise Architecture and IT investment management processes. When completed, the DEA's Enterprise Architecture will provide an agency-wide roadmap to achieve the DEA's mission through an efficient IT environment. However, the DEA has 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 has not established a schedule for fully developing all IT investment management practices.

Similarly, the OIG has continually examined the FBI's IT acquisition and management of its IT projects. We found that while the FBI is making progress, it needs to continue to focus attention on these issues given their complexity and importance to the FBI's overall mission. In a review in December 2002, the OIG concluded that the FBI was not effectively selecting, controlling, and evaluating its IT investments because it had not fully implemented any of the critical processes necessary for successful IT investment management. As a result, the FBI was spending hundreds of millions of dollars on IT projects without having adequate selection and project management controls in place to ensure that IT projects would meet intended goals.

In September 2003, the OIG examined the FBI's implementation of IT recommendations and found that the FBI had implemented many of them (93 out of 148). However, we concluded that further action was necessary to ensure that the FBI's IT program effectively supports its mission. Current FBI leadership has stated that it is committed to enhancing controls to ensure recommendations are implemented in a consistent and timely manner. Most significantly, the FBI has reorganized the IT function and created the Office of the Chief Information Officer to manage centrally all IT responsibilities, activities, policies, and employees across the FBI.

The OIG is closely following the development and implementation of Trilogy, the FBI's most ambitious and costly IT modernization initiative. An ongoing OIG follow-up audit is examining the cost, schedule, technical, and performance baselines for the Trilogy project. One critical component of Trilogy will replace the FBI's archaic and limited Automated Case File System (ACS) with the Virtual Case File (VCF). When implemented, the VCF will enable the FBI to more efficiently manage its criminal cases and allow more efficient sharing of information agency-wide, thereby assisting the FBI to "connect the dots" and piece together seemingly disparate information on possible terrorist plots.

We remain concerned, however, about the FBI's ability to timely complete the Trilogy project. While the infrastructure portions of Trilogy such as hardware and communications networks were completed on April 30, 2004, completion of the VCF and user applications has been problematic. Development of Trilogy has been plagued with missed deadlines and escalating costs, and firm schedule baselines were never established for much of the project's history. Costs increased from an original estimate of $380 million to $581 million by FY 2003. Given the importance of the issue, in FY 2005 the OIG will continue to monitor the FBI's efforts to modernize its IT systems and implement user applications such as the VCF.

4. Computer Systems Security: Another critical challenge is the security of the Department's critical IT systems and information. Since FY 2001, the OIG has performed security assessments and penetration testing of Department computer systems, as initially mandated by the Government Information Security Reform Act and as of December 2002 by the Federal Information Security Management Act (FISMA). Under FISMA, the OIG performs an annual independent evaluation of the Department's information security program and practices, and reports the results to the Office of Management and Budget (OMB). Our reviews have found that the Department continues to make progress in improving its IT security.

   Our FY 2003 FISMA consolidated audit of the Department's IT security oversight found

vulnerabilities as well as progress in other areas. As a continuing vulnerability, we found that formal policies and procedures were not established for monitoring component adherence to Department policies. In addition, the Department's database for tracking vulnerabilities in sensitive but unclassified systems contained erroneous or missing data, while such a tracking database for classified systems did not even exist. We also found that the Department did not perform sufficient oversight with respect to the components' corrective action plans to remedy identified vulnerabilities.

However, the Department has responded to these findings by improving its IT security process and revamping its IT security personnel staff and system certification and accreditation process. The Department also enhanced its vulnerability tracking capability and implemented documented structured compliance evaluation procedures for both classified and sensitive but unclassified systems. The Department now has a procedure in place to ensure that changes to IT systems are effectively tested before being placed into production. Furthermore, the Department enforces timely reporting of computer security incidents and conducts a review of Department systems to determine if re-certification is needed after a major incident occurs.

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.

5. Financial Management and Systems: The Department received a disclaimer of opinion for FY 2004 on its consolidated financial statements. The reason for the disclaimer was that one Department component, 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 overall consolidated opinion. A second component, the ATF, received a qualified opinion for FY 2004. All other Department components received unqualified opinions.

   In FY 2004, the Department faced significant challenges because of the accelerated reporting timetables and the need to correct longstanding financial and accounting control issues. In FY 2004, the number of material weaknesses and reportable conditions at both the consolidated and component levels increased. The consolidated report included two material weaknesses and one reportable condition, up from one material weakness and one reportable condition last year. For the components, the number of material weaknesses and reportable conditions at the component level increased to 23 from the 19 reported last year. The ten material weaknesses reported for FY 2004 represent an increase of one material weakness from FY 2003.

   The Department's financial controls remain a serious management challenge. 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 FY 2002, the Department initiated the Unified Financial Management System project to replace the seven major accounting systems currently used throughout the Department in an effort to address these and other deficiencies. Currently, none of the Department's accounting systems are integrated with each other. Consequently, production of Department-wide information must be done manually or by duplicative inputting of data from one system into another.

   Several of the older systems in use by Department components predate the current accounting requirements and do not support the production of timely, relevant information that is needed for preparing financial statements or performing accrual accounting transactions. For example, as we pointed out in last year's list of top management challenges, property transactions in several components are entered into separate accounting and property systems - systems that need to be reconciled periodically, often manually and sometimes line-by-line.

   The Department continues to perform too many tasks manually because of the lack of adequate automated systems. In FY 2003, the Department intended to expedite its reporting by one month but was unable to do so because of the extraordinary manual efforts it took to complete the year-end audit. Such manual efforts are not only costly because they are so labor intensive, but they also compromise the Department's ability to prepare financial statements that are timely and

in accordance with generally accepted accounting principles.

While the vendor for the unified system was selected in FY 2004, little progress has been made in implementing the new system. 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 remains limited.

Financial statements are now required quarterly, not just at year-end. Consequently, financial information must be kept up-to-date throughout the year to enable preparation of full accrual quarterly statements and to ensure Department managers are provided information on an ongoing basis to allow them to most effectively manage the Department's resources. Importantly, auditors must be able to test and rely upon the components' internal control processes throughout the year.

For OJP, the auditors were not able to test and rely upon significant controls at interim testing periods because of the material weaknesses identified in financial management system controls, documentation problems, and the inability of OJP to support major account balances related to grant accrual. For ATF, there was insufficient time at year-end to complete the testing on the accounts payable accrual because of the material weakness identified in the process for recording accounts payable.

Beginning in FY 2004, component audits must be completed within 20 days of the end of the fiscal year in order for the Department to successfully meet the OMB's accelerated deadlines. As the OIG has reported in previous years, the key to success in meeting the expedited timelines 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.

6. Grant Management: Managing the Department's more than $5 billion in grant programs remains a top management challenge. The Attorney General has recognized the importance of this challenge by listing restructuring OJP and reforming grant management as one of the Department's Ten Management Goals.

   The Department is making progress in its management of its grant programs. An August 2003 OIG audit examined activities and functions in OJP and the Office of Community Oriented Policing Services (COPS) that could be streamlined to increase the operational efficiency of the Department's federal financial assistance programs. As a result of that audit, the COPS Office and OJP are working together to finalize a written agreement specifying the process for identifying proposed programs and grants that have similar purposes to ensure awards are not made to grantees for similar efforts. In addition, the COPS Office is moving towards an on-line application capability for all COPS grants by the end of FY 2005, and OJP is making progress towards full automation of its grant process from application to closure by the end of FY 2004.

   For its part, the OIG continues to review individual grantees as well as the Department's management of its myriad grant programs. We found areas that need further improvement. For example, in June 2004 we issued a Management Information Memorandum to the COPS Office concerning a lack of program-specific guidance in its technology grant program. We cited as examples the lack of a grant owner's manual and the COPS Office's awarding of multi-year extension of grants without requiring grantees to report on their progress in meeting program goals.

   In a September 2004 audit, the OIG examined the OJP's Technical Assistance and Training Grant Program to determine if OJP implemented internal control measures to ensure accurate financial reporting by grantees. We 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.

   With respect to OJP, we found that grant managers did not ensure that all required Financial Status Reports and Progress Reports were submitted timely and accurately. Further, other monitoring requirements were not being adhered to, and communications between grantees and

grant managers were not documented properly.

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. In addition, we 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 with the report's recommendations and agreed to take corrective actions by the end of FY 2005 to strengthen its grant administration process.

7. Detention and Incarceration: The BOP and the United States Marshals Service (USMS) are the two Department components responsible for providing detention space, programs, and health care for long and short-term incarceration. Obtaining detention space at reasonable cost and efficiently managing that space remains a top management challenge for the Department. In addition, the Department's aggressive efforts over the past three years to investigate and prosecute terrorism suspects present new challenges for these two components in housing these individuals.

   As of September 30, 2004, the BOP housed 179,895 inmates in 104 facilities across the country. The BOP's FY 2005 budget request of $4.7 billion represents 24 percent of the total Department budget and ranks above the budget requests of the DEA, USMS, ATF, and only slightly below that of the FBI.

   The USMS is responsible for individuals arrested by federal agencies, as well as for housing and transporting these individuals from the time they are brought into federal custody until they are either acquitted or incarcerated.

   In recent years, the number of federal detainees increased at an annual rate of almost 12 percent between 1994 and 2003. As of July 31, 2004, 52,951 detainees were in the custody of the USMS. The Department has attributed the growth in detainees to new law enforcement initiatives, Departmental and agency policies, and laws enacted by Congress that result in increasing numbers of arrests or apprehensions of individuals suspected of violating federal laws.

   Last year, due to the transfer of the INS to the DHS, we removed "incarceration and detention" as a top Department management challenge. However, with the current crowding rate in federal prisons and problems noted in our audits and reviews relating medical contracting costs, detention and incarceration is again a top management challenge.

   The BOP's current overcrowding rate is 33 percent, according to the Department's FY 2003 Accountability Report. Overcrowding increases the risk of injuries to staff and inmates. It also increases the difficulty of providing inmates and detainees education and rehabilitation services that can improve their chances of successful reentry into society.

   Provision of adequate medical care to inmates and detainees is part of this critical challenge. In a February 2004 review, we examined the USMS provision of medical care to the prisoners in its custody. In-house medical care includes health care provided at local jail clinics and in some cases emergency care provided in USMS facilities. Our review concluded that the USMS is not properly managing its prisoner medical care. We found that USMS districts are not adequately tracking and monitoring communicable diseases, such as tuberculosis, hepatitis, and HIV/AIDS; not taking sufficient action needed to ensure that federal prisoners housed in local detention facilities are receiving standard basic health care; not providing adequate emergency response to prisoners housed in their cellblocks; and not properly reviewing the performance and billings of hospital guard contractors. We also found that by failing to comply fully with statutory cost saving measures, the USMS is paying out approximately $7 million more annually than is necessary for prisoner medical care.

   The OIG recommended that the USMS complete its ongoing effort to negotiate a national managed health care contract for prisoner medical services that would streamline the administration of prisoner medical care. The USMS reported that as of September 2004 its Technical Evaluation Board had submitted its report to the USMS contracting office and an award is anticipated by November 1, 2004. The USMS also informed us that the necessary funding has been committed by the Office of the Federal Detention Trustee (OFDT).

In a detention issue involving non-citizens, 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. For example, we found that certain conditions of confinement at the MDC were unduly harsh, such as illuminating the detainees' cells for 24 hours a day. Further, we found that MDC staff failed to inform detainees in a timely manner about the process for filing complaints about their treatment.

In our December 2003 supplemental report, we found that some MDC staff physically abused some of the detainees. In addition, we found systemic problems at the MDC related to the treatment of these detainees, including inappropriate use of strip searches. We recommended discipline for several MDC staff members. In response, the BOP has taken responsible actions to address the systemic recommendations, including: 1) modifying its training of prison staff on the appropriateness of specific techniques for escorting inmates; 2) providing guidance to prison staff on the general prohibition on audio monitoring of communications between inmates and their attorneys; and 3) implementing policies on videotaping incoming high-security inmates and documenting injuries to inmates. In addition, the BOP is in the final stages of formulating revised policies on strip searching inmates and on selecting and training officers to handle high-security and sensitive inmates. The BOP also is evaluating our discipline recommendations for MDC staff members.

In response to concerns from several members of Congress about how the BOP selects Muslim chaplains to serve in its institutions, the OIG reviewed the recruitment, endorsement, selection, and supervision of Muslim religious services providers who work with BOP inmates. We found that the BOP typically did not examine the doctrinal beliefs of applicants for religious services positions to determine whether their beliefs are inconsistent with BOP security policies, nor did the BOP and the FBI adequately exchange information on the organizations the BOP relies on to endorse candidates who provide religious services to Muslims.

The OIG also found that because of a shortage of Muslim chaplains, inmates often lead Islamic services subject only to intermittent supervision from BOP staff members. This greatly enhances the likelihood that radical, inappropriate messages could be delivered to inmates. Within the BOP's chapels, the OIG found that significant variations exist in the level of supervision correctional officers provide. Further, once contractors and certain volunteers gain access to BOP facilities, ample opportunity exists for them to work without direct supervision from BOP staff and to possibly deliver inappropriate messages. Our report provided recommendations to assist the BOP in improving its process for selecting, screening, and supervising Muslim religious services providers.

Since issuance of the report, the BOP has taken steps to implement the recommendations. For example, the BOP is developing enhanced screening criteria for religious services providers and will require that each future chaplain candidate be interviewed by a BOP chaplain who is knowledgeable about the applicant's faith group and its practices. To improve information sharing with the FBI on inmate radicalization issues, the BOP is recruiting 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 BOP also said it planned to strengthen its ties to local FBI Joint Terrorism Task Forces, consistent with the report's recommendations.

Part of the BOP's mission is to ensure that inmates are provided opportunities to learn skills necessary to become productive members of society when released from prison. The OIG examined the BOP's Inmate Release Preparation and Transitional Reentry Programs to determine whether the BOP's institutions maximize the number of inmates that complete programs designed to prepare them for reentry into society, including occupational, educational, psychological, and other programs, and that all eligible inmates are provided the opportunity to transition through a Community Corrections Center (CCC) in preparation for reentry into society. Our audit concluded that each BOP institution offers similar types of reentry programs that are generally recognized to reduce recidivism. However, we found that the BOP does not ensure that its institutions are maximizing the number of inmates that complete these programs. Thus, all eligible inmates are

not provided the opportunity to transition through a CCC to help prepare them for reentry into society. The BOP agreed with all of the report's recommendations and is taking corrective action.

In an ongoing review, the OIG is examining the OFDT, which was formed in FY 2001 to centralize responsibility for detention in order to better manage detention resources for the USMS and the former INS. We are finding that the OFDT faces challenges related to the accuracy of forecasting detention needs. As a result, in FY 2004 the OFDT's $814 million budget proved to be inadequate and the Department was required (with the approval of Congress) to reprogram $109 million from other initiatives to cover the shortage. Further, the Department has shifted $150 million in funds previously budgeted for other Department initiatives into the OFDT's FY 2005 budget request, which now totals almost $1.09 billion.

In FY 2005, the OIG will continue to examine BOP and USMS-related incarceration and detention issues. For example, we plan to examine the BOP's pharmacy services to assess the costs, security, and management of this program. We also plan to examine the USMS's Cooperative Agreement Program that provides money to local jails for expansion in return for jail space for federal detainees.

8. Human Capital: The Department's ability to attract and retain qualified personnel is both a top management challenge and a fundamental prerequisite to meeting other top management challenges. The Department has recognized the importance of addressing the issue of human capital and has cited "strengthening of hiring, training, and diversity policies" as one of the Department's Ten Management Goals.

   By several measures, the Department has experienced significant success in managing its human capital over the past few years. In particular, the Department has experienced low to moderate attrition rates; has well-established training programs for new law enforcement and legal job entrants; maintains a work force average age (40) significantly lower than the federal government average (47); and has an extensive data bank on job competencies needed for all its occupations.

   According to the DOJ Strategic Plan for FYs 2003-2008, the Department intends to complete a full-scale work force analysis and planning initiative that will identify specific human capital shortcomings and have accompanying strategies to overcome them. A new unified performance management system will be in place for Senior Executive Service mangers, General Schedule managers and supervisors, and all non-bargaining unit employees. Information on work force diversity will be captured and shared routinely. The Department will institutionalize the use of unified recruitment strategies, exit interviews, organization surveys, and mentoring programs.

   Hiring qualified personnel for specialized purposes is an ongoing challenge. A key issue for the FBI's successful counterterrorism efforts is the hiring of sufficient qualified translators to review the critical information collected by the FBI in foreign languages. As noted above, a July 2004 OIG audit examined the FBI's foreign language translation program and, among other things, the FBI's success at meeting its linguist hiring goals. Since September 11, 2001, the FBI's Foreign Language Program has grown significantly, increasing from 883 linguists in FY 2001 to 1,214 in FY 2004. However, the OIG review found that the FBI's collection of material requiring translation has continued to outpace its translation capabilities, and the FBI cannot translate all the foreign language counterterrorism and counter-intelligence material it collects. We attributed the FBI's backlog of unreviewed material to its insufficient number of linguists as well as limitations in the FBI's translation IT systems. We found that the FBI has difficulty hiring qualified linguists because it must compete with other Intelligence Community agencies as well as private firms.

   One important aspect of management of personnel is to ensure that allegations of misconduct are handled consistently, timely, reasonably, and in accordance with policy. To assist the Department in assessing and improving in this area, the OIG is reviewing Department components' employee disciplinary systems. As of October 2004, the OIG has reviewed disciplinary systems in the USMS, the DEA, and the BOP, and we are currently reviewing the ATF's disciplinary system.

   In each of the components reviewed, we found some problems in the disciplinary systems that weaken the agency's ability to ensure consistent, reasonable, and timely disciplinary decisions.

For example, in a review issued in September 2004, we found that the BOP does not ensure that its employees receive similar penalties for similar infractions BOP-wide. In addition, the independence of the investigative and adjudicative phases of the BOP's disciplinary process can be compromised because BOP wardens play a deciding role in both phases. In our review, we made ten recommendations to the BOP, including ensuring that sustained misconduct allegations are fully adjudicated; documenting adequately the reasons for mitigating discipline; investigating and adjudicating misconduct cases in a timely manner; and developing controls to monitor disciplinary decisions for consistency throughout the BOP.

In our DEA review, we concluded that the DEA's three-tiered system for investigating and disciplining alleged employee misconduct generally functioned well. The DEA's investigations of alleged misconduct appeared to be thorough and well documented and provided a sound basis for making disciplinary decisions. We also concluded that the DEA usually imposed reasonable and consistent discipline for confirmed misconduct.

However, we found problems in the discipline imposed in various cases that revealed weaknesses. Among those weaknesses were inadequate guidance and the possible failure of the Deciding Officials to properly consider prior mitigation before applying additional mitigating factors that resulted in penalties that appear to be too lenient; the failure to adequately document disciplinary decisions; and the failure of DEA management to monitor the timeliness of the disciplinary process. We recommended improving guidance for the DEA officials in making their disciplinary determinations, establishing standards to improve the timely processing of disciplinary cases, and requiring more effective DEA management of the overall disciplinary system. The DEA agreed to take corrective actions.

In our review of the USMS's disciplinary system, we found that in half of the cases reviewed the discipline imposed raised serious concerns, and the reasons for the final discipline decisions were not documented adequately. Also, in about one-third of the cases reviewed we found significant periods of unexplained time that appeared to prolong case adjudication. The USMS agreed to take corrective action in response to our 12 recommendations.

In addition to our reviews of component disciplinary systems, the OIG has initiated a review of the use of polygraph examinations by Department components. Polygraph examinations are used in criminal investigations and counterintelligence operations, as a pre-condition of employment or access to classified information, in background investigations, and in administrative misconduct investigations. In our review, the OIG is examining how polygraphs are used throughout the Department. The review focuses on the legal authorities and statutory and regulatory requirements governing the use of polygraph examinations, Department policy and oversight of polygraph examinations, and Department compliance with federal and professional standards for managing polygraph examinations.

The OIG also has begun reviewing the USMS's background investigations of its employees to determine whether background investigations, reinvestigations, and related adjudications are conducted appropriately and timely. Building on this ongoing review, the OIG plans to conduct a consolidated review of background investigations for the FBI, DEA, ATF, and BOP.

9. Forensic Laboratories: Forensic laboratories, or "crime labs," process evidence ranging from paint chips and tool marks to DNA and drugs. This information is critical to the successful investigation of a variety of crimes. Because of the increasing reliance law enforcement places on forensic laboratories, particularly DNA testing to solve crimes, the increasing sophistication of the science involved, and the backlogs and quality concerns regarding laboratories, the OIG has identified forensic laboratory quality control and backlog reduction as top management challenges.

   Over the past five years, the OIG has completed a series of audits of the FBI Laboratory's Combined DNA Index System (CODIS). CODIS enables participating federal, state, and local crime labs to exchange and compare DNA profiles electronically, thereby linking crimes to each other and to convicted offenders. The National DNA Index System (NDIS) is the highest level in the CODIS hierarchy and enables the laboratories participating in the CODIS program to compare DNA profiles on a national level. Participants in the CODIS system must observe certain standards in developing and uploading DNA profiles. The OIG's CODIS audits to date have identified

concerns with some participants' compliance with quality assurance standards and uploading of unallowable and inaccurate DNA profiles to the national level of CODIS.

For example, our audit of the Office of the Chief Medical Examiner Forensic Sciences Laboratory in Wilmington, Delaware, found that the laboratory was not in full compliance with applicable standards. The laboratory did not comply with FBI Quality Assurance Standards related to timely submission of external laboratory audit reports, implementation of corrective action for instances of noncompliance identified by internal laboratory audit reports, and implementation of appropriate review and oversight procedures for DNA profiles sent to outside contractors for analysis. The laboratory is working with the FBI to ensure that corrective action is taken to address our recommendations.

At the request of the FBI, we are auditing eight laboratories that participate in CODIS. For example, our review of the Virginia Central Laboratory found that it generally complied with the FBI's Quality Assurance Standards and NDIS requirements. With three exceptions, we found the laboratory uploaded DNA profiles to NDIS that were complete, accurate, and in accordance with quality standards, NDIS requirements, and state legislation. The OIG currently is auditing other CODIS laboratories nationwide. In one such audit, we found that the Georgia Bureau of Investigation's laboratory complied with CODIS standards, except that some of the profiles in CODIS databases were incomplete or inaccurate.

In May 2004, the OIG issued a review that examined the failure of a former technician in the FBI Laboratory's DNA Analysis Unit I to complete steps designed to detect contamination in the DNA testing process. Working with three nationally known DNA scientists, the OIG also conducted a broader assessment of the DNA Analysis Unit's protocols and procedures to determine if other vulnerabilities existed in its operations. The OIG's review concluded that certain DNA Analysis Unit protocols and practices were vulnerable to inadvertent or willful noncompliance. We found that certain protocols lacked sufficient detail, failed to inform the exercise of staff discretion, failed to ensure the precision of manual note taking, and were outdated. While in most instances the work practices of Unit staff members diminished the risks to some degree of these protocol vulnerabilities, the review concluded that the DNA Unit will remain subject to an increased risk of employee error or inadvertent protocol noncompliance unless the protocols are revised.

In the OIG report, we made 35 recommendations to the FBI to help address vulnerabilities in protocols and practices and to address issues regarding management's response to the former technician's misconduct. These recommendations included: 1) replacing vague sections of the protocols with comprehensive guidance and descriptions of the "best practices" currently in use; 2) adding workflow and decision aides to protocols to assist staff members in exercising proper judgment during the DNA testing process; 3) providing staff members with guidance to ensure that case documentation and case file reviews meet management expectations; and 4) updating protocols to reflect current methods within the Unit. We also recommended that the Laboratory develop a comprehensive, written training curriculum and complete implementation of an information management system to improve efficiency and evidence tracking capabilities.

In September 2004, the FBI Laboratory reported that its DNA Analysis Unit I is amending its protocols to address vulnerabilities identified in the OIG report. The FBI said that it expects to complete most of the revisions this year. In addition, the Laboratory will provide the OIG with information regarding its progress in modifying various Laboratory-wide protocols that the OIG found susceptible to abuse. Further, the DNA Analysis Unit I agreed to improve its training program and to enhance Unit communications by disseminating protocol-related information more consistently. In future incidents involving serious protocol violations, Laboratory management has committed to provide evidence contributors with timely and comprehensive information about the violation and planned remedial measures.

In an ongoing matter, the OIG is reviewing the FBI's activities in connection with the case of Oregon lawyer Brandon Mayfield who, based on an erroneous fingerprint match by the FBI, was detained for two weeks as a "material witness" in connection with the Madrid train bombing investigation. Among other issues, the OIG is examining whether the FBI Laboratory used correct procedures in the Mayfield case and whether the case is indicative of any broader problems with the FBI Laboratory's analysis of fingerprints.

In a separate audit, we are examining OJP's "No Suspect Casework DNA Backlog Reduction Program," under which states receive grant funds to increase the capacity of state laboratories to process and analyze crime scene DNA in cases in which there are no known suspects. Our audit found that OJP was successful in funding the analysis of over 24,700 backlogged no suspect cases. However, we could not determine if the program achieved the goal of increasing laboratory capacity due to data limitations. We noted that many laboratories experienced lengthy delays in implementing proposals and drawing down Program funds on a timely basis. We also found that grantees experienced delays in uploading completed profiles to CODIS.

Our FY 2004 follow-up audit up of the DEA's Laboratory Operations evaluated how effectively the DEA supports the investigation and prosecution of drug cases and the gathering of drug information for intelligence purposes. In addition, we reviewed how the DEA laboratories manage evidence and other controlled substances to prevent loss or compromise. The audit found that DEA laboratory services were effective overall and the quality of work was well managed. However, we found that turnaround times were significantly longer for latent print and digital evidence services than for drug analyses because of limited resources. We also found that procedures for handling latent print exhibits could be improved to help identify more suspects. Additionally, we found deficiencies in laboratory facilities that posed health risks to employees and security weaknesses.

In FY 2005, the OIG intends to perform a follow-up audit of the ATF's laboratories to determine how effectively ATF forensic services support the investigation and prosecution of cases, and how well ATF laboratories manage evidence and other controlled items to prevent loss or compromise.

10. Supply and Demand for Drugs: One of the Department's strategic objectives in FY 2004 is to "break the cycle of illegal drugs and violence through prevention and treatment." Early federal drug control efforts concentrated primarily on enforcement to reduce the supply of illegal drugs in this country. However, it has been widely recognized that enforcement alone is not sufficient and that federal efforts to reduce the demand for drugs are necessary. These demand reduction efforts include programs dealing with drug abuse education, prevention, treatment, research, rehabilitation, drug-free workplace programs, and drug testing. In addition, as we reported in FY 2003, the illegal diversion of prescription drugs for non-medical purposes continues to be a significant problem.

    The Department attempts to reduce the availability of drugs by targeting the largest drug supply and money laundering networks in an effort to dismantle their infrastructure, from international supply and national transportation cells to regional and local distribution organizations. As part of this effort, the Department relies on the Organized Crime Drug Enforcement Task Force program with its federal, state, and local partnerships and its focus on coordinated investigations against entire drug networks. According to the DEA, in FY 2003 it disrupted or dismantled 319 domestic and foreign priority drug organizations, including several significant international drug trafficking and money laundering organizations.

    In a September 2003 report, however, the OIG found that the DEA had failed to meet key aspects of the Government Performance and Results Act (GPRA). GPRA seeks to shift government performance and accountability away from counting activities to focusing instead on the results or outcomes of those activities. For example, we found that the DEA's strategic goal (to identify, target, investigate, disrupt, and dismantle the international, national, state, and local drug trafficking organizations that are having the most significant impact on America) and the DEA's 15 strategic objectives were not quantitative, directly measurable, or assessment-based, as required by GPRA. As a result, we concluded it was impossible for the Department, Congress, and the public to assess whether the DEA is adequately achieving its stated goal and objectives.

    Since issuance of the report, the DEA has established quantitative, measurable, and assessment-based strategic goals and objectives in its FY 2003-2008 Strategic Plan. These strategic goals and objectives contained milestones and specific performance measures, such as percentages of organizations to be disrupted or dismantled in a given year. In addition, the DEA reported performance results for each of its four performance indicators in its FY 2005 Congressional budget submission.

One of the key issues in reducing the supply of illegal drugs is the illegal diversion of controlled pharmaceuticals. In September 2002, the OIG issued a report that found that the DEA did not adequately address the problem of controlled pharmaceutical diversion, which accounts for 30 percent of all reported deaths and injuries associated with drug abuse. In addition, 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 such as Hydrocodone and OxyContin.

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; increased its training of special agents on diversion investigation procedures; and completed a review of intelligence capabilities to provide improved support for diversion control.

In January 2003, the OIG issued an evaluation of the BOP's efforts to keep drugs out of its prisons and to rehabilitate drug-addicted inmates. We found that the BOP did not search visitors or monitor visiting rooms adequately, take sufficient measures to prevent drug smuggling by BOP staff, or provide adequate non-residential drug treatment to inmates. In response to our recommendations, the BOP has proposed or implemented revisions to strengthen visitor searches, improve surveillance of visiting rooms, expand drug interdiction training to staff, increase sanctions against inmates who commit prohibited drug-related acts, limit the size and content of staff's property entering the prisons, limit unsolicited mail received by inmates, improve the identification and tracking of inmates with drug abuse problems, and provide incentives to inmates to participate in non-residential drug treatment. Although the BOP has taken steps to improve its drug interdiction activities, the OIG intends to evaluate the results of these actions in a follow-up review.

To provide additional information about this management challenge, the OIG also plans to review the DEA's management of the High Intensity Drug Trafficking Area Program (HIDTA). Under HIDTA, created by the Anti-Drug Abuse Act of 1988, the Office of National Drug Control Policy (ONDCP) has designated 31 regional offices across the country as eligible for HIDTA funds because they have the most critical drug-trafficking problems that affect the rest of the country. HIDTA funds are used to dismantle drug-trafficking organizations, demand reduction efforts, and drug treatment initiatives. The OIG audit will attempt to determine whether the DEA has effectively managed the HIDTA program and what impact the shift in law enforcement priorities toward counterterrorism has had on the program.

In sum, reducing the supply of illegal drugs while at the same time reducing the diversion of legal prescription drugs for illegal use remains a critical, ongoing challenge for the Department.