# Office of the Inspector General
# United States Department of Justice

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice

*before the*

Senate Committee on Appropriations
Subcommittee on Commerce, Justice, Science
and Related Agencies

*concerning*

Overview of the Fiscal Year 2011 Budget Request
for the Department of Justice

May 6, 2010

**Statement of Glenn A. Fine**
**Inspector General, U.S. Department of Justice,**

**before the**
**Senate Committee on Appropriations**
**Subcommittee on Commerce, Justice, Science**
**and Related Agencies**

**on**
**Overview of the Fiscal Year 2011 Budget Request**
**for the Department of Justice**

**May 6, 2010**

Madame Chairwoman, Senator Shelby, and Members of the Subcommittee:

Thank you for inviting me to testify about the Office of the Inspector General's (OIG) oversight work related to the Department of Justice (Department). In my testimony today, I will discuss some of the top challenges facing the Department as you consider its Fiscal Year (FY) 2011 budget request. My comments are based on the many reviews the OIG has conducted during recent years and on the general insight we have gained through our work in the Department.

Overall, I believe the Department has made progress in addressing many of its top challenges, but improvement is needed in some areas.

## 1. Counterterrorism

Over the years, the Department has made progress in addressing its highest priority – counterterrorism. The Department underwent a transformation following the September 11 terrorist attacks, when its highest priority shifted from traditional law enforcement concerns to counterterrorism. While the Department has been effective at reorienting its priorities to focus on counterterrorism, the Department continues to face challenges in this area.

For example, last year the OIG issued an audit report examining the FBI's practices for making nominations to the consolidated terrorist watchlist. This watchlist is used by frontline government screening personnel to determine how to respond when a known or suspected terrorist requests entry into the United States. A failure either to place appropriate individuals on the watchlist or to place them on the watchlist in a timely manner increases the risk that they are able to enter and move freely within the United States. Our review of the consolidated watchlist was the third in a series of audits assessing the accuracy of the watchlist and the timeliness of entries made to

the watchlist. Our audit concluded that the FBI did not consistently nominate known or suspected terrorists to the consolidated terrorist watchlist and did not update or remove watchlist records, as required by FBI policy.

In our audit report, we made 16 recommendations to the FBI to improve its administration of the watchlist, and the FBI concurred with all of the recommendations. The FBI has made progress in addressing the recommendations, fully implementing 9 of the 16, including the development of a web-based refresher training course to ensure all FBI counterterrorism personnel are familiar with current FBI watchlist procedures and the establishment of additional internal controls within the watchlist process to ensure that known or suspected terrorists are nominated to the watchlist and that existing records are modified or removed as required. The FBI is in the process of implementing the other recommendations.

Another issue we have reviewed regularly is the FBI's allocation and utilization of its personnel resources. In past reviews, we found that the FBI was using significantly more field agent resources than it had allocated for counterterrorism matters, and was using significantly fewer field agent resources than it had allocated for non-terrorism matters.

In a follow-up review we released this month, we again assessed the FBI's allocation and management of its personnel resources. Our audit determined that in FY 2009, the FBI had used 26 percent of its field agents on counterterrorism matters, while it used 51 percent on criminal matters. This is a significant change from FY 2001 when the FBI used 13 percent of its field agents on counterterrorism matters and 72 percent on criminal matters.

Our review determined that between FYs 2005 and 2009, the FBI used field agents in line with the allocations it made to its highest national priorities, including counterterrorism, counterintelligence, cyber crime, and civil rights. However, we found that the FBI used fewer field agents than it had allocated to some other national priorities, including gangs and criminal enterprises, white collar crime, and violent crime.

We also determined that the FBI continued to experience substantial gaps between the number of intelligence analyst positions allocated and utilized between FYs 2005 and 2009. FBI officials stated the rate of attrition and time it takes to hire applicants affected the FBI's ability to fill vacant intelligence analyst positions.

In addition, our audit determined that the FBI had improved in how it managed its personnel resources. For example, the FBI established a Resource Planning Office to oversee the allocation and utilization of personnel resources and established other initiatives to manage its resources. However, the FBI had not formalized all of the policies and procedures related to its resource

management initiatives and did not fully integrate them into FBI operational practices. This contributed to inconsistent execution of some initiatives by FBI operational divisions and field offices.

The OIG report provided 10 recommendations to assist the FBI in its resource planning and allocation decisions, including recommendations that the FBI require operational divisions to regularly examine resource utilization and that the FBI establish policies, procedures, and guidelines that formalize resource management initiatives. The FBI agreed to implement these recommendations.

Another area that affects national security is the FBI's ability to timely translate the large amount of foreign language materials it regularly collects. In previous audit reports on the FBI's foreign language translation program, we found that large amounts of audio material collected for FBI counterterrorism and counterintelligence operations were awaiting translation. In a follow-up audit issued in October 2009, we concluded that the FBI continued to have significant amounts of unreviewed foreign language materials in counterterrorism and counterintelligence matters. However, data on the exact quantity of unreviewed material is imprecise, partly because the FBI still does not have an automated means for accurately assessing the amount of material it collects for translation. In addition, we found that the FBI continues to fall short in meeting its linguist hiring goals, resulting in a decrease in the number of FBI linguists since 2005, at the same time there has been an increase in the amount of material collected for translation.

The OIG made 24 recommendations to assist the FBI in improving the management of its foreign language translation program. The FBI agreed with our recommendations and is taking steps to implement them, and the OIG will continue to monitor the FBI's performance in this important area.

Counterterrorism efforts can also be affected by coordination issues between Department components. We conducted a review of coordination between the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) in responding to explosive incidents. In our October 2009 audit, we found that jurisdictional disputes continued to occur between the FBI and ATF in explosives investigations. Despite an Attorney General memorandum in August 2004 and a 2008 Memorandum of Understanding between the FBI and ATF, the allocation of investigative authority between the two agencies remains unclear, and disputes between the agencies have continued regarding which agency should be the lead agency on explosives investigations.

For example, our audit found that FBI and ATF investigators sometimes raced to be the first federal agency on the scene of an explosives incident, and disputes have occurred when one agency arrived first and the other agency believed the explosives incident fell within its lead agency authority. These

disputes can delay investigations, interviews, and crime scene processing; confuse local first responders about which federal agency is the federal lead on explosives matters; and undermine federal and local relationships.

We also found that the FBI and ATF still maintain separate explosives-related databases to manage laboratory forensic reports, incident reporting, and technical explosives-related information and intelligence, and the FBI and ATF separately operate their explosives-training facilities and programs. In addition, ATF does not participate in the majority of Joint Terrorism Task Forces led by the FBI. Likewise, the FBI does not fully participate in ATF-led Arson and Explosives Task Forces.

Our audit made 15 recommendations to the Department, FBI, and ATF to improve explosives-related coordination. The Department appears committed to implementing these recommendations, and has established four working groups, composed of representatives from the Deputy Attorney General's Office, the FBI, and ATF, to address the recommendations and to resolve jurisdictional disputes.

We are currently conducting several reviews that involve other aspects of the Department's efforts to address counterterrorism challenges. For example, we are assessing whether the Department is prepared to fulfill its responsibilities in response to a weapons of mass destruction attack, including whether Department field offices are prepared to carry out a coordinated response if such an attack occurs in the Washington, D.C., area.

**2. Protecting Civil Rights and Civil Liberties**

Meeting the Department's counterterrorism responsibilities is a difficult task, but in this mission the Department must also balance its responsibility to protect individual civil rights and civil liberties.

The need for the Department to pursue the appropriate balance was highlighted by several reviews we conducted on the FBI's use of national security letters. We first reported on the FBI's widespread misuse of national security letters in 2007 and issued a second review in March 2008. Our third report, issued in January 2010, examined in detail the FBI's use of so called "exigent letters" and other informal requests to obtain telephone records without legal process. We found widespread misuse of these exigent letters and other informal requests for telephone records.

For example, contrary to the statements in the exigent letters, many of the FBI investigations for which the letters were used did not involve emergency circumstances and subpoenas had not been sought for the records. In addition, the FBI engaged in widespread use of other more informal requests for telephone records from communication service providers, in lieu of

appropriate legal process or a qualifying emergency. The FBI asked for and obtained telephone records through requests made by e-mail, face-to-face, on post-it notes, and by telephone. The FBI also obtained telephone records using a practice referred to by the FBI and the providers as "sneak peeks." Our report described other troubling practices regarding FBI requests for telephone records, including improper requests for reporters' telephone records, inaccurate statements made by the FBI to the Foreign Intelligence Surveillance Act (FISA) Court, and improper use of administrative subpoenas.

In addition, our report analyzed the various attempts made by the FBI to address the misuse of exigent letters. We concluded that from 2003 to March 2007 when we issued our first report, the FBI repeatedly failed to ensure that it complied with the law, Attorney General Guidelines, and FBI policy when obtaining telephone records from the on-site communications service providers.

By contrast, we found that after we issued our first report in March 2007 the FBI took appropriate steps to address the difficult problems that its exigent letters practice had created. For example, the FBI ended the use of exigent letters, issued clear guidance on the use of national security letters and on the proper procedures for requesting such records, and provided training on this guidance.

Our report also assessed the accountability of FBI employees for these improper practices and made 13 recommendations to ensure that past abuses do not recur. We believe that the FBI is taking the recommendations seriously, but additional work remains in this area. For example, the FBI's Office of Integrity and Compliance was established after issuance of the OIG's March 2007 national security letters report to detect and correct non-compliance with the rules governing FBI investigative authorities. The OIG intends to review the work of this office to determine whether it is operating effectively. In addition, the Department has yet to issue final minimization procedures concerning the retention of information obtained through national security letters. While a Department Working Group has developed recommendations for minimization procedures, the procedures have not yet been issued in final form.

In short, while the Department's counterterrorism responsibilities are its highest priority, the Department faces the ongoing challenge of balancing individual civil rights and civil liberties as it seeks to protect national security.

### 3. Restoring Confidence in the Department

In the past several years, the Department of Justice has faced significant criticism for alleged misconduct in prosecutions, the dismissal of certain U.S. Attorneys, and politicization in the hiring of career officials. While these issues involve a small number of the many important responsibilities the Department

handles and involve only a small percentage of the Department's dedicated work force, they can affect confidence in the objectivity and non-partisanship of the Department as a whole. Restoring confidence in the Department is an important and ongoing challenge.

In 2008 and 2009, the OIG and the Department's Office of Professional Responsibility (OPR) issued three joint reports which substantiated serious allegations of improper politicization in the hiring processes for career attorney positions in the Department's Honors Program and Summer Law Intern Program, in hiring for career positions by staff in the Office of the Attorney General, and in hiring lawyers for career positions and making other personnel decisions in the Civil Rights Division. Another joint OIG/OPR report issued in 2008 concluded that the process used to remove certain U.S. Attorneys in 2006 was fundamentally flawed, and the oversight and implementation of the removal process by the Department's most senior leaders was significantly lacking.

In response, the Department has taken steps to address the problems we found in these reviews. For example, the Department returned the responsibility for hiring career attorneys from politically appointed officials to the Department's career management officials, and the Department has provided training to these selecting officials on inappropriate considerations in hiring. The Department also developed new briefing and training materials for Department political appointees which emphasized that the process for hiring career attorneys must be merit based.

In addition, the Department has faced criticism about the conduct of its prosecutors in several recent prosecutions, including the prosecution of former Alaska Senator Ted Stevens. After a jury trial, the Department moved to dismiss the indictment of Senator Stevens because the Department had concluded that certain information should have been disclosed to the defense for use at trial. The Department's handling of this case created concern about the prosecutors' conduct, and federal judges in other districts also have questioned whether the Department is adequately adhering to professional standards of conduct and addressing concerns of prosecutorial misconduct.

In response to the concerns about attorney conduct, the Department has taken a variety of actions. In June 2009, a Department working group appointed by the Deputy Attorney General produced a report reviewing the Department's discovery and case management policies, procedures, and training, and made recommendations for improvement. In response to that report, the Department conducted a training conference at the National Advocacy Center in October 2009 on criminal case management and discovery for newly designated "discovery trainers" from all United States Attorneys' Offices. The discovery trainers were required to present mandatory training to all Assistant U.S. Attorneys in their districts on discovery issues. In January

2010, the Department provided guidance to prosecutors concerning best practices on discovery in criminal cases. The guidance set forth an approach for prosecutors to follow in gathering, reviewing, and producing discoverable information in a timely manner. In addition, the Department created the position of National Criminal Discovery Coordinator to oversee the ongoing training process for prosecutors on discovery issues, to assess the need for additional improvements, and to ensure continued implementation of the reforms.

In short, we believe that restoring confidence is a continuing challenge for the Department. The Department needs to ensure that the diligence, hard work, and sound ethics of the overwhelming majority of Department employees are not undermined by the few but highly visible incidents of potential misconduct. While the Department's leadership, both at the end of the past Administration and during this Administration, has taken important steps to confront this challenge, the Department must remain focused on this important issue.

### 4. Financial Crimes, Violent Crime and Cyber Crime

While the Department's highest priority is counterterrorism, it must also focus attention on its traditional law enforcement functions, including the investigation and prosecution of financial crimes, cyber crimes, and violent crimes.

The investigation of financial crimes, including mortgage fraud, white collar crimes, health care fraud, and grant and procurement fraud, is an important priority. The Department recently created the Financial Fraud Enforcement Task Force, an inter-agency initiative aimed at implementing a coordinated and proactive approach to investigating and prosecuting financial crimes. The Task Force is composed of representatives from a broad range of federal agencies, regulatory authorities, Inspectors General, and state and local law enforcement. For the Task Force to be effective, the Department needs to ensure effective collaboration with these partners, with private industry, and with consumers.

In addition to the growing problem of financial crimes, the Department faces significant new challenges in combating cyber crime. Rapid technological advances and the widespread use of the Internet make cyber crime more challenging to detect and deter. For example, recent estimates suggest that identity theft is one of the fastest growing crimes in the United States and that it affects an estimated 10 million Americans annually. In addition to financial losses, identity theft victims suffer tremendous inconvenience and emotional trauma when attempting to repair damage to their names or credit histories.

The OIG recently assessed the Department's efforts to combat identity theft. Our audit found that the Department had not adequately coordinated its efforts to combat identity theft, and that to some extent identity theft initiatives had faded as a Department priority. We determined that the Department did not have its own internal strategy to combat identity theft and had not appointed any individual or office to have responsibility for coordinating the Department's overall identity theft efforts. We also identified problems with the Department's data collection efforts on identity theft investigations and with the notification of victims of identity theft. Our audit concluded that additional leadership is needed to ensure that the Department's efforts to combat identity theft are coordinated and given greater priority.

The Department must also ensure that it places appropriate emphasis on combating violent crime, and that it coordinates its efforts in this area. For example, as noted previously in my testimony, we found that the FBI and ATF are not adequately coordinating their explosives-related investigations and operations.

Similarly, a review we issued in November 2009 concluded that two Department gang intelligence and coordination centers have not significantly improved the coordination and execution of the Department's anti-gang initiatives. Administered by the FBI, the National Gang Intelligence Center (NGIC) is a multi-agency center that develops and shares gang-related information. However, NGIC has not established a centralized gang information database as directed by statute due to technological limitations and operational problems, and has not shared gang intelligence and information effectively with other law enforcement organizations. The National Gang Targeting, Enforcement, and Coordination Center (GangTECC), administered by the Criminal Division, is a coordination center for multi-jurisdictional gang investigations, but we found that the lack of an operating budget prevents GangTECC from providing essential coordination and outreach. We recommended that the Department consider merging the two centers or ensure that their activities are better integrated. Because of the prevalence of gang violence, it is critical that the Department of Justice take swift action to improve the coordination of its anti-gang initiatives. The Department has recently informed us that it is progressing towards establishing a formal working agreement to collocate NGIC at the Organized Crime Drug Task Force fusion center and GangTECC at the Special Operations Division, and may begin moving personnel in early summer. We will continue to monitor the Department's actions to improve the coordination and effectiveness of its anti-gang operations.

Another area of increasing concern is violent crime along the Southwest Border. The OIG is reviewing ATF's implementation of Project Gunrunner, ATF's initiative to reduce firearms trafficking to Mexico and associated violence along the Southwest border. Our review follows another OIG review, completed

in September 2009, which examined ATF's planning, hiring, staffing, and allocation of resources for Project Gunrunner.

Apprehending violent fugitives is critical in the effort to address violent crime. The United States Marshals Service (USMS) is the federal government's primary agency for apprehending violent fugitives. In July 2005, the OIG reported that the USMS had increased its apprehension of violent fugitives by 51 percent from FY 2001 to FY 2004 and also increased the efficiency of its apprehension efforts. However, the increase in violent federal fugitives at large outpaced the USMS's progress, rising 3 percent from FY 2001 through FY 2004. In response to recommendations in the OIG report, the USMS increased the number of regional fugitive task forces (there are now seven); established performance measures and goals related to the apprehension of violent fugitives; and established requirements to ensure that warrants for violent offenders are entered into the Warrant Information Network within one business day.

Another aspect of the challenge of addressing violent crimes relates to the Department's efforts to implement the requirements of the *Sex Offender Registration and Notification Act* to help identify, arrest, and prosecute sex offenders who violate registration laws, and to help improve the quality of information available to law enforcement and the public about registered, non-compliant, and fugitive sex offenders. In a report issued in December 2008, we found that the Department's efforts have led to more investigations and arrests of fugitive sex offenders. However, the registries that make up the national sex offender registration system were missing records; existing records often failed to identify known fugitives; and the records often did not contain sufficient information to enable law enforcement or the public to accurately identify registered, non-compliant, or fugitive sex offenders. Since our report, the FBI has modified the National Sex Offender Registry so that it now reflects the fugitive status of registered sex offenders, initiated quality control audits of the state sex offender registries that contribute records to the registry, and started providing the USMS with data from the registry for use in USMS fugitive sex offender investigations.

It is also important that the Department ensures that it is taking full advantage of forensics tools available for the investigation and prosecution of violent crime. To that end, the OIG is examining the FBI's efforts to reduce its backlog in the forensic analysis of DNA samples. We are finding a continuing backlog that can affect the investigation of violent crimes.

### 5. Recovery Act Funding and Grant Management

The Department faces challenges each year in managing the award of more than $3 billion in grant funds. In addition to these grants, the *American Recovery and Reinvestment Act of 2009* (the Recovery Act) provided the

Department an additional $4 billon in grant funds to award. The management and oversight of these Recovery Act funds is a significant challenge for the Department which must distribute this large amount of grant funding quickly, monitor the use of these funds, and continue to manage its annual grant programs at the same time. Moreover, despite the significant influx of Recovery Act money and the expansion of the Department's grant programs, the number of grant administrators who award and oversee grant programs has not significantly increased.

Effective monitoring by each of the Department's grant-making agencies is crucial to the early identification and correction of problems among the Recovery Act grant recipients.

The OIG is conducting a series of audits of the Department's Recovery Act grant award programs. For example, we reviewed the Office of Justice Program's (OJP) selection of grants in the Edward Byrne Memorial Justice Assistance Grant Program, and found that the Department generally awarded these grants in a timely and transparent manner. In addition, the OIG is completing reviews of the administration of Recovery awards for the Office of Community Oriented Policing Services (COPS) Hiring Recovery Program, Office of Violence Against Women (OVW) programs, the Office for Victims of Crime programs, and Bureau of Justice Assistance Grants for Correctional Facilities on Tribal Lands. These programs represent $3.8 billion of the Department's approximately $4 billion in Recovery Act grant funding. As each of these audits progressed, we issued interim reports and informed the Department of any concerns related to transparency of the grant process, allocation of grant funds, interagency coordination, and improving grant management. We intend to continue to monitor and issue reports on these grant programs.

At the same time the Department faces the challenge of overseeing the infusion of Recovery Act funding, it must continue to focus on making timely awards of its regularly appropriated grant funds and in maintaining proper oversight over grantees to ensure the funds are used as intended. Several recent OIG reviews demonstrate the difficulties the Department has faced in the past in ensuring proper management of its grant funds. In September 2009 the OIG issued a report that raised concerns about the fairness and openness of OJP's National Institute of Justice's (NIJ) practices for awarding tens of millions of dollars in grants and contracts from FY 2005 through FY 2007. Our audit, which was requested by this Subcommittee, found that the NIJ's process for reviewing grant applications – including initial program office reviews, peer reviews, documentation of program office recommendations, and documentation of NIJ Director selections – raised concerns about the fairness and openness of the competition process.

In addition, we found that several NIJ staff involved in the grant award process had potential conflicts of interest when participating in the approval

process for certain grants. We also determined that the NIJ did not adequately justify the sole-source basis for some non-competitively awarded contracts and could not demonstrate that these contracts were exempt from the competitive process. We made nine recommendations in this report to improve NIJ's grant process, and the Department agreed to implement them.

We believe that the Department has taken some significant steps toward improving its grant management process during the past two years. For example, in May 2008 the Department issued a memorandum directing OJP, COPS, and OVW to document all discretionary funding recommendations and decisions. In addition, OJP has made progress in staffing its Office of Audit, Assessment, and Management (OAAM), a unit intended to improve internal controls and streamline and standardize grant management policies and procedures. However, we believe that OJP needs to ensure that our audit recommendations regarding a particular grant program will be implemented throughout all applicable Department programs, rather than only in the specific program the OIG audited.

To help the Department meet its grant management challenges, the OIG drafted a guide entitled, "*Improving the Grant Management Process.*" This document, which was based on our prior work regarding grant management issues throughout the Department, provides 43 recommendations and examples of best practices that granting agencies should consider adopting to minimize opportunities for fraud, waste, and abuse in awarding and overseeing both Recovery Act and non-Recovery Act grant funds. The Department has taken positive steps in response to the recommendations in this document. For example, OJP is more aggressively identifying and working to mitigate risks among individual grantees by assessing each potential grantee's risk during the grant-award process and imposing on high-risk grantees special conditions that provide a range of potential sanctions, including the withholding of funds. OJP also is working more closely with the OIG and now meets with the OIG on a quarterly basis to discuss grant issues.

We believe that the Department is demonstrating a commitment to improving the grant management process, and we have seen significant signs of improvement. However, considerable work remains in ensuring effective grant management of the Recovery Act funds and the billions of dollars awarded annually in Department grants.

### 6. Information Technology Systems Planning, Implementation, and Security Upgrades and Security

The Department faces ongoing challenges in managing the more than $2 billion it annually spends on information technology (IT) systems and in ensuring that its IT planning, development, and security measures maximize the effectiveness of these expenditures.

One of the major challenges in this area has been the FBI's ongoing development of its Sentinel case management project. This project is intended to upgrade the FBI's electronic case management system and provide the FBI with automated workflow processes. The OIG has issued a series of reports examining the FBI's ongoing development of Sentinel. In March 2010, we issued our sixth report in this series.

In this latest report, we identified significant concerns about the progress of the FBI's Sentinel project. Specifically, because of continuing issues regarding the usability, performance, and quality of Phase 2 of the Sentinel project that was delivered by Lockheed Martin to the FBI, on March 3, 2010, the FBI issued a partial stop work order to Lockheed Martin for portions of Phase 3 and all of Phase 4. In addition, the stop work order returned Phase 2 of the project from an operations and maintenance phase to a development phase.

As a result, the cost of the Sentinel project is rising and the completion of Sentinel has been delayed. In a previous report, we had noted that Sentinel's overall completion date had already been postponed to September 2010, which was 9 months later than originally planned, and the total projected cost was $451 million, $26 million more than originally planned. Because of the recent problems with Phase 2 of Sentinel and the stop work order, the FBI currently does not have official cost or schedule estimates for completing Sentinel. But the FBI has now acknowledged that Sentinel will cost more than $451 million and that Sentinel will likely not be completed until 2011.

Our report noted that the FBI has taken several steps to improve Sentinel's chances for success, including the use of independent assessments, performed by other contractors of the primary contractor's deliverables. However, our report identified major issues that the FBI needs to address. For example, the FBI does not have a documented strategic plan outlining how it will transfer remaining case file data from its Automated Case Support system to Sentinel. We also noted our concern that the FBI has either discontinued or delayed some of the internal assessments of Sentinel's progress that it previously was performing on a routine basis, which could compromise the FBI's ability to perform real-time evaluations of the project's development and apply appropriate risk management strategies.

Given the importance of Sentinel to the future of FBI operations, our recent report concluded that the FBI must ensure that its revisions to Sentinel's budget, schedule, and requirements are realistic, achievable, and satisfactory to its users. The FBI must also ensure that users' concerns and perspectives are integrated into all phases of the remaining development of Sentinel. While we believe that Sentinel can succeed, it will take close scrutiny

and careful oversight by the FBI to minimize any further schedule delays and budget increases and to ensure that the final product meets users needs.

We believe that the Department has made some progress in planning for other new IT systems, but it still faces challenges of delayed implementation, deficient functionality, and cost overruns in IT systems. Historically, the Department's components have resisted centralized control or oversight of major IT projects, and the Department's Chief Information Officer (CIO) does not have direct operational control of Department components' IT management. We believe the Department should enhance the CIO's oversight of the development of high-risk IT systems throughout the Department.

Several of our audits identified concerns about the development of critical Department IT systems. For example, last year an OIG audit report examined the Department's progress toward developing the Litigation Case Management System (LCMS). The LCMS project was intended to develop an IT infrastructure for storing case information, managing it centrally, and making it available to the approximately 14,500 authorized users in the Department's seven litigating divisions. Our audit found that the LCMS project, which the Department began in 2004, was more than 2 years behind schedule, approximately $20 million over budget, and at significant risk of not meeting the Department's requirements for litigation case management.

Our audit concluded that both the Department and its contractor shared responsibility for the significant delays and budget overruns in this project. We urged better oversight of this project to minimize or avoid further schedule and cost overruns. In response to our report, the Department has expressed a strong commitment to implementing the LCMS and to fully adopting our recommendations. However, the implementation of LCMS is still struggling.

Another example of delays in implementing a new IT system involves the FBI's efforts to implement a Laboratory Information Management System for the FBI Laboratory, which the FBI has been working on since 1998.

As the Department develops its new IT systems, it also must ensure the security of those systems and the information they contain. The Department must balance the need to share intelligence and law enforcement information with the need to ensure that such information sharing meets appropriate security standards.

A December 2008 OIG audit found that the Department lacked effective methodologies for tracking the remediation of identified IT vulnerabilities. Our report made four recommendations to assist the Department in its efforts to address such vulnerabilities. Since the issuance of our report, the Justice Security Operations Center (JSOC), which provides real-time monitoring of the Department's networks to detect vulnerabilities and threats, became fully

functional, and now covers all of the Department's components. The JSOC mitigates threats and vulnerabilities by blocking known threats from accessing the Department's systems and creating real-time alerts to components for immediate remediation as issues arise. In addition, the Department has developed an inventory of all IT devices on the Department's networks, updated annually, to ensure that monthly scans adequately cover the Department's entire IT environment. As part of our follow-up efforts, we intend to initiate an audit of the JSOC that will review its capabilities to detect and respond to intrusion incidents and communicate computer-intrusion efforts.

Portable IT media continues to pose IT security risks in the Department and across government. In an effort to assess the Department's efforts to safeguard information stored on portable devices, the OIG recently conducted audits of both the Civil Division's and the Criminal Division's laptop computer encryption program and practices. These audits found that a significant percentage of the laptop computers owned by contractors working with the Civil Division and the Criminal Division were not encrypted, and the contractors were not notified of Department laptop encryption requirements. In addition, we found that 25 percent of the Criminal Division laptops that we tested had sensitive data but did not have encryption software installed and did not have operating system passwords enabled. We asked the Department to ensure that all components are aware of the findings of our reports and also ensure that laptops are properly encrypted, even though our audit findings were directed at the Civil and Criminal Divisions.

In sum, the Department must closely manage its IT projects to ensure the systems are cost-effective, well-run, secure, and able to achieve their objectives.

### 7. Detention and Incarceration

The Department's responsibility to safely and economically manage its rising federal inmate and detainee populations is a challenge that has significant budget implications. The federal inmate population has dramatically increased over the past 30 years, from fewer than 25,000 inmates in the Federal Bureau of Prisons' (BOP) custody in 1980 to more than 210,000 inmates in 2010. Approximately 83 percent of these inmates are confined in BOP-operated facilities, with the balance housed in privately managed or community-based facilities and local jails. Overcrowding continues to be a serious concern in BOP facilities.

In addition to issues presented by overcrowding, the BOP must address other safety threats, including staff sexual abuse of prisoners. Staff sexual abuse has severe consequences for victims, undermines the safety and security of prisons, and in some cases leads to other crimes. For example, federal correctional workers who are sexually involved with prisoners have been subject to extortion demands and may be more easily pressured to violate other

prison rules and federal laws. Compromised personnel who have sexually abused prisoners also have been found to have provided contraband to prisoners, accepted bribes, and committed other serious crimes in an effort to conceal their sexual involvement with federal prisoners.

In a September 2009 review, we concluded that the Department and the BOP both need to take additional steps to effectively deter, detect, investigate, and prosecute staff sexual abuse of federal prisoners. Allegations of criminal sexual abuse and non-criminal sexual misconduct at BOP institutions more than doubled from FY 2001 through FY 2008. Yet, our review found that deterrence and detection of staff sexual abuse are hampered by the practice at some BOP prisons of automatically isolating, segregating, or transferring victims, which inmates often regard as punitive. We also concluded the BOP needs to improve staff training, inmate education, and program oversight on sexual abuse of inmates. In addition, we found that some Department prosecutors have a general reluctance to prosecute certain staff sexual abuse cases, and we concluded that training federal prosecutors on the detrimental impact of staff sexual abuse on inmates, other prison staff, and prison security would improve the Department's effectiveness in prosecuting these cases.

The *Prison Rape Elimination Act of 2003* requires the Department to promulgate national standards for the detection, prevention, reduction, and punishment of sexual abuse in detention facilities by June 2010. The Department is now engaged in creating these standards.

The OIG is also reviewing other aspects of the BOP's efforts to handle its difficult mission of housing inmates in safe, secure, and cost-efficient facilities. For example, the OIG is currently examining the BOP's strategies and procedures for hiring correctional officers. In another review, we are investigating allegations that the BOP failed to adequately address concerns that staff and inmates at several BOP institutions were exposed to unsafe levels of lead, cadmium, and other hazardous materials in computer recycling operations. We also are conducting a follow-up audit of the BOP's efforts to manage inmate health care.

In addition to the BOP's challenges, the Department must also provide adequate and economical housing for the increasing number of federal detainees taken into custody by the USMS. Over 50,000 federal detainees awaiting trial or sentencing are housed each day by the USMS, primarily in jails under contract with the USMS. The Department's Office of the Federal Detention Trustee (OFDT) oversees the USMS's detention activities and manages the budget for housing USMS detainees. For FY 2011, the OFDT is requesting over $1.5 billion to pay for housing, transporting, and providing medical care for detainees.

The USMS places the majority of its federal detainees in space leased from state and local governments, with the remaining detainees housed in BOP facilities or in private correctional facilities. The USMS maintains contracts, known as Intergovernmental Agreements (IGA), with about 1,800 state and local facilities to house its detainees. Over the years we have found problems with the manner in which the per diem charges that the Department pays for each detainee (also known as a jail-day rate) are determined and with the Department's monitoring of the charges. Increases in these charges can have an enormous affect on the OFDT's budget. We are now conducting another audit of OFDT's process for identifying and negotiating fair and reasonable per diem rates.

In addition, the Department plays an important role in integrating released inmates back into society and attempting to reduce recidivism by providing grants to state and local agencies, law enforcement, and community groups for prisoner re-entry programs. We currently are auditing the Department's design and management of its prisoner re-entry initiative grant programs. This audit will assess whether the Department has an effective system for monitoring grantees and for determining whether the grantees are meeting program goals.

### 8. Financial Management

Our audits have found that the Department has made significant improvements in its financial reporting. At the same time, there is an increasing demand for financial accountability and transparency throughout the federal government, and the need for accurate, near real-time financial information continues to present a significant management challenge for the Department.

In FY 2009, the Department again earned an unqualified opinion and improved its financial reporting. For the third straight year, the financial statement audit did not identify any material weaknesses in the Department's consolidated financial statements. Additionally, Department components reduced significant deficiencies in their financial statements from 14 in FY 2008 to 8 in FY 2009. The Department deserves significant credit for these efforts.

Similar to past years, however, much of this success was achieved through heavy reliance on contractor assistance, manual processes, and protracted reconciliations done for quarterly and year-end statements. We remain concerned about the sustainability of these ad hoc and costly manual efforts.

The decentralized structure of the Department also presents a major challenge to obtaining current, detailed, and accurate financial information

about the Department as a whole because there is no one single source for the financial data. The Department currently uses six major accounting systems that are not integrated with each other. In some cases, the Department components' outdated financial management systems are not integrated with all of their own subsidiary systems and therefore do not provide automated information necessary to support the need for timely and accurate financial information throughout the year. As a result, many financial tasks must be performed manually at interim periods and at year end. These costly and time-intensive efforts will continue to be necessary to produce financial statements and to satisfy other financial requirements until automated, integrated systems are implemented that readily produce financial information throughout the year.

The Department has placed great reliance on the implementation of the Unified Financial Management System (UFMS), which is intended to replace the six major accounting systems currently used throughout the Department. This unified system is expected to address many of the Department's financial management automation issues. The UFMS is intended to standardize and integrate financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes. It also will enable the Department to exercise real-time, centralized financial management oversight. We support the Department's implementation of the UFMS and believe the system can help eliminate the weaknesses in the Department's current disparate financial management systems.

**Conclusion**

In sum, the Department has made progress in addressing many of its top management challenges, but improvements are needed in important areas. The Department must maintain its focus on counterterrorism while effectively pursuing its traditional law enforcement duties, protecting civil rights and civil liberties, restoring public confidence in the Department, providing effective oversight of the billions of dollars in grant awards each year, ensuring safe and economic detention facilities, and effectively managing information technology and financial management systems.

These are difficult tasks which require constant attention and strong leadership by the Department. To aid in this effort, the OIG will continue to conduct vigorous oversight of Department programs and provide recommendations for improvement.

This concludes my prepared statement, and I would be pleased to answer any questions.