November 5, 2003

MEMORANDUM FOR THE ATTORNEY GENERAL
THE ACTING DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management Challenges

Attached to this memorandum is the Office of the Inspector General's (OIG) 2003 list of top management challenges facing the Department of Justice (Department). We have prepared similar lists since 1998, initially in response to Congressional requests. By statute, this list is now required to be included in the Department's annual Performance and Accountability Report.

The challenges are not presented in order of priority - we believe that all are critical management issues facing the Department. However, as with last year's list, 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. Two challenges from last year's list have been removed and replaced by two other challenges. We removed "Detention Space" because the responsibility for obtaining adequate and cost-efficient detention space for many immigration detainees has been transferred to the Department of Homeland Security, which now must address this difficult challenge. We also have removed "Department of Justice Reorganizations" from the list because a large part of that challenge was accomplished by the Department when it smoothly assimilated the Bureau of Alcohol, Tobacco, Firearms and Explosives into the Department while transferring the Immigration and Naturalization Service out of the Department.

In their place, we have added two new challenges: "Reducing the Supply of and Demand for Illegal Drugs" and "Security of Classified Information and Critical Infrastructure." The first is a critical issue for the Department - to reduce the supply of illegal drugs coming into this country, the diversion of legal drugs for illicit use, and the demand for drugs. These multi-faceted problems have an enormous impact on law enforcement, health, and social issues in this country.

The other new challenge, "Security of Classified Information and Critical Infrastructure," is related to but different from the counterterrorism challenge. Maintaining the security of classified information, while at the same time ensuring that such information is shared appropriately among law enforcement and intelligence agencies that have a need to know,

is a difficult but critical task for the Department, particularly after the September 11 terrorist attacks.

We hope that this list and the accompanying analysis will assist Department managers in developing strategies to address the top management challenges facing the Department. We look forward to continuing to work with the Department to address these important issues.

Attachment

---

1. Counterterrorism: The Department's top priority is preventing, detecting, and deterring future terrorist acts. Creation of the Department of Homeland Security (DHS) and the resulting shift of the Immigration and Naturalization Service (INS) to the DHS were only two aspects of extraordinary government-wide efforts during the past year to address this challenge.

   Within the Department, the focus on counterterrorism has been clearly articulated and consistently stressed. The Department's Strategic Plan for 2001-2006 makes clear this is the top priority and notes the challenges facing the Department as it seeks to effectively manage its counterterrorism programs while coordinating with other intelligence agencies and law enforcement entities, both federal and local. In addition, the infusion of billions of dollars to help fund the Department's expanded counterterrorism efforts require managers to ensure that these funds are spent in an effective manner.

   For its part, the OIG continues to audit and evaluate Department programs and operations that relate to counterterrorism and follow up on previous reviews to ensure that Department components take timely actions and address identified deficiencies. For example, in September 2002 the OIG issued an audit (OIG Report #02-38) that assessed the FBI's management of aspects of its counterterrorism program from 1995 through April 2002. The OIG review found that the FBI had never performed a formal comprehensive assessment of the risk of the terrorist threat facing the United States. We concluded that such an assessment would be useful not only to define the nature, likelihood, and severity of the threat, but also to identify intelligence gaps and determine appropriate levels of resources to effectively combat terrorism. Further, although the FBI had developed an elaborate, multilayered strategic planning system, the FBI did not perform and incorporate into its planning system a comprehensive assessment of the threat of terrorist attacks on United States soil.

   Since our audit was issued, the FBI has issued its national-level threat and risk assessment, which includes to some extent an assessment of the chemical and biological agents most likely to be used in a terrorist attack. We recommended that the FBI separately assess the threat and risk of all categories of weapons of mass destruction using intelligence information and a multidisciplinary team of subject-

matter experts. To date, the FBI has not fully complied with our recommendation but has made progress recently by completing a draft of a separate threat assessment of chemical and biological agents. In addition, the FBI reports that it has improved its hiring and use of intelligence analysts, and we are evaluating this issue as part of an ongoing audit. The FBI also reports that it nearly has completed revising its strategic plan, in accordance with our recommendation, which is intended to conform to the Department's strategic plan and its emphasis on preventing terrorism. As part of our follow-up work on these issues, we will review the FBI's updated strategic plan when it is completed.

The FBI also reported that it continues its efforts to close the gap between counterterrorism planning and operations through performance measures and standards and by holding managers accountable. All FBI divisions are now required to submit annual program plans with specific measures that will be used to gauge both program and field office performance. Once the plans are final, the FBI will develop a complete set of performance measures. During fiscal year (FY) 2004, the FBI intends to establish an integrated management system that more clearly links planning, performance, and accountability. We will continue to monitor these efforts.

While the Department appropriately is focusing significant efforts and resources to prevent acts of terrorism, its attention also is needed to prepare to respond to terrorist acts and other critical incidents should they occur. In 1996, the Department implemented the Crisis Management Coordinator Program (CMC Program), under which each United States Attorney's Office (USAO) was directed to designate a Crisis Management Coordinator to develop a critical incident response plan (Plan) and make other preparations to ensure that the USAOs were ready to respond to a critical incident, including acts of terrorism or natural disasters. To assess the Department's implementation of the CMC Program, the OIG is examining whether the USAOs have acted to improve their ability to respond quickly and appropriately to critical incidents by developing comprehensive plans and by training staff to carry out those plans. Our findings indicate that most USAOs have not fully implemented effective response plans.

In a separate ongoing review, the OIG is examining a variety of terrorism-related task forces to determine how their law enforcement and intelligence functions support the Department's efforts to detect, deter, and disrupt terrorism. Specifically, this review is evaluating the purpose, priorities, accomplishments, and functioning of the Anti-Terrorism Task Forces (ATTF), the FBI's Joint Terrorism Task Forces and Foreign Terrorist Tracking Task Force, and the Deputy Attorney General's National Security Coordination Council.

Because the FBI plays such a central role in the Department's counterterrorism strategy, the OIG continues to expend significant resources to review FBI programs and operations, many of which affect its counterterrorism missions. For example, in September 2003, the OIG released an audit of the FBI's Casework and Human Resource Allocation (OIG Report #03-37). In summary, this review found that prior to the September 11, 2001, terrorist attacks the FBI devoted significantly more special agent resources to traditional law enforcement activities, such as white-collar crime, organized crime, drugs, and violent crime, than it did to terrorism-related programs. The OIG is following up on this audit with an examination of the FBI's efforts to reprioritize and refocus its investigative resources on counterterrorism-related issues in the aftermath of the September 11 terrorist attacks. In this review,

the OIG will seek to identify the operational changes in the FBI resulting from this reprioritization effort, including the types of offenses that the FBI is no longer investigating at pre-September 11 levels. We plan to survey federal, state, and local law enforcement agencies regarding the impact on their operations of the FBI's reprioritization.

Two additional ongoing OIG reviews focus on the FBI's efforts to meet other aspects of its varied counterterrorism-related challenges. First, because much information relevant to counterterrorism and counterintelligence is in languages other than English, the OIG is examining the extent and causes of FBI translation backlogs and the FBI's efforts to hire additional translators. This review will evaluate whether FBI procedures ensure appropriate prioritization of translation work, accurate and timely translations of pertinent information, and proper security of sensitive information.

Second, the OIG is reviewing the FBI's hiring and training of intelligence analysts and reports officers. Our 2002 counterterrorism audit identified concerns about the FBI's intelligence capability and recommended that the agency improve its intelligence analysis capabilities. The current audit is evaluating how effectively the FBI recruits and trains the various categories of intelligence analysts and reports officers in support of the FBI's counterterrorism mission. Looking ahead, the OIG plans to examine additional facets of the FBI's counterterrorism initiatives, including its role in conducting counterterrorism exercises.

As noted above, the reprioritization of the Department's counterterrorism priority has resulted in significantly increased Department funding for counterterrorism efforts. A challenge for the Department is to ensure that the increased funding is used economically, effectively, and for its intended purposes. In one review completed this year, the OIG conducted a follow-up audit of the Department's Counterterrorism Fund (Fund), which was created by Congress in 1995 after the bombing of the Murrah Federal Building in Oklahoma City, Oklahoma, to assist Department components with the unanticipated costs of responding to and preventing acts of terrorism. Since its creation, Congress has appropriated more than $360 million to the Fund. Originally established to provide reimbursement solely to Department components, since 1996 more than $167 million from the Fund has supported counterterrorism initiatives of non-Department agencies, including other federal agencies and state and local governments. Past terrorism events for which Department components received reimbursement include the Oklahoma City bombing, the U.S. embassy bombings in Africa, and the September 11, 2001, terrorist attacks.

The OIG's follow-up audit (OIG Report #03-33) reviewed Fund expenditures from 1998 through 2002 and found that the Department's Justice Management Division (JMD), the entity that administers the Fund, has improved its management of the Fund since the OIG's original audit in 1999. However, the follow-up audit recommended that JMD implement additional improvements to the claims review process to ensure that adequate resources are available for emergency situations resulting from acts of terrorism. We also tested more than $38 million in Fund expenditures during the audit and identified over $3 million in questioned costs. These costs included expenses unrelated to approved counterterrorism initiatives, expenses for which the component could not provide supporting documentation, and expenses that were denied or billed erroneously.

A somewhat different but related challenge for the Department in responding to the heightened terrorism threat is to use its law enforcement and intelligence-gathering authorities without inappropriately affecting the civil rights and civil liberties of individuals. Section 1001 of the USA PATRIOT Act (Patriot Act) directs the Department's Inspector General to "receive and review" allegations of civil rights and civil liberties abuses by Department employees and report to Congress every six months about these responsibilities under Section 1001.

In furtherance of its responsibilities under Section 1001, the OIG issued a special report on June 2, 2003, that examined the treatment of 762 aliens held on immigration charges in connection with the investigation of the September 11 terrorist attacks. The OIG examined the treatment of these detainees, including their processing, bond decisions, the timing of their removal from the United States or their release from custody, their access to counsel, and their conditions of confinement. The OIG's 198-page report focused in particular on detainees held at the BOP's Metropolitan Detention Center (MDC) in Brooklyn, New York, and at the Passaic County Jail (Passaic) in Paterson, New Jersey, a county facility under contract with the INS to house federal immigration detainees.

As our report pointed out, the Department was faced with unprecedented challenges responding to the attacks, including the chaos caused by the attacks and the possibility of follow-up attacks. Yet, while recognizing these difficulties and challenges, we found significant problems in the way the Department handled the September 11 detainees. Among the report's findings:

- The FBI in New York City made little attempt to distinguish between aliens who were subjects of its terrorism investigation (called "PENTTBOM") and those encountered coincidentally to a PENTTBOM lead. The OIG concluded that even in the chaotic aftermath of the September 11 attacks, the FBI should have expended more effort to distinguish between aliens who it actually suspected of having a connection to terrorism from those aliens who, while possibly guilty of violating federal immigration law, had no connection to terrorism but simply were encountered in connection with a PENTTBOM lead.
- The INS did not consistently serve the September 11 detainees with notice of the charges under which they were being held within the INS's stated goal of 72 hours. The review found that some detainees did not receive these charging documents for weeks - in some instances not for more than a month - after being arrested. These delays affected the detainees' ability to understand why they were being held, to obtain legal counsel, and to request a bond hearing.
- The Department instituted a policy that all aliens in whom the FBI had an interest in connection with the PENTTBOM investigation required clearance by the FBI of any connection to terrorism before they could be removed or released. The policy was based on the belief - which turned out to be erroneous - that the FBI's clearance process would proceed quickly. The OIG review found that instead of taking a few days as anticipated, the FBI clearance process took an average of 80 days, primarily because it was understaffed and not given sufficient priority by the FBI.
- In the first 11 months after the terrorist attacks, 84 September 11 detainees were housed at the MDC in Brooklyn under highly restrictive conditions. These conditions included "lock down" for at least 23 hours a day; escort procedures

that included a "four-man hold" with handcuffs, leg irons, and heavy chains when the detainees were moved outside their cells; and a limit of one legal telephone call a week and one social call a month.

- BOP officials imposed a communications blackout for September 11 detainees immediately after the terrorist attacks that lasted several weeks. After the blackout ended, the MDC's designation of the September 11 detainees as "Witness Security" inmates frustrated efforts by detainees' attorneys, families, and even law enforcement officials to determine where the detainees were being held. We found MDC staff frequently - and mistakenly - told people who inquired about a specific detainee that the detainee was not held at the facility when, in fact, the opposite was true.
- With regard to allegations of abuse at the MDC, the evidence indicated physical and verbal abuse by some correctional officers against some detainees, particularly during the first months after the attacks and during intake and movement of prisoners. Although the allegations of abuse have been declined for criminal prosecution, the OIG is continuing to investigate these matters administratively.
- By contrast, the OIG review found the detainees confined at Passaic had much different, and significantly less harsh, experiences than the MDC detainees did. Passaic detainees housed in the general population were treated like "regular" INS detainees who also were held at the facility. Although we received some allegations of physical and verbal abuse, we did not find the evidence indicated a pattern of abuse at Passaic.

The OIG report made 21 recommendations to the FBI, BOP, and the DHS's Bureau of Immigration and Customs Enforcement. The recommendations dealt with issues such as developing uniform arrest and detainee classification policies, improving information-sharing among federal agencies on detainee issues, improving the FBI clearance process, clarifying procedures for processing detainee cases, revising BOP procedures for confining aliens arrested on immigration charges who are suspected of having ties to terrorism, and improving oversight of detainees housed in contract facilities. The OIG has received and analyzed responses to the recommendations, and has requested additional information on some of the recommendations. In general, we found that the agencies agreed with the recommendations and are taking steps to implement them.

Finally, in addition to directing the Inspector General to receive and review allegations of civil rights and civil liberties abuses by Department employees, Section 1001 of the Patriot Act directs the OIG to publicize how people can contact the OIG to file a complaint and requires the OIG to submit a semiannual report to Congress discussing its implementation of these responsibilities. In July 2003, the OIG issued its third Section 1001 report summarizing its activities from December 16, 2002, through June 15, 2003. The report described the status of OIG and Department investigations of alleged civil rights and civil liberties abuses by Department employees. In addition, the report highlighted several OIG reviews undertaken in furtherance of its Section 1001 responsibilities.

In the year ahead, the OIG will continue to evaluate how effectively the Department is meeting aspects of its varied counterterrorism challenge through OIG audits, inspections, and special reviews, as well as through the OIG's semiannual reports to Congress required under Section 1001 of the Patriot Act.

2. Sharing of Intelligence and Law Enforcement Information: Immediately after the September 11 terrorist attacks, the Attorney General directed 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. In October 2001, the President signed the Patriot Act, which permits greater sharing of intelligence and law enforcement information, such as information derived from Title III intercepts, information provided to grand juries, and information contained in criminal history databases. It also attempts to break down the wall which prevents the sharing of intelligence information with law enforcement officers.

   Since then, the Attorney General, the FBI Director, Members of Congress, the Secretary of DHS, and other officials have consistently and repeatedly stressed the critical importance of sharing information to help prevent future acts of terrorism. This is a difficult challenge, given the multitude of federal and state entities that have or need access to intelligence and law enforcement information as well as the sensitive nature of much of the information. Even within the Department, getting information to the right individuals and entities so that they can use it effectively is an ongoing challenge. But the Department's ability to share law enforcement and intelligence information is critical to its capacity - and the capacity of other federal, state, and local governments - to prevent, mitigate, and respond to terrorist attacks. Moreover, while emphasizing timely sharing of intelligence and law enforcement information, the Department has to balance that with maintaining the security of sensitive information and limiting that information to those with a "need to know," as we discuss below in management challenge 9.

   In a review that reflected the importance of sharing intelligence and law enforcement information, in December 2002 the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence released the results of its Joint Inquiry into the activities of the U.S. Intelligence Community in connection with the September 11 terrorist attacks. The 832-page report, much of it declassified and publicly released in July 2003, presents the Joint Inquiry's findings and conclusions. One of these findings was that prior to September 11 2001, information was not shared sufficiently.

   The Joint Inquiry report concluded that information sharing is a problem not only across the intelligence community, but also within individual agencies and between the intelligence community and law enforcement agencies. Among the report's recommendations was that the FBI should increase the exchange of counterterrorism-related information between the FBI and other federal, state, and local agencies. The Joint Inquiry also recommended that the Attorney General and the FBI Director take action to ensure that the FBI better disseminate the results of searches and surveillances authorized under the Foreign Intelligence Surveillance Act to appropriate personnel within the FBI and throughout the intelligence community.

   As a variety of OIG reviews also have shown, the Department's challenge in this area is formidable. While the Department has made significant strides in this area, especially in its coordination with state and local law enforcement agencies, much critical work remains, including ensuring adequate sharing of information between the Department and the newly created DHS.

   For example, in the OIG's 2002 report on the FBI's counterterrorism program (OIG Report #02-38), we recommended that the FBI develop criteria for evaluating and

prioritizing incoming threat information. The FBI receives a constant flow of information about possible terrorist threats and, consequently, faces an enormous challenge in deciding what information requires what type of response. Among the weaknesses we noted during our audit were the lack of criteria for initially evaluating and prioritizing incoming threat information and the lack of a protocol for when to notify higher levels of FBI management, other units and field offices, and other agencies in the law enforcement and intelligence communities. We also found that the FBI's ability to process intelligence information is hampered by its lack of an experienced, trained corps of professional intelligence analysts for both tactical and strategic threat analysis.

Since issuance of our audit, the FBI has made improvements to its training process for intelligence analysts. In addition, it hired a new Executive Assistant Director for Intelligence from the National Security Agency who has embarked on substantial improvements to the intelligence processes with the FBI.

The OIG's June 2003 review of the treatment of September 11 detainees also identified certain weaknesses in Department information sharing. This report recommended 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. As part of its ongoing follow-up work with respect to this review, the OIG has requested specific information regarding the status of information-sharing mechanisms between the Department and the DHS.

An August 2003 OIG special review that examined the FBI's performance in deterring, detecting, and investigating the espionage activities of former FBI agent Robert Hanssen made additional recommendations to enhance information sharing. The OIG review concluded that Hanssen escaped detection not because he was extraordinarily clever in his espionage, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed FBI internal security program. In this review, the OIG discussed the need for improved coordination and information sharing within the Department related to counterintelligence investigations. Specifically, the OIG recommended that the Department's Criminal Division should be a full participant in FBI counterintelligence investigations.

In an ongoing review, the OIG is examining the FBI's progress in addressing deficiencies in its intelligence-sharing capabilities identified by the FBI, Congress, the OIG, and others subsequent to the September 11 attacks. This audit will determine the extent to which the FBI has identified impediments to the sharing of counterintelligence and other information, the extent to which the FBI has improved its ability to share intelligence information internally, with the Department, with the intelligence community, and with state and local law enforcement agencies, and the extent to which the FBI is providing useful threat and intelligence information to intelligence and law enforcement agencies.

In another ongoing review, the OIG is examining the FBI's handling of intelligence information that it had prior to the September 11 attacks. This review is examining aspects of the FBI's ability to process and share intelligence information. Among the issues we are reviewing at the request of the FBI Director is how the FBI handled an

electronic communication written by its Phoenix Division in July 2001 regarding Islamic extremists attending civil aviation schools in Arizona.

In an example of the critical need to share information across agencies, the OIG has examined the status of the Department's efforts to integrate the FBI's and former INS's automated fingerprint systems. A March 2000 OIG special report ("The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System") highlighted the failure of the FBI and INS to integrate automated fingerprint systems. We noted the importance of expeditiously combining the FBI's Integrated Automated Fingerprint Identification System (IAFIS) with the INS's Automated Biometric Identification System (IDENT) to enable the fingerprint systems to share information. A follow-up OIG review in December 2001 (OIG Report #I-2002-003) concluded that integration of IDENT and IAFIS had proceeded slowly and remains years away.

In the most recent review of these integration efforts, issued in June 2003, the OIG found that integration is still progressing slowly (OIG Report #I-2003-005). A fully integrated IDENT/IAFIS system would provide immigration employees with immediate information on whether a person they apprehend or detain is wanted by the FBI or has a record in the FBI's Criminal Master File. Similarly, linking IDENT and IAFIS would provide state and local law enforcement agencies with valuable immigration information as part of a response from a single FBI criminal history search request. The lack of an integrated automated fingerprint system hinders the Department, the DHS, and state and local law enforcement agencies from sharing valuable immigration and law enforcement information about detained or apprehended persons. Our recent review found that the IDENT/IAFIS integration project is at least two years behind schedule.

According to JMD officials, the deployment date has been delayed until at least December 2003 because the INS staff and contractors working on the project were redirected in June 2002 to a competing priority. We found that despite the mounting delays, JMD did not prepare a revised schedule for completing the integration of IDENT and IAFIS. Moreover, the integration project may be at risk of further delay because JMD did not plan for continuing its stewardship of the project after the INS transferred to the DHS and now relies on informal working relationships with the DHS for system planning and implementation. The continued delays create additional risks to public safety and national security.

Finally, an ongoing OIG review of the operation of the FBI's Legal Attaché program is examining aspects of information sharing on an international level. Among other issues, the OIG is assessing the Attaché program's effectiveness in establishing liaisons with foreign law enforcement agencies.

3. Information Technology Systems Planning and Implementation: Information technology (IT) systems play a vital role in supporting the Department's varied operational and administrative activities. Employees rely on complex and often interrelated Department IT systems to meet challenges ranging from sifting through thousands of leads in a criminal investigation to developing annual financial statements. While the Department is making progress in this area, information technology systems planning and implementation continues to be a top management challenge across the Department.

In the past, OIG reviews have found numerous deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training. These deficiencies can severely impede the FBI's ability to effectively accomplish its mission because the FBI must be able to use its IT systems to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. Since FY 2002, the Department listed the FBI's management of IT as a material weakness.

A December 2002 OIG audit of the FBI's management of its IT investments (OIG Report #03-09) found that the FBI has not effectively managed its IT investments because it has not fully implemented a series of critical management processes. Specifically, the audit found that the FBI: 1) did not have fully functioning IT investment boards that are engaged in all phases of IT investment management; 2) had not followed a disciplined process of tracking and overseeing each project's cost and schedule milestones; 3) failed to document a complete inventory of existing IT systems and projects and did not consistently identify the business needs for each IT project; and 4) did not have a fully established process for selecting new IT project proposals that considered both existing IT projects and new projects. FBI officials acknowledged to the OIG that prior to March 2002, individual FBI divisions determined their IT needs in a "stovepipe" without knowledge of the business needs and priorities of the FBI as a whole.

The OIG audit also concluded that because the FBI had not fully implemented the critical processes associated with effective IT investment management, it had spent hundreds of millions of dollars on IT projects without adequate assurance that these projects would meet their intended goals. In addition, the FBI did not have adequate assurance that its IT projects were being developed on schedule and within established budgets.

In the same audit, the OIG found that the FBI is making strides toward correcting these deficiencies. For example, the OIG found that since March 2002, when it began pilot testing a new IT investment management process, the FBI has made measurable progress towards implementing key practices necessary for an effective IT management system, especially in the area of selecting new IT projects. At the beginning of the OIG audit in January 2002, the FBI was executing only 4 of the 38 required "key practices" for building an IT investment foundation. By June 2002, the FBI was executing 14 of the 38 key practices. As part of its audit, the OIG offered 30 specific recom-mendations for actions the FBI should take to improve its IT investment management.

Following through and correcting previously cited deficiencies takes dedicated resources and agency commitment. In a September 2003 OIG audit, the OIG examined the FBI's implementation of various IT recommendations (OIG Report #03-36). We found that while the FBI has implemented many of the recommendations in prior OIG reports (93 out of 148), it still needs to take additional significant actions to ensure that the IT program effectively supports the FBI's mission. For example, until recently the FBI lacked an effective system of management controls to ensure that OIG recommendations were implemented. However, the FBI Director has committed the FBI to enhancing its internal controls to ensure that OIG recommendations are implemented in a timely and consistent manner. To this end, the FBI recently developed a system to facilitate the tracking and implementation of recommendations for improvement. In addition, the FBI

expects that its IT modernization efforts will correct many of the deficiencies identified over the years by the OIG.

Due to the importance of sound information systems planning and implementation across all Department components, the OIG plans to conduct additional reviews on IT throughout the Department. This fiscal year, the OIG plans to audit the Drug Enforcement Administration's (DEA) IT investment management process. As part of this review, the OIG will examine the DEA's strategic planning and performance measurement activities related to IT management. In addition, we also plan to audit JMD's implementation of IT investment management processes.

4. Computer Systems Security: Computer security has been a Department Material Weakness in one form or another since 1989. The threat to Department networks and databases from unauthorized access remains, as hackers and potential terrorists attempt to develop new technologies that could potentially breach the Department's computer systems.

   Since FY 2001, the OIG has performed security assessments and penetration testing of Department computer systems as mandated initially by the *Government Information Security Reform Act* (GISRA) and, as of December 2002, by the *Federal Information Security Management Act* (FISMA). The FISMA directs the OIG to perform an annual independent evaluation of the Department's information security program and practices and report the results to the Office of Management and Budget (OMB).

   In meeting these responsibilities, the OIG has conducted 22 computer security audits of Department IT systems over the past 3 years. For FY 2003, we selected five mission-critical Department computer systems - three classified systems and two sensitive but unclassified systems - to review. In addition, we reviewed the Department's oversight initiatives with respect to computer security. Overall, we concluded that the Department's IT security program requires additional improvement at both the Department and component levels, particularly in program oversight and vulnerability management to protect computer systems and reduce the number of vulnerabilities within the Department's IT systems. While we noted progress in certain areas, continued improvements are needed to help reduce the total number of vulnerabilities within the Department's IT systems.

   Without effective IT system security oversight and security management controls, system vulnerabilities may not be identified or tracked properly and corrective action plans may not be implemented in a timely and effective manner. Consequently, the underlying data within these IT systems may not be reliable and data manipulation may go undetected. In light of our audit results, we also remain concerned that the Department's functions have not been centralized sufficiently to provide the vigorous enforcement oversight - supported by a substantial, technically proficient work force - that the Department needs.

   In July 2003, in a separate audit we examined SENTRY, the BOP's primary mission support database that processes over 1 million transactions each day (OIG Report #03-25). The system tracks critical information on more than 165,000 inmates in federal prisons including inmate location, medical history, behavior history, and release data. Our audit assessed the system's application controls and examined whether SENTRY data are valid, properly authorized, and completely and accurately

processed. The audit identified weaknesses in 4 of the 27 control areas that we tested: supervisory reviews, audit logs, access controls, and computer matching of transaction data. We concluded that these weaknesses occurred because BOP management did not fully develop, document, or enforce BOP policies in accordance with current Department policies and procedures.

Our past audits have reported progress in the Department's oversight of computer security, particularly with the restructuring of the Chief Information Officer (CIO) position and initiatives undertaken by the new CIO. However, many of the deficiencies identified by the OIG in its recent GISRA and FISMA reviews revealed repeated deficiencies from prior reviews. For example, our audits of the Department's systems in FY 2001 and 2002 revealed vulnerabilities in the management, operational, and technical controls that protect each system and its data from unauthorized use, loss, or modification. Of these three control areas, the vulnerabilities noted in technical controls are the most significant because these controls are used to prevent unauthorized access to system resources by restricting, controlling, and monitoring system access.

Additionally, our FY 2002 consolidated audit of the Department's computer security management procedures (OIG Report #03-19) identified inconsistencies in the oversight of computer security that we attributed to the bifurcation of responsibility between the JMD's Security and Emergency Planning Staff and its Information Management and Security Staff. We found security reviews of the Department's systems conducted by these offices were uneven or inadequate and major systems and applications lacked elementary protections that the Department's accreditation process is intended to ensure are in place.

Our consolidated report made nine recommendations, including that:

- the Department's CIO should have greater authority over classified IT systems and the CIO's staff should be commensurately augmented;
- the tracking system used to record and monitor corrective action should be expanded in terms of both the IT systems it encompasses and the types of corrective actions it tracks;
- the use of automated technical control solutions should be expanded because of the vulnerabilities that can result when IT personnel are scarce, overextended, or inattentive;
- the Department should extend its specifications for system assessment and testing, contingency plans, emergency response preparations, and consequence management (including data retrieval and alternative site drills); and
- the Department should increase its oversight of components' and managers' compliance with established IT security rules. The Department agreed with the recommendations and is in the process of implementing corrective actions.

Finally, the OIG's review of the Hanssen case, described above in challenge 2, identified serious security flaws in the FBI's Automated Case Support (ACS) computer system. This review found that Hanssen had improperly used the ACS system to track some of the FBI's most sensitive espionage investigations, including the investigation that was looking for him. The OIG found that access restrictions to the ACS system are subject to override by FBI Headquarters employees who, like

Hanssen, may have no need to know about sensitive operations the access restrictions are designed to protect. In addition, the system is prone to human error, with documents concerning highly sensitive operations, such as the Hanssen investigation, being made available to many users because of improper uploading or inadequate restriction codes. We found that the ACS system's audit function, mandated by Department regulations and a principal tool against unauthorized usage, was rarely used before Hanssen's arrest. The FBI is implementing a new automated case system known as the Virtual Case File (VCF), a computerized database that will maintain information on FBI investigations in electronic case files. In developing and implementing VCF, it is vital for the FBI to rectify the types of security flaws in the ACS system identified by the OIG and others.

5. Financial Management: In FY 2002, for the second consecutive year the Department received an unqualified opinion on its financial statements. In addition, the number of material weaknesses on the Department's consolidated financial statements declined from three in FY 2001 to two in FY 2002. The Department also received unqualified opinions on all ten of the reporting components' financial statements that make up the consolidated report. Importantly, several components were able to reduce the number of material weaknesses and reportable conditions, reducing the overall number of material weaknesses from 13 to 9. In particular, the DEA eliminated the four material weaknesses reported in FY 2001. These results reflect a continued commitment by the Department to financial accountability and improvement of internal controls. The Department and its components deserve significant credit for these accomplishments.

   However, important challenges remain. Antiquated and ineffective automated accounting systems and decentralized financial management threaten the Department's ability to maintain its unqualified opinion. For example, because of these deficient systems, problems related to financial accounting and reporting in FY 2002 were overcome only by significant year-end manual efforts. Many tasks had to be performed manually because the Department lacks automated systems to readily support ongoing accounting operations, financial statement preparation, and the audit process. Such manual efforts compromise the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles, and which provide Department managers information on an ongoing basis to allow them to more effectively manage Department programs.

   In order to meet the accelerated reporting deadlines for the FY 2003 and FY 2004 financial statement audits, the Department has significant hurdles to overcome because of its continued dependence on these manual efforts. During FY 2003, quarterly financial statements were due 45 days after the close of a quarter, and for FY 2004 the *Performance and Accountability Report* is due by November 15, 2004 - nearly 2½ months earlier than the current OMB reporting deadline.

   To succeed within the expedited time frames, the Department must move away from manual processes to prepare financial statements more timely and, in turn, auditors must be able to test and rely upon internal control processes throughout the year. Recent interim audit tests performed for the FY 2003 audit were discouraging, given that many components failed portions of the testing. While additional year-end testing and manual efforts to fix problems is possible for the FY 2003 audits, it will not be possible in FY 2004 because component audits need to be completed within

14 days of the end of the fiscal year in order to meet the OMB's accelerated deadlines.

In addition, we continue to find that component financial and other automated systems are not integrated and do not readily support the production of financial statements and other required financial reporting. In FY 2002, the Department initiated the Unified Financial Management System (UFMS) project to replace the seven major accounting systems currently used throughout the Department in an effort to address these deficiencies. Currently, none of the Department's accounting systems are integrated. Consequently, production of Department-wide information must be done manually or by duplicative inputting of data from one system into another.

In fact, 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, property transactions in several components are entered twice into separate accounting and property systems - systems that need to be periodically reconciled, often manually and sometimes line-by-line.

As another example, the U.S. Marshals Service (USMS) continues to use two different major accounting systems. The older of the two systems, the Financial Management System, is used by staff in USMS field offices and was scheduled to be replaced approximately 5 years ago by STARS, the Headquarters' accounting system. However, efforts to implement the STARS system throughout the USMS were halted in 1998 due to difficulties encountered in implementing STARS at Headquarters. While the USMS has been able to develop a linkage between these two systems in order to be compliant with the Standard General Ledger requirements and have more timely access to detailed field office information, this patch is not a desired solution. The USMS financial systems still do not include key financial data related to property and procurement, and consequently the USMS has to perform manual data calls for this information to ensure that the financial statements are complete.

When fully implemented, the Department's UFMS will replace the majority of Department financial systems with a single, integrated, user-friendly system. We believe such a uniform system is necessary to help address many of the Department's longstanding weaknesses. However, some of the challenges that may arise as a result of the Department's transition to the UFMS include: 1) unexpected funding shortfalls and competing initiatives; 2) implementing the system without disrupting daily operations; and 3) hiring and training staff qualified to operate the new system.

As a result of the Department's reliance on manual processes and multiple, ineffective financial systems, its capability to provide current, timely, and accurate financial information to managers remains limited. The Department also continues to utilize extraordinary efforts to obtain audit opinions and satisfy financial reporting requirements. It will be difficult for the Department to maintain a clean audit opinion for FY 2004 and future years and meet the expedited reporting dates unless it modernizes and streamlines its financial management systems.

6. Grant Management: The Department awards approximately $6 billion dollars annually in grants to more than 6,000 state and local governments as well as profit and not-for-profit entities. The grants fund a wide variety of activities, including community policing, drug treatment, reimbursement to states for incarcerating illegal aliens, counterterrorism training, and reimbursement to victims of crime. Managing such an extensive grant-making operation efficiently and effectively continues to be a major challenge for the Department, given the large amount of money involved and the diversity and complexity of the grant programs.

   To assist the Department in meeting this challenge, an August 2003 OIG audit (OIG Report #03-27) examined the two offices primarily responsible for managing the Department's grant programs - the Office of Justice Programs (OJP) and the Office of Community Oriented Policing Services (COPS) - to identify activities that could be streamlined to increase efficiency.

   The OJP has experienced dramatic growth since it was established in 1984. Its funding programs are divided into two main categories: formula grants and discretionary grants. Formula grants are awarded to state and local governments based on a predetermined formula using, for example, a jurisdiction's crime rate or population. States are generally required to pass through a significant portion of formula awards to local agencies and organizations in the form of sub grants. Discretionary grants are awarded on a competitive basis to public and private agencies and private non-profit organizations. However, certain discretionary programs are awarded on a noncompetitive basis, consistent with congressional earmarks.

   The COPS Office was established in 1994 as a result of the Violent Crime Control and Law Enforcement Act of 1994. The single largest component of the 1994 Crime Act - the Public Safety Partnership and Community Policing Act of 1994 - authorized $8.8 billion over 6 years to fund additional community oriented policing officers and to advance community policing nationwide, and COPS continued to receive annual appropriations from FY 1995 - 2003 totaling approximately $11.3 billion. To implement the COPS grant program, the Attorney General created the COPS Office as a separate office from OJP.

   Our audit determined that the Department's federal financial assistance programs are fragmented, resulting in reduced efficiency and increased costs to award and administer federal financial assistance funds to state and local agencies. We found structural overlap between OJP and the COPS Office, overlap in grant programs between the COPS Office and OJP, lack of on-line grant application processing in the COPS Office, overlap in OJP's organization structure, and inefficiencies in OJP's automated grant management systems. We also found overlap between the types of grants awarded by the COPS Office and OJP. For example, the COPS Universal Hiring Program grants and Making Officer Redeployment Effective grants are sometimes duplicative of grants awarded by OJP under the Local Law Enforcement Block Grants program. Yet, both COPS and OJP officials told us that no formal communication procedures exist between the two agencies to ensure that grantees do not receive funds for similar purposes from both agencies.

   We found that COPS had not developed a capability to receive grant applications on-line and to download the application information directly into its grant management

system. Instead, grantees must submit applications on paper and COPS must manually input the data into its tracking system.

In addition, the audit found that OJP did not have a fully effective automated system to manage its federal financial assistance funds and, in fact, we found that OJP had more than 70 automated application systems in place. Some of these systems were developed by the individual components within OJP, and they duplicate information in other OJP systems. Despite having more than 70 automated systems to help manage its federal financial assistance funds, OJP still relied primarily on a manual system for processing grants.

Our report contains eight recommendations to improve the Department's grant-making activities, including taking steps to enhance coordination between COPS and OJP to eliminate duplication of effort and ensure that awards are not made to the same grantee for similar purposes. OJP agreed with our recommendations and is in the process of implementing corrective actions. Although the COPS Office took exception to some of the information and conclusions in the report, it agreed with the recommendations directed to it and is in the process of implementing corrective actions. Specifically, the COPS Office, as well as OJP, agreed to coordinate and exchange information about grant programs to ensure duplicative awards are not made to the same grantee by both agencies. In addition, the COPS Office agreed to continue to develop an on-line application system for COPS grants. Further, OJP is working to implement, by the end of December 2003, an enhanced grant management system with modules that will expand the system to manage grants from beginning to end.

In other reviews over the years, the OIG has devoted considerable attention to auditing individual Department grant programs to examine grantee compliance. For example, more than 375 OIG audits of COPS grants have resulted in significant dollar-related findings. In FY 2002, our audits of COPS grant recipients identified more than $11 million in questioned costs and more than $3 million in funds to better use. In the first six months of FY 2003, our audits had even greater dollar-related findings - more than $17 million in questioned costs and more than $11 million in funds to better use. In light of these findings and because of the large amounts of money earmarked for this program, the OIG will continue its program to audit COPS grants.

In addition to reviewing COPS grants, the OIG audits other types of Department grant programs. For example, the OIG currently is auditing OJP training and technical assistance grants. This review includes both an internal audit that will evaluate the OJP's efforts to award and monitor the training and technical assistance grants, and a series of external grant audits that will examine compliance by recipients with the terms of the grants.

The OIG also audits activities of the organizations that receive funding from the Department. The OIG's workplan for FY 2004 includes internal audits of several broad categories of OJP programs and grants, including grants for DNA backlog reduction, victims' services, and assistance to tribal governments. The OIG also intends to evaluate OJP's oversight of the grants and to perform individual audits testing grantees' compliance with the terms of the grant. For example, the OIG plans to initiate an audit of Antiterrorism and Emergency Assistance Program grants issued

by OJP's Office for Victims of Crime. In conjunction with this internal audit, the OIG intends to conduct a number of individual audits of grant recipients.

7. Performance-Based Management: A significant challenge for the Department is to ensure, through performance-based management, that its programs are achieving their intended purposes. This is a challenge throughout the federal government, and it is also one of the Administration's most important management initiatives. As a regular part of OIG audits, we continue to examine performance measures for the component or program under review and to determine whether the performance results are supported by reliable measurement methods or systems. Additionally, as part of our annual financial statement audits, we collect information about the existence and completeness of performance measurement data.

   OIG audits generally have found that the performance measures need improvement. Many are not focused on outcomes or are not quantifiable and verifiable. For example, in an audit completed in September 2003, the OIG reviewed the DEA's implementation of the GPRA (OIG Report #03-35). We found that the DEA had developed a strategic goal and objectives that were consistent with the Department's strategic goals and objectives, but the DEA's strategic goal and objectives were not definitive enough to allow for an assessment of whether they were being achieved. In addition, even though the DEA had established performance indicators for all of its budget decision units, it had not established:

   - specific criteria for its field divisions to designate organizations as "priority target" organizations, a key element of its strategic goal;
   - specific criteria for its field divisions to report on the primary performance indicator - priority target organizations disrupted or dismantled;
   - an effective system to collect, analyze, and report performance data for all of its performance indicators;
   - procedures to verify the performance data for all of its performance indicators; and
   - accurate performance data for one of the five field divisions included in our review.

   As a result of these deficiencies, the ability of the DEA, the Department, Congress, and the public to assess the effectiveness of the DEA's performance is diminished. We made seven recommendations to the DEA, including that it establish a strategic goal and objectives that are quantitative, directly measurable, or assessment-based; and establish specific criteria for determining what constitutes a priority target organization and a disrupted or dismantled priority target organization. The DEA concurred with our recommendations and stated that its new draft FY 2003-2008 Strategic Plan includes a general long-term goal and four specific strategic goals with two- and five-year quantitative, time-specific objectives. The DEA also has prepared definitions and specific criteria for what constitutes a priority target organization and a disrupted/dismantled organization. The DEA stated that the definitions and criteria are under review and will be included in a new Priority Target Handbook. The DEA plans to complete these actions by November 2003.

   Reporting verifiable performance-based accomplishments also is critical to the Department's planning and priority setting. In an ongoing review of the U.S. Attorneys' Offices (USAOs) Critical Incident Response Plans (Plans), described above in the first management challenge, the OIG found that the Department overstated

the degree of implementation of the USAOs' crisis response planning in the Department's Annual Performance Report for FY 2001 by suggesting a much higher performance level than actually was achieved. Providing accurate and verifiable performance data is a critical component of performance-based management.

8. Human Capital: Hiring, training, and retaining adequate personnel to handle the myriad duties of the Department are ongoing challenges. The increasing technical and sophisticated nature of the Department's work, coupled with the competition for qualified employees - often against private sector companies or other government agencies such as the Department of Homeland Security that may be able to offer greater monetary awards - only increases the Department's challenge in this area. Without a continued focus on recruitment, retention, and training, the Department runs the risk of losing ground in its efforts to address several other top management challenges, such as Computer Systems Security, Financial Management, and Information Systems Planning and Implementation. Furthermore, lack of adequately trained personnel could impede the Department's counterterrorism efforts, its effort to upgrade its IT systems, and its ability to share intelligence and law enforcement information.

   For example, in January 2003, as part of its Major Management Challenges and Program Risks series, the General Accounting Office expressed its concern about the Department's ability to attract and retain qualified special agents, intelligence analysts, and language professionals (GAO Report #03-105) due to the demand for employees with language skills throughout government, especially proficiency in Middle Eastern and Asian languages. The GAO recommended that the FBI look to sharing language resources with other agencies as a way of meeting its needs for language services.

   In October 2003 the OIG initiated an audit of the FBI's hiring, training, and staffing of intelligence analysts and reports officers to ensure that these critical positions are being staffed in a timely manner with qualified personnel. The review will examine: 1) how analyst and reports officer hiring requirements and qualifications were established; 2) progress made toward meeting the hiring goals and retaining the personnel; 3) progress made toward establishing a comprehensive training program and meeting the training goals; and 4) how analysts and reports officers are staffed and utilized to support the FBI's counterterrorism mission.

   The National Commission on Terrorism in its report *Countering the Changing Threat of International Terrorism* stated that, "All U.S. Government agencies face a drastic shortage of linguists to translate raw data into useful information. This shortage has a direct impact on counterterrorism efforts." Indeed, shortly after the September 11 attacks, the FBI issued a public call for Middle Eastern and Central Asian linguists. In the past, at the FBI shortages of linguists have resulted in thousands of hours of audiotapes and pages of written material not being reviewed or translated in a timely manner. To examine this issue, the OIG has initiated an audit of the FBI Language Services program to review. The objectives of the audit are to determine the extent and causes of any FBI translation backlog; evaluate whether FBI procedures ensure appropriate prioritization of work, accurate and timely translations of pertinent information, and proper security of sensitive information; and assess the FBI's efforts to hire additional translators.

In another area, our ongoing audit work in the financial management area continues to find that several Department components lack adequate staff to perform many of the tasks needed to produce financial statements. Consequently, the Department continues to rely heavily on the use of contractors to prepare financial statements which, in addition to affecting the expense associated with producing the statements, contributes to diminishing the institutional knowledge and expertise. In addition, Department components have difficulty recruiting and retaining highly qualified information technology specialists who are knowledgeable about the latest hardware and software. As a result, the components have found it difficult to address some of the IT issues identified in the financial statement audits.

In 2003, the OIG continued to examine another important aspect of the Department's efforts to successfully manage human capital - its ability to develop fair and consistent methods of addressing allegations of employee misconduct. In FY 2001, the OIG completed a review of the disciplinary system of the USMS (OIG Report I-2001-011) - the first in a series of reviews of components' disciplinary systems. Our review of the USMS found misconduct cases where the consistency of the discipline or the degree of discipline imposed raised serious concerns, and the reasons for the final discipline decisions were not adequately documented. In addition, we found significant periods of unexplained elapsed time that appeared to prolong case adjudication. We made 12 recommendations to help the USMS improve its disciplinary system.

Most recently, the OIG examined the process by which the DEA identifies, refers, and investigates employee misconduct and imposes and enforces disciplinary actions in response to substantiated allegations of employee misconduct. The review evaluated the DEA's compliance with procedures for reporting allegations of misconduct to its Office of Professional Responsibility as well as the timeliness of the process from the referral of allegations to the implementation of disciplinary actions. The review also examined the appropriateness and consistency of disciplinary actions. We found that the DEA's system for investigating employee misconduct generally functioned well in that its investigations generally appeared to be thorough and well documented, and provided a sound basis for making disciplinary decisions.

However, we found problems in various cases that revealed weaknesses in DEA's disciplinary system. These weaknesses included inadequate guidance and dual mitigation which resulted in penalties that appear to be too lenient; the improper consideration of external factors by Board members and a Deciding Official when making disciplinary decisions; a failure to adequately document disciplinary decisions by the Board and Deciding Officials; a failure of DEA management to monitor the timeliness of the disciplinary process; and a lack of management oversight over the Deciding Officials. We made eight recommendations to help the DEA ensure that its disciplinary decisions are reasonable, free of inappropriate external influences, well documented, and timely.

9. Protecting the Security of Department Information and Infrastructure: A difficult challenge for the Department is the need to not only share intelligence and law enforcement information with a wider audience but also to protect the security of that information. Striking a balance between these competing objectives is critical to the Department's efforts to prevent future terrorist acts. In addition, the security of the Department's infrastructure - including its buildings, computers, and

communications systems - presented a significant challenge well before the September 11, 2001, terrorist attacks.

For example, in April 1997 the OIG issued a classified report examining the FBI's performance in uncovering the espionage activities of former Central Intelligence Agency (CIA) Directorate of Operations officer Aldrich Ames. The review found that throughout nearly the entire 9-year period of Ames' espionage, the FBI devoted inadequate attention to determining the cause of the sudden, unprecedented, and catastrophic losses suffered by both the FBI and the CIA in their Soviet intelligence programs. One of the recommendations made by the OIG in the report focused on the FBI's inability to provide the OIG review team with a definitive answer concerning the distribution of various top secret documents. Given the sensitive nature of such documents, the OIG recommended that the FBI develop and maintain a better record-keeping system for tracking dissemination of its documents.

Six years later, the OIG released its review of the Hanssen case, which found this and other recommendations from the Ames matter had not been sufficiently implemented. Our Hanssen review found that over the course of more than 20 years, former FBI supervisory special agent Robert Philip Hanssen compromised some of this nation's most important counterintelligence and military secrets, including the identities of dozens of human sources, at least three of whom were executed. Hanssen's espionage began in November 1979 - three years after he joined the FBI - and continued intermittently until his arrest in February 2001, just two months before his mandatory retirement date.

In August 2003, the OIG released the results of its review of the FBI's performance in deterring, detecting, and investigating Hanssen's espionage activities. The OIG's 674-page report, classified at the Top Secret/Codeword level, revealed that there was little deterrence to espionage at the FBI during Hanssen's 25-year career. The FBI did not employ basic personnel security techniques - such as counterintelligence polygraph examinations and financial disclosure reviews - and the one background reinvestigation Hanssen underwent during his career was not thorough.

The FBI's information security program likewise offered little deterrence to Hanssen's espionage. Because of inadequate document security, Hanssen felt comfortable removing hundreds of pages of classified documents from FBI offices, including numbered original Top Secret documents. In addition, inadequate computer security permitted Hanssen to conduct thousands of searches on the FBI's computer system for references to his own name, address, and drop and signal sites to see if he was under suspicion and to search for information concerning the FBI's most sensitive counterintelligence cases. The computer system's audit function, mandated by Department regulation and a principal tool against unauthorized use as well as espionage, was rarely used before Hanssen's arrest.

The OIG found 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 made 21 recommendations to help the FBI improve its internal security and enhance its ability to deter and detect espionage in its midst and protect sensitive information. For example, the OIG recommended that the FBI create and implement programs enabling it to account for and track hard copy documents and electronic media containing sensitive information to prevent the unauthorized removal of

sensitive information from FBI facilities. In addition, we recommended that the FBI implement measures to improve computer security, including an audit program to detect and give notice of unauthorized access to sensitive cases on a real-time basis and procedures to enforce the "need to know" principle in the context of usage of FBI computers.

We also recommended that the FBI consider enhanced security measures to protect its information from misuse or compromise, including more frequent polygraph examinations, more frequent and thorough background reinvestigations, and more detailed financial disclosures for employees who enjoy unusually broad access to sensitive information. In response to these security-related recommendations, the FBI reported that it has initiated a financial disclosure program and expanded the pool of counterintelligence-focused polygraph examinations. In addition, the FBI reported taking a number of steps to improve background investigations, including automating the collection of information acquired during background investigations.

However, we found that many of the changes that the FBI says it is implementing are either ongoing or still in the planning stages. Moreover, some of the FBI's responses do not address the core concern underlying our recommendations. For others, we are closely examining the FBI's response and plan to request additional information and monitor the FBI's ongoing changes.

In another review recently initiated at the request of the FBI Director, the OIG began examining the FBI's controls over safeguarding classified information and preventing espionage in its China program. This review stems from the indictment of a former FBI Agent in Los Angeles on charges of gross negligence in handling classified information. The OIG review will, among other issues, examine allegations that the agent improperly removed classified information from FBI offices and allowed a Chinese informant access to sensitive and classified information. The informant was indicted on charges of obtaining, copying, and retaining U.S. national defense documents without authorization.

With respect to critical infrastructure, the OIG has conducted several reviews of the Department's efforts to protect its critical infrastructure in the event of a terrorist attack or other threats. Presidential Decision Directive 63 requires the Department and other government departments and agencies to prepare plans for protecting their critical infrastructure. The plans must include an inventory of mission-essential assets, a vulnerability assessment of each asset, and steps to remediate the vulnerabilities. Issued by the President, the National Plan for Information Systems Protection calls for a similar assessment of information system vulnerabilities and the adoption of a multi-year funding plan.

In an audit issued in November 2001 - Departmental Critical Infrastructure Protection Planning for the Protection of Physical Infrastructure (OIG Report #02-01) - the OIG concluded that the Department had not adequately planned for the protection of critical physical assets. Specifically, the Department had not 1) adequately identified all of its mission-essential physical assets, 2) assessed the vulnerabilities of each of its physical assets, 3) developed remedial plans for identified vulnerabilities, and 4) developed a multi-year funding plan for reducing vulnerabilities. We concluded that, as a result, the Department's ability to perform vital missions is at risk from terrorist attacks or similar threats. We recommended that the Department properly inventory its critical physical assets, complete

vulnerability assessments, and develop remedial plans to address the weaknesses identified. After initially disagreeing with our recommendations, the Department has now embarked upon, but has not yet completed, an appropriate inventory of its critical physical assets.

In an OIG audit completed in October 2003, we examined the adequacy of the Department's efforts to protect its critical computer-based infrastructure. We found that the Department has not achieved "full operating capability" - that is, the ability to protect critical infrastructures from intentional acts that would significantly diminish the ability to perform essential national security missions and ensure general public health and safety. The audit concluded that the Department needs to complete critical infrastructure protection efforts in risk mitigation, emergency management, and interagency coordination. Among the recommendations we made to help improve the Department's efforts to manage critical infrastructure protection are that the Department should:

- develop a risk mitigation tracking system to inventory classified mission-essential infrastructure systems;
- develop a multi-year funding plan based on resources required to mitigate vulnerabilities as identified in Plans of Actions and Milestones;
- develop and test contingency plans for all critical IT assets; and
- contact other agencies to determine whether any Department assets are critical to their missions.

The Department needs to focus on these and other related issues as it seeks to strike the appropriate balance between sharing intelligence and law enforcement information with a wider audience to meet its counterterrorism challenge while at the same time protecting the security of that information.

10. Reducing the Supply of and Demand for Drugs: An ongoing challenge for the Department, along with other federal and state governments and non-government entities, is to reduce both the supply of and demand for drugs. This is a difficult mission that will not be solved easily or quickly. With regard to reducing supply, the Department's challenge extends beyond illegal drugs such as cocaine and heroin to reducing the diversion or misuse of legal drugs, including prescription medication. It also is widely recognized that enforcement alone to reduce the supply of illegal drugs and diversion of legal drugs is only part of the challenge, and that federal efforts to reduce the demand for drugs also are necessary.

    During the past two years, the OIG has completed several reviews that highlight the difficulties facing the Department in attempting to address these challenges.

    In addition to the millions of users of illegal narcotics, the illegal diversion of prescription drugs for non-medical purposes is a growing and staggering problem. According to the Substance Abuse and Mental Health Services Agency, emergency rooms across the country recorded a 163 percent increase in the number of visits tied to the abuse of prescription drugs between 1995 and 2002. Furthermore, prescription drugs are now a factor in one-fourth of all drug overdose deaths reported in the United States. The DEA Administrator, in a speech to the American Pain Society in March 2002, noted that the number of people who abuse controlled pharmaceuticals each year approximately equals the number who abuse cocaine - 2 to 4 percent of the U.S. population.

Therefore, an important and growing challenge to the Department is to reduce the diversion of controlled pharmaceuticals. Diversion occurs when legally produced pharmaceuticals are illegally obtained for non-medical use. Diversion commonly involves physicians or pharmacists selling prescriptions to drug dealers or abusers, employees stealing from drug inventories or pharmacies, individuals improperly obtaining multiple prescriptions from different doctors or over the Internet, and individuals forging prescriptions. Within the DEA, the Office of Diversion Control is responsible for overseeing the distribution system for controlled pharmaceuticals and regulated chemicals, and for preventing the diversion of those substances.

In September 2002, the OIG issued a review of the DEA's investigative response to the diversion of controlled pharmaceuticals (OIG Report #I 2002-010). Our review found that the DEA's enforcement efforts did not adequately address the problem of controlled pharmaceutical diversion. Despite the widespread problem of pharmaceutical abuse, the DEA dedicated only 10 percent of its field investigator positions to diversion investigations. In addition, we found that since 1990 the number of diversion investigators as a percentage of total DEA investigators decreased by 3 percent. While the DEA has traditionally focused the majority of its resources on disrupting illicit drug trafficking operations, we concluded that it is critical for the DEA to devote more resources to counteract the widespread problem of controlled pharmaceutical diversion.

We also found the DEA failed to provide sufficient DEA special agents to assist diversion investigators in conducting investigations of controlled pharmaceutical diversion. Diversion investigators lack law enforcement authority and therefore must request either DEA special agents or local law enforcement officers to perform essential activities such as conducting surveillance, issuing search warrants, managing confidential informants, and performing undercover drug purchases. We found that difficulties in obtaining law enforcement assistance caused delays in developing cases for prosecution. The quality of investigations also has suffered because of the need to use investigators external to the diversion control program who lack experience in conducting controlled pharmaceutical investigations, which often requires establishing the criminal intent of doctors, pharmacists, and other medical professionals. DEA officials acknowledged these problems and over the past 25 years have proposed solutions ranging from vesting diversion investigators with criminal investigative authority to assigning special agents to diversion units on a full-time basis. However, as of October 2003 the DEA still has not implemented an effective solution. The DEA advised the OIG that the reclassification of diversion investigators to special agents requires more discussion before a decision is made.

In addition, our review found that the DEA provides minimal intelligence support to its diversion investigators, instead focusing its intelligence efforts on developing and analyzing intelligence information on illicit drug trafficking. The one potential intelligence resource currently available to diversion investigators is the Automation of Reports and Consolidated Orders System (ARCOS). The ARCOS contains information on the inventories, acquisitions, and dispositions of certain controlled pharmaceuticals, as reported quarterly by manufacturers and distributors. These quarterly reports show transactions for broad categories of controlled pharmaceuticals but not specific drugs. ARCOS details the flow of DEA-controlled pharmaceuticals from their point of manufacture through commercial distribution channels to the sale or distribution to dispensing or retail outlets (such as pharmacies, health care practitioners, and hospitals). However, diversion

investigators told the OIG that ARCOS reports are limited in their value as an intelligence resource because of problems of completeness, accuracy, and timeliness. Diversion staff at Headquarters and in DEA field offices also told the OIG that they do not have the adequate resources to analyze and develop ARCOS data into useful intelligence products.

With regard to reducing the supply of illegal drugs, in September 2003 the OIG issued an audit examining the DEA's performance measures assessing its impact on reducing the supply of illegal drugs. The audit entitled, "The DEA's Implementation of the Government Performance and Results Act" (GPRA) (OIG Report #03-35), concluded that the DEA failed to meet key aspects of the GPRA and noted that while the DEA developed a strategic goal and objectives that were consistent with the Department's, the DEA's strategic goal and objectives were not definitive enough to allow for an assessment of whether they are being achieved.

For example, even though the DEA had established performance indicators for all of its budget decision units, it had not established: 1) specific criteria for its field divisions to designate organizations as "priority target" organizations, a key element of its strategic goal; 2) specific criteria for its field divisions to report on the primary performance indicator - priority target organizations disrupted or dismantled; 3) an effective system to collect, analyze, and report performance data for all of its indicators; 4) procedures to verify performance data for all of its indicators; and 5) realistic goals for its performance indicators.

As a result of these deficiencies, the ability of the Department, Congress, and the public to assess the effectiveness of the DEA's performance in reducing the supply of illegal drugs was diminished. We recommended, among other things, that the DEA establish a strategic goal and objectives that are quantitative, directly measurable, or assessment-based and develop specific criteria for determining what constitutes a priority target organization and a disrupted or dismantled priority target organization. The DEA concurred with our recommendations and is updating its strategic plan. The new strategic plan will include, according to the DEA, one general long-term goal and four strategic goals with quantitative, time-specific objectives that will address the OIG's recommendations.

In FY 2004, the OIG will continue to examine other supply-reduction aspects of this challenge by reviewing the operations of the High Intensity Drug Trafficking Area Task Forces, a program designed to help federal, state, and local law enforcement organizations invest in infrastructure and joint initiatives to confront drug-trafficking organizations. The objectives of the audit will be to determine the relationship between DEA's mission and the Office of National Drug Control Policy's mission for the High Intensity Drug Trafficking Area (HIDTA) program; DEA's overall relationship to the HIDTA program; the efficiency and cost effectiveness of HIDTA's delivery of funds to federal, state, and local law enforcement agencies; and the impact on agencies that participate in HIDTA task forces as a result of changes in law enforcement priorities in response to the events of September 11, 2001.

Attempting to reduce the supply of drugs alone will not solve the problem of illegal use of drugs; reducing the demand for illegal drugs is a critical component of the strategy to reduce drug abuse in the United States. In a February 2003 audit, the OIG examined the Department's drug demand reduction activities, one of the objectives identified in the DEA's current Strategic Plan. While early federal drug

control efforts concentrated primarily on enforcement, federal drug demand reduction efforts today include drug abuse education, prevention, treatment, research, rehabilitation, drug free workplace programs, and drug testing.

The OIG reviewed the Department's drug demand reduction activities to: 1) identify all Department programs that related to drug demand reduction, quantify the total obligations for each program, and verify that financial information provided to the ONDCP was prepared appropriately; 2) determine whether the Department's performance measures are adequate to determine the success of its programs; 3) identify whether Department drug demand reduction activities were duplicative and whether Department components were coordinating drug demand reduction efforts; and 4) review the DEA activities and funding dedicated to drug demand reduction. During its audit, the OIG examined drug demand reduction programs in the BOP, COPS, OJP, and the DEA.

The ONDCP reported that the total federal drug demand reduction budget for FY 2001 was $5.9 billion, of which the Department reported spending $336 million for 19 drug demand reduction programs administered by the DEA, BOP, COPS, and OJP. Our audit of the Department's drug demand efforts found that the Department's report to the ONDCP did not accurately reflect its drug demand reduction activities, overstating by more than 50 percent the Department's actual funding of drug demand reduction programs. We identified 10 programs with total reported obligations of $223 million that were not directly related to drug demand reduction. As a result, the Department's obligations directly related to drug demand reduction for the remaining Department programs were actually $163 million, not the $336 million reported in FY 2001.

The OIG audit also found that the performance indicators did not adequately measure the effectiveness of the Department's drug demand reduction programs. Further, the DEA did not establish any performance indicators for its drug demand reduction programs, even though drug demand reduction is one of the DEA's strategic objectives. In addition, we found that the Department had not established a formalized mechanism for sharing drug demand reduction program information among its components.

Finally, we found that the DEA spent only $3 million on drug demand reduction efforts in FY 2001 - two-tenths of one percent of its $1.4 billion budget. The DEA's drug demand reduction efforts were largely conducted by its Demand Reduction Section, which consisted of 8 headquarters staff and 27 Demand Reduction Coordinators located in DEA field offices or other operational offices. The OIG's audit questioned the impact the DEA can achieve on reducing the demand for drugs with such a small percentage of its funding devoted to this effort. In response to this concern, the DEA indicated that it is completing an evaluation to determine the impact of the drug demand reduction program.

Within the past year, the OIG also has focused on efforts by components other than the DEA to reduce drug supply and demand. In January 2003, the OIG issued an evaluation of the BOP's drug interdiction activities (OIG Report #I-2003-002). Drug use by federal inmates represents a serious health and prison management problem. Drugs are in every prison. Moreover, while the BOP's national rate for positive inmate drug tests in 2001 was 1.94 percent, the statistics vary widely among BOP facilities. For example, the high-security U.S. Penitentiary in Beaumont, Texas,

posted a positive inmate drug test rate of 7.84 percent. In addition, 50 federal inmates have died from drug overdoses since 1997 and the BOP has recorded more than 1,100 "drug finds" in its institutions since 2000.

We determined that visitors, BOP staff, and the mail are the three primary ways drugs enter BOP institutions. The OIG concluded that the BOP fails to search visitors adequately, and that most of the BOP institutions we visited have an insufficient number of cameras, monitors, and staff to adequately supervise inmate-visiting sessions. In addition, the OIG concluded that the BOP has not taken sufficient measures to prevent drug smuggling by its staff. The report noted that interdiction activities common in many state correctional systems - such as random searches of staff or their property, or conducting random drug tests of staff - currently are not used by the BOP.

The OIG also concluded that an insufficient number of BOP inmates receive drug treatment to reduce their demand for drugs - a critical component of the BOP's drug interdiction strategy - partly because the BOP underestimates and inadequately tracks inmates' treatment needs. The BOP has estimated that 34 percent of all federal inmates need drug treatment. However, the OIG review determined that this figure is outdated and under represents the number of BOP inmates who need drug treatment.

In addition, the report concluded that the BOP does not provide adequate non-residential drug treatment in BOP facilities due to insufficient staffing, lack of policy guidance, and lack of incentives for inmates to seek such drug treatment. Even though the BOP states that non-residential treatment is a major component of its strategy to reduce inmates' demand for drugs, non-residential treatment was limited or not available at five of the institutions visited by the OIG.

The OIG report made 15 recommendations to help improve the BOP's efforts to prevent drugs from entering its institutions, including implementing "pat" searches of visitors; investing in additional cameras, monitors, and ion spectrometry technology to detect drugs; implementing policies to restrict the size and content of property that staff bring into institutions; implementing a policy regarding searching staff and their property when they enter BOP institutions; implementing random drug testing for staff; and implementing additional non-residential treatment programs for inmates in the general population. The BOP agreed with many of the recommendations, and is in the process of implementing various corrective actions.

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