



**1. Counterterrorism:** The most critical challenge the Department of Justice (Department) continues to face is the ongoing effort to deter and disrupt acts of terrorism. This has been the Department's highest priority since the terrorist attacks of September 11, 2001. Five years later, the Department has substantially enhanced its counterterrorism capabilities, but its counterterrorism efforts still remain a top challenge in need of continued improvement.

The most significant changes in the Department's counterterrorism efforts during the past 5 years involve the Federal Bureau of Investigation's (FBI) transformation into a more proactive, intelligence-driven agency dedicated to preventing acts of terrorism rather than primarily a law enforcement agency focused on investigating crimes after they have occurred. In its most recent reorganization, announced in July 2006, the FBI created an organizational structure of five branches that reflects its new counterterrorism priority: National Security, Criminal Investigations, Science and Technology, Office of the Chief Information Officer, and Human Resources. The National Security Branch consists of the FBI's Counterterrorism and Counterintelligence Divisions, Directorate of Intelligence, and Weapons of Mass Destruction Directorate.

Since the September 11 attacks, the FBI led the effort to create the Terrorist Screening Center (TSC), a multi-agency effort designed to consolidate information on domestic and international terrorists and provide 24-hour, 7-day a week responses for screening individuals against the consolidated terrorist watch list. Prior to establishment of the TSC, the federal government relied on more than a dozen separate watch lists maintained by a variety of federal agencies to search for terrorist-related information about individuals who, for example, apply for a visa, attempt to enter the United States through a port of entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation.

In addition, in 2005 the FBI created a Directorate of Intelligence to manage its expanded intelligence program. As part of that effort, the FBI has increased the size of its analytical corps from 1,023 analysts in October 2001 to 2,161 analysts in September 2006 – a net increase of 1,138 intelligence analysts or 111 percent – and the FBI has placed intelligence analysts in each of its 56 domestic field offices.

As we discuss in more detail in the challenge relating to violent crime, after the September 11 attacks the FBI reallocated significant agent and analyst resources from traditional criminal investigations, such as drug trafficking, health care fraud, and financial crimes, to counterterrorism and counterintelligence matters. These shifts present management challenges not only for the FBI, which continues to have responsibility for traditional criminal matters, but also for other federal, state, and local law enforcement organizations affected by the FBI's reduced involvement in certain criminal investigations. For example, an Office of the Inspector General (OIG) review of the effects of the FBI's reallocation of resources found that the FBI opened 28,331 fewer criminal cases in fiscal year (FY) 2004 than it had in FY 2000, a 45-percent reduction. Each of the FBI's criminal programs experienced fewer case openings during this period, including a 47-percent reduction in Violent Crimes and a 40-percent reduction in Financial Crimes. The FBI's greatest reduction occurred in drug-related investigations, with 70 percent fewer drug cases opened during this 5-year period.

The Department has also recently restructured itself to improve its counterterrorism capabilities. The Department created a National Security Division that brings together the Office of Intelligence and Policy Review (OIPR) and the Counterterrorism and Counterespionage sections formerly part of the Criminal Division. The Department expects this new National Security Division to serve as the principal point of contact with the Office of the Director of National Intelligence (DNI), the Central Intelligence Agency, the Department of Defense, and other components of the intelligence community. Creation of the Department's new National Security Division and the FBI's National Security Branch also implements key recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), which recommended greater coordination of intelligence-gathering activities within the Intelligence Community under the DNI.

The Department's new national security elements requires implementing new reporting structures and developing new relationships with other federal, state, and local agencies. Accomplishing these tasks effectively and efficiently presents a critical ongoing challenge for the Department.

Another continuing challenge for the Department, and in particular the FBI, with respect to its counterterrorism effort is to support and integrate to a greater degree non-agent or non-lawyer staff with technical skills. For example, OIG reviews had found that, until recently, the FBI did not adequately value the contributions of its intelligence analysts. Historically, the FBI's general view was that special agents performed the key work of the agency, and intelligence analysts were used primarily as support personnel to assist the agents with their cases. Many special agents appeared not to understand or value the role of intelligence analysts, resulting in poor utilization of analysts. While the FBI is attempting to change this attitude, we believe it still exists in parts of the FBI. We believe the FBI needs to do more to support the work of its intelligence analysts – and other non-agent staff such as scientists and linguists – who are critical to meeting the FBI's changing mission.

As we have discussed in past years, the effectiveness of the FBI – and in particular the FBI's leadership in various areas including counterterrorism – has also suffered because of a lack of continuity due to frequent turnover among all levels of management. For example, the FBI's Counterterrorism Division has had seven leaders in the past 5 years. In addition, the FBI has suffered from rapid turnover in FBI field office managers. This turnover in many key positions has hindered the FBI's ability to transform itself in many areas, including counterterrorism.

In addition, many reviews by the OIG and others have found that the FBI's counterterrorism and intelligence-gathering efforts have been hampered because of difficulties in modernizing its information technology (IT) systems. Although the FBI recently has made progress in improving its management of IT upgrades (which we discuss under the challenge relating to IT systems implementation), agents and analysts will not benefit from a fully functional case management system for several more years.

The OIG has conducted other reviews of aspects of the Department's activities that relate to its counterterrorism challenges. For example, during the past year we reviewed the FBI's efforts to protect the nation's seaports, the FBI's progress toward achieving biometric interoperability between its fingerprint systems and the system used by the Department of Homeland Security, and the use of Intelligence Research Analysts by United States Attorneys' offices. While each of these reviews found that some positive steps were being taken, each also found problems that illustrate the difficulty the Department faces as it continues to transform itself to better meet the challenge of combating terrorism.

Similarly, a March 2006 OIG audit of the FBI's efforts to protect U.S. seaports from terrorism found that while the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks at seaports, important deficiencies remain. We found that the FBI did not always allocate the agents who are responsible for maritime security according to the threat and risk of a terrorist attack on a given seaport. For example, one FBI field office with six significant seaports in its territory had only one Maritime Liaison Agent while another FBI field office with no strategic seaports had five Maritime Liaison Agents. We also noted a lack of coordination between FBI and the Coast Guard that could hinder the two agencies' ability to coordinate an effective response to a terrorist threat or incident in the maritime domain. In addition, the interim Maritime Operational Threat Response (MOTR) plan issued in September 2005 to establish protocols for agencies in responding to terrorist threats in the maritime domain did not resolve issues of overlapping jurisdiction and responsibilities between the FBI and the Coast Guard.

Since we issued our seaports audit, the FBI has informed us that the MOTR has been revised to clarify the roles of the FBI and the Coast Guard in the event of a terrorist attack in the maritime domain or at a seaport. Under the revised protocols, the FBI will be responsible for leading all maritime-related terrorist investigations and for all intelligence collection in the United States. In addition, since issuance of the OIG's report the FBI, Coast Guard, and other MOTR agencies have conducted five national-level joint maritime exercises simulating the new command and control roles established in the new MOTR. These and other actions are important steps towards resolving the coordination issues between the two agencies. However, the FBI still does not assign its agents to protect seaports in a coordinated way, leaving such assignments to the discretion of individual field offices.

In sum, the Department's counterterrorism efforts remain a work in progress. Among the key issues requiring continued attention are allocation of resources based on the threat and risk of terrorist attack; communication and coordination within and among Department components and with other federal, state, and local law enforcement agencies; development of reliable and secure IT systems to facilitate information gathering, sharing, and analysis; human capital planning to provide for hiring, training, and retention of skilled personnel; stability within the

management ranks of Department components; and use of the significant investigative and intelligence-gathering tools while respecting civil rights and civil liberties. Many of these issues are discussed in greater detail in the challenges that follow.

**2. Sharing of Intelligence and Law Enforcement Information:** The Department continues to make progress in improving its sharing of law enforcement and intelligence information with federal, state, and local officials. The ability to share such information timely and effectively is critical to the Department's success in preventing acts of terrorism and violent crime. However, ongoing efforts throughout the Department to upgrade IT systems remain a key factor in the Department's ability to more fully meet this challenge.

Since the September 11 attacks, the FBI has increased the number and frequency of its written and oral communications about terrorism with all levels of the law enforcement and intelligence communities while almost tripling its formal collaborative investigative efforts related to terrorism. For example, in the last 5 years the number of Joint Terrorism Task Forces (JTTFs) has grown from 35 to 101. These multi-agency teams, composed of staff from the FBI, local police and sheriffs' offices, and officials from more than 20 federal law enforcement agencies, investigate terrorism cases within the United States. In addition, members of the Intelligence Community and federal, state, and local participants on the FBI's National Joint Terrorism Task Force – which serves as a liaison for information on threats and leads from FBI Headquarters to the local JTTFs and participating agencies – have access to FBI databases and share access to their organizations' databases in counterterrorism investigations.

The FBI also has taken action in areas where its initial information-sharing efforts have been deficient. For example, our March 2006 report on the FBI's project to develop its new automated case management system, Sentinel, found that the FBI had not taken adequate steps to ensure that Sentinel would allow sharing of information between the FBI and other intelligence and law enforcement agencies. In addition, we were concerned that Sentinel would not provide a common framework for other agencies' case management systems as initially intended. We recommended that the FBI discuss with other intelligence community and law enforcement agencies their information-sharing requirements to ensure compatibility with those systems in the requirements and design of Sentinel.

In our current review of the Sentinel project, we found that since the March 2006 audit the FBI has focused more attention on external information sharing needs, coordinating its requirements for Sentinel with the requirements of other Department agencies, the Department of Homeland Security (DHS), and other federal entities, including the Office of the Director of National Intelligence. In addition, Sentinel is being built to meet the standards of the new National Information Exchange Model, a joint Department of Justice/Department of Homeland Security standard that has become the government-wide standard for any new law enforcement and intelligence systems being developed. Adoption of the new standard by other agencies is expected to facilitate government-wide information sharing.

With respect to sharing other types of important information, the FBI moved forward this past year in sharing fingerprint information with the DHS. The FBI and the former Immigration and Naturalization Service, now part of the DHS, originally developed separate, incompatible automated fingerprint systems in the early 1990s. The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is based on 10 rolled fingerprints, while the DHS's Automated Biometric Identification System (IDENT) system uses 2 flat fingerprints. In May 2005, the agencies resolved the impasse between the differing fingerprint collection requirements that had stalled interoperability efforts when the DHS agreed to modernize IDENT and convert US-VISIT – its entry/exit and border security system – from a 2- to a 10-fingerprint system.

An OIG report issued in July 2006, the sixth report issued by the OIG on this topic, noted that the FBI and the DHS are in the first phase of a three-phase plan to make IDENT fully interoperable with IAFIS by December 2009. According to the FBI, on September 3, 2006, the FBI and the DHS implemented the first phase of the interoperability plan by deploying a link between the two agencies' systems that will allow the exchange of copies of key immigration and law enforcement data. Yet, despite these improvements, the FBI will continue to face higher than warranted risks that criminal aliens or terrorists will enter the United States undetected until a fully interoperable system is achieved in 2009. To address this challenge, the FBI has taken interim steps to mitigate this risk, which include transmitting "Known or Suspected Terrorists" records to the DHS on a daily basis, improving

the availability of IAFIS to other users, and reducing the response time to DHS requests for checks of aliens' fingerprints.

Other aspects of the Department's counterterrorism efforts highlight the need for greater consistency in information sharing. For example, an OIG review examining the use of intelligence research specialists in United States Attorneys' Offices (USAO) to coordinate antiterrorism activities, analyze the relevance and reliability of threat information, investigative leads, and ensure that cases with terrorism connections are identified for prosecution. While we found that individually the specialists made valuable contributions to the USAOs' antiterrorism efforts, we determined that the specialists' overall effectiveness could be increased through improved coordination and guidance. For example, analytical products developed by the specialists were not consistently shared or widely disseminated within the Department. In response to the OIG report, a Department working group is developing standard requirements for analytical work and corresponding quality review of intelligence research products.

The Department's efforts to upgrade and secure information in its IT systems remains a key factor in its ability to more fully meet this information-sharing challenge. The IT and computer security challenges are addressed more fully elsewhere in this document.

In sum, the Department continues to make progress in improving its ability to share more law enforcement and intelligence information both within the Department and with other federal, state, and local law enforcement agencies through improved IT and more effective use of joint task forces. Nevertheless, the Department still faces significant challenges to ensure the timely, effective, and secure sharing of vital intelligence and law enforcement information.

**3. Information Technology Systems Planning, Implementation, and Security:** The Department made important strides this past year in its efforts to upgrade critical IT systems in a timely and cost-effective manner. In the past, widespread and deeply rooted problems, ranging from a lack of critical managerial processes to mismanagement of individual systems, have hobbled attempts by the Department to upgrade some IT systems, particularly the FBI's case management system, and provide employees with the tools needed to maximize their effectiveness.

During the past year, the Department has attempted to more effectively meet this challenge by monitoring the progress of major IT projects through an executive board called the Department Investment Review Board (DIRB). Chaired by the Deputy Attorney General, the DIRB provides high-level oversight as part of the Department's Information Technology Investment Management (ITIM) process. The DIRB's mission is to monitor the Department's major IT investments and ensure they are aligned with the Department's mission.

Improvements in IT management will be sustained only if top Department officials and senior managers in each component maintain a focus on strengthening the general processes associated with IT and the management of mission-critical IT systems.

In the past, the OIG has found that the Department lacked the ability to track the cost of its major IT systems, and more fundamentally exercised little direct control over components' IT projects. Historically, Department components have resisted any form of centralized control over major IT projects, and the Department's Chief Information Office (CIO) does not have direct operational control of component IT management. We believe the Department should consider providing increased control to the CIO for certain high-risk functions and for individual components experiencing difficulty with particular IT systems. These high-risk functions may include hiring for critical positions, completion of system requirements, and oversight of contract administration.

Notwithstanding these concerns, we found that several components made positive strides during the past year to improve their IT management practices. For example, the Drug Enforcement Administration (DEA) has done well in developing its Enterprise Architecture and ITIM processes. Having a mature Enterprise Architecture enables the DEA to make better management decisions on how individual IT projects fit into the agency's overall IT architecture. In addition, well developed ITIM practices better position the DEA to ensure that the development, design, and implementation of its IT projects are performed within cost and schedule baselines.

























