



Office of the Inspector General
United States Department of Justice

Statement of Cynthia A. Schnedar
Acting Inspector General, U.S. Department of Justice

before the

U.S. House of Representatives
Committee on Appropriations
Subcommittee on Commerce, Justice, Science
and Related Agencies

concerning

“Oversight of Department of Justice and
Department of Commerce”

February 9, 2011

**Statement of Cynthia A. Schnedar
Acting Inspector General, U.S. Department of Justice**

**before the
U.S. House of Representatives
Committee on Appropriations
Subcommittee on Commerce, Justice, Science
and Related Agencies**

**on
“Oversight of Department of Justice and
Department of Commerce”**

February 9, 2011

Mr. Chairman, Congressman Fattah, and Members of the Subcommittee:

Thank you for inviting me to testify about the activities and oversight work of the Office of the Inspector General (OIG) for the Department of Justice (Department or DOJ).

The OIG has compiled a list of top management and performance challenges for the Department of Justice annually since 1998 in an effort to provide strategic guidance for the Attorney General and top DOJ officials to take appropriate management actions. In my testimony today, I will provide an overview of the top management and performance challenges for the Department that we identified during this past year. My testimony is based on reviews conducted by the OIG and insight we have gained through our work in the Department. A more detailed discussion of our assessment of the top management and performance challenges facing the Department is available on our website at <http://www.justice.gov/oig/challenges/2010.htm>. Overall, I believe that the Department has made progress in addressing many of its top challenges, but improvement is needed in some areas.

1. Counterterrorism

Counterterrorism continues to be the highest priority of the Department, and the OIG has consistently identified it as a top management challenge facing the Department. To better address the threat of terrorism, the Department has undergone transformational changes since 2001, such as structural modifications in its law enforcement components and the creation of the National Security Division in 2006. The Department must ensure that these changes are effective and that the Department and its components are

effectively sharing information to disrupt attacks and to respond effectively to acts of terrorism. The Department also must be prepared to ensure public safety in the event of a terrorist act.

In a recent review, the OIG examined the readiness of the Department and its components to respond to a potential incident involving a weapon of mass destruction (WMD), as well as the readiness of Department field offices in the Washington area to respond in a coordinated way to a WMD incident. Our review found that the Federal Bureau of Investigation (FBI) had taken appropriate steps to prepare for responding to a potential WMD attack, but the Department as a whole and its other components had not implemented adequate WMD response plans. In particular, the Department's management of plans for responding to a WMD attack was uncoordinated and fragmented, with no entity or individual assigned responsibility for central oversight of WMD response activities throughout the Department. Moreover, other than the FBI, Department components provided little to no training for responding to a WMD incident and rarely participated in WMD exercises. In addition, while the Department had designated the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) as the lead agency to coordinate the use of federal law enforcement resources to maintain public safety and security if local and state resources are overwhelmed during a WMD incident, ATF had not adequately prepared for this role.

The Department has been responsive to the recommendations made in our report. It assigned to the Associate Deputy Attorney General for National Security the responsibility for coordinating all Department policies associated with continuity of operations, continuity of government, and emergency response at the scene of an incident. The Department established the Emergency Preparedness Committee (EPC) which is responsible for ensuring that the Department's leadership stays appropriately informed on emergency response and preparedness issues. The EPC recommended and the Department approved the creation of a position within the Office of the Deputy Attorney General that will serve as the Department's full-time "Emergency Preparedness and Crisis Response Coordinator." The EPC has also established several working groups to examine the Department's plans for responding to an incident involving a WMD.

Another example of insufficient counterterrorism coordination among Department components relates to the FBI and ATF response to explosives incidents. Federal law gives the FBI and ATF concurrent jurisdiction over most federal explosives incidents. In an October 2009 review, we determined that the FBI and ATF had developed separate and often conflicting approaches to explosives investigations and explosives-related activities such as training, information sharing, and forensic analysis. These conflicts resulted in unnecessary competition and duplication of effort and also could result in problematic responses to terrorist incidents involving explosives. Moreover,

this lack of coordination is not cost efficient, particularly with regard to training and forensic analysis.

In response to our report, in August 2010 the Acting Deputy Attorney General issued a new protocol designed to improve coordination between the FBI and ATF. The Acting Deputy Attorney General also directed ATF and the FBI to develop a joint plan for consolidated explosives training and to convene a board to discuss how laboratory resources and training could be better coordinated and integrated. We believe these actions are positive steps, but the Department needs to ensure that its protocols are workable and are enforced, and that the FBI and ATF consistently coordinate and cooperate in explosives investigations. In addition, the Department is also addressing other issues raised during our review, including explosive database consolidation, joint training coordination, and laboratory resource allocation.

Another important Department counterterrorism responsibility involves management of the consolidated terrorist watchlist, which is used for many purposes, including by frontline government screening personnel when a known or suspected terrorist requests entry into the United States. In May 2009 the OIG issued an audit examining the FBI's practices for making nominations to the consolidated terrorist watchlist. The audit concluded that the FBI did not consistently nominate known or suspected terrorists to the terrorist watchlist in a timely manner or in accordance with FBI policy, and the FBI also did not update or remove watchlist records as required. Since we issued our report, the FBI has reported that it has improved the timeliness of its nomination activities and has increased its monitoring of field office submissions. The OIG recently initiated a new review of the FBI's management of the watchlist to assess the progress in this area.

The Department also seeks to disrupt terrorist acts by attacking terrorists' financing. The OIG is currently reviewing the FBI and the National Security Division's (NSD) efforts to identify, investigate, and prosecute terrorist-related financing activities. Our audit is also reviewing how the FBI and NSD coordinate efforts throughout the law enforcement community to combat terrorist-financing operations.

In addition to improving information sharing and coordination, the Department should regularly evaluate the balance of resources devoted to counterterrorism and traditional law enforcement activities. In April 2010 we issued a report that examined the process by which the FBI assigns its personnel resources, including how the FBI utilizes agents and intelligence analysts on counterterrorism matters and other investigative areas. The FBI recently informed us that it has implemented our recommendation to develop a more sophisticated resource allocation methodology based on a risk-based analysis of threats and FBI priorities.

The Department is also faced with the challenge of hiring specialized employees essential to its counterterrorism efforts, such as employees with foreign language capabilities or expertise in information technology. In a follow-up review we conducted of the FBI's Foreign Language Translation Program, we found significant amounts of material collected for counterterrorism, counterintelligence, and criminal investigations that had not been reviewed. While the FBI made some improvements, such as in its quality control of translations, the FBI continued to experience problems meeting its goals for hiring linguists proficient in critical languages.

In sum, the Department must continue to improve information sharing and coordination in its counterterrorism efforts, and we believe that counterterrorism remains a critical challenge for the Department.

2. Restoring Confidence in the Department of Justice

We first identified this as a top management challenge 3 years ago. We believe the Department has taken aggressive steps to respond to issues we raised in a series of reports concerning the controversy about the Department's firing of U.S. Attorneys and the politicized hiring of certain career Department employees. However, other concerns persist, such as allegations of prosecutorial misconduct and the Department's ability to address these allegations in a timely and transparent manner.

The Department has been subject to significant criticism for some of its prosecutorial actions, including allegations of misconduct in the prosecution of former Alaska Senator Ted Stevens. In response, the Department has issued new guidance to prosecutors, appointed a coordinator to ensure improved training of prosecutors related to criminal discovery obligations, and expanded training on these topics to include federal law enforcement agents. These initiatives demonstrate commitment by the Department to reduce the risk of prosecutorial misconduct.

We believe, however, that the Department faces additional challenges in ensuring that it has an adequate process to investigate and hold accountable Department attorneys who commit professional misconduct. For example, The Office of Professional Responsibility, (OPR) the internal entity that investigates allegations of prosecutorial misconduct by Department attorneys, has taken steps during the past 2 years to address the backlog in its annual reports and to more promptly post its annual reports containing summaries of its investigations of allegations of prosecutorial misconduct. However, these reports provide only limited details on the cases and the basis of OPR's conclusions. We believe that the timeliness and transparency of the Department's internal processes for addressing allegations of prosecutorial misconduct need improvement to increase public confidence in the Department's ability to address such allegations.

In addition, the Attorney General recently announced that a new Professional Misconduct Review Unit will handle disciplinary actions for career DOJ attorneys. The Unit will review cases involving findings of intentional or reckless professional misconduct by OPR, determine whether these findings are supported by the evidence and applicable law, and where appropriate, refer cases for disciplinary state bar referrals. We note that this newly created unit will similarly need to provide transparency concerning its internal processes and findings in order to allow the public to have confidence that allegations of prosecutorial misconduct and attorney discipline issues are being adequately addressed.

Allegations have also arisen regarding the enforcement of federal voting rights law by the Voting Section of the Civil Rights Division. The OIG is reviewing the enforcement of civil rights laws by the Voting Section. This review will examine the types of cases brought by the Voting Section over time, any changes in Voting Section enforcement policies or procedures, whether the Voting Section has enforced the civil rights laws in a non-discriminatory manner, and whether any Voting Section employees have been harassed for participating in the investigation or prosecution of particular matters.

In September 2010 we also issued a report which found that a significant number of FBI employees had cheated on the FBI exam regarding the Domestic Investigations and Operations Guide (DIOG). The DIOG implements the Attorney General's Consolidated Guidelines for FBI Domestic Operations, which were issued in 2007 and replaced several older sets of guidelines that separately addressed the requirements FBI agents must follow in criminal investigations, national security investigations, and foreign intelligence collection. In our limited investigation of the cheating allegations, we found that a significant number of FBI employees had engaged in some form of cheating or improper conduct on the DIOG exam, some in clear violation of FBI directives regarding the exam. We recommended that the FBI take action regarding those who cheated on the DIOG exam, consider other appropriate steps to determine whether other test takers engaged in similar inappropriate conduct, and also conduct a new exam on the revised DIOG. The FBI is considering what steps it will take in response to our recommendations.

3. Law Enforcement Issues Along the Southwest Border

Organized crime activities along the 2,000-mile U.S. border with Mexico present stark challenges for the Department. To combat violent crime, gun smuggling, drug trafficking, and illegal immigration along the Southwest Border, the Department created the Southwest Border Enforcement Initiative, which seeks to promote cooperation and enhanced intelligence and enforcement activities to attack major Mexican-based trafficking organizations on both sides of the border.

ATF's Project Gunrunner is a key component of the Southwest Border Enforcement Initiative. Project Gunrunner is intended to reduce cross-border drug and firearms trafficking and the high level of violence associated with these activities on both sides of the border. An OIG review of Project Gunrunner found that it has major deficiencies. For example, ATF does not systematically and consistently exchange intelligence with its Mexican and some U.S. partner agencies and that intelligence personnel in ATF's Southwest border field divisions do not routinely share firearms trafficking intelligence with each other. We also found that ATF focuses largely on inspections of gun dealers and investigations of straw purchasers, rather than on higher-level traffickers, smugglers, and the ultimate recipients of the trafficked guns. ATF also is not using intelligence effectively to identify and target firearms trafficking organizations operating along the Southwest Border and in Mexico. According to ATF's June 2007 Gunrunner strategy, tracing guns seized in Mexico is the "cornerstone" of Project Gunrunner. However, we found that despite ATF's efforts it has been unable to expand gun tracing throughout Mexico, and the majority of recovered guns in Mexico were not traced. In September 2010 ATF circulated a revised strategy for combating firearms trafficking to Mexico and related violence. We believe that ATF's strategy can address many of the weaknesses identified in our review, but ATF must still develop an implementation plan – with defined goals, specific actions, and resources.

The OIG's report in June 2010 on the El Paso Intelligence Center (EPIC), a multi-agency intelligence center funded primarily by the DEA, also identified improvements that are needed in intelligence relating to Southwest Border drug smuggling and associated violence. Our review found that EPIC's partner agencies and users regard its products and services as valuable and useful, but we identified weaknesses in EPIC operations and programs. For example, EPIC does not analyze some information that it alone collects. As a result, EPIC may be overlooking drug trafficking trends and patterns that could assist law enforcement agencies in their interdiction investigations and operations. In response to the recommendations in the OIG report, the DEA reported it has taken steps to improve EPIC's systems for sharing information with federal, state, and local law enforcement users, and that EPIC is improving its capability to use seizure information to better identify vulnerabilities along the Southwest Border.

In addition to addressing violent crime and drug trafficking problems, the Department also plays a key role in immigration policy and enforcement along the Southwest Border. We are now conducting a review that is examining the Department's operation of its immigration courts, the backlog in immigration cases, and other issues that affect the Department's enforcement of immigration laws.

4. Civil Rights and Civil Liberties

At the same time that the Department is pursuing its counterterrorism and law enforcement responsibilities, the Department must also seek to protect civil rights and civil liberties. Several of our recent reviews demonstrate the challenges the Department faces in pursuing this balance.

In September 2010 we issued a report concerning allegations that the FBI targeted certain domestic advocacy groups for scrutiny based upon their exercise of rights guaranteed under the First Amendment to the U.S. Constitution. The OIG review did not find that the FBI targeted any of the groups for investigation on the basis of their First Amendment activities. However, the OIG concluded that the predication for opening some of the investigations of individuals associated with the groups was factually weak. In some cases, the FBI extended the duration of investigations involving advocacy groups or their members without an adequate basis, and in a few instances the FBI improperly retained information about the groups in its files. The FBI also classified some investigations related to nonviolent civil disobedience under its “Acts of Terrorism” classification, which resulted in the watchlisting of subjects during the investigation. We made six recommendations to help ensure that if the FBI investigates groups or individuals in connection with their exercise of First Amendment rights, it does so in strict compliance with Attorney General Guidelines. The FBI stated that it concurred with the recommendations in our report, and we believe the FBI should take prompt action to ensure that these recommendations are implemented.

The need for an appropriate balance between the Department’s counterterrorism and law enforcement responsibilities on the one hand, and the need to protect civil rights and civil liberties on the other was also highlighted by an OIG report examining the FBI’s use of exigent letters and other processes to obtain telephone records without legal process. In addition to prior reports on the FBI’s misuse of national security letters (NSLs), in January 2010 the OIG examined the extent of the FBI’s use of exigent letters and other informal requests to obtain telephone records without legal process, which we found to be widespread. Contrary to the statements in the letters, many of the investigations for which the letters were used did not involve exigent circumstances and subpoenas had not been sought for the records. In addition, we found widespread use of other, even more informal requests for telephone records in lieu of appropriate legal process or a qualifying emergency. Our review also found that the FBI’s initial attempts at corrective action were seriously deficient, ill-conceived, and poorly executed. Our report described other troubling practices regarding requests, including improper requests for reporters’ telephone records, inaccurate statements made by the FBI to the Foreign Intelligence Surveillance Act (FISA) Court, improper use of administrative subpoenas, and serious lapses in training, supervision, and oversight.

The OIG is again examining the FBI's use of NSLs and Section 215 orders for business records. Among other issues, our review is assessing the FBI's progress in responding to recommendations from prior OIG reports. In addition, the review is examining the FBI's use of its pen register and trap and trace authority under the Foreign Intelligence Surveillance Act.

In addition, based upon the requirements of Section 702 of the *Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008*, the OIG is examining the number of disseminated FBI intelligence reports that contain a reference to a U.S. person identity, the number of U.S. person identities subsequently disseminated in response to requests for identities not referred to by name or title in the original reporting, the number of targets later determined to be located in the United States, and whether communications of such targets were reviewed. Our review is also examining the FBI's use of and compliance with the targeting and minimization procedures required under FISA.

Also, the OIG is reviewing the Department's use of the material witness warrant statute, 18 U.S.C. Section 3144. Pursuant to the OIG's responsibility under Section 1001 of the USA PATRIOT Act, the review is addressing allegations of civil rights and civil liberties abuses in the Department's post-9/11 use of the statute in the national security context. The review is also examining the Department's controls over the use of material witness warrants, trends in the use of material witness warrants over time, and the Department's treatment of material witnesses in national security cases, including issues such as length of detention, conditions of confinement, and access to counsel.

5. Information Technology Systems Planning, Implementation, and Security

The Department annually spends almost \$3 billion on planning, implementing, and securing its many complex information technology (IT) systems. The Department must plan those systems so that they keep pace with technological innovations and meet the changing IT needs of the Department. At the same time, the Department must seek to implement those systems in a timely and cost-effective fashion and ensure the security of those systems.

The Department has experienced significant problems in developing and implementing these IT systems. Several of the Department's major IT initiatives have failed to meet their objectives after hundreds of millions of dollars were expended. Some of these IT systems have taken so long to develop that they were technologically outdated by the time of implementation.

As evidence of the Department's difficulties in this area, in August 2010 the Office of Management and Budget (OMB) issued a list of 26 high-risk IT projects across the federal government that "experienced problems such as significant cost increases or schedule delays." That list contained three Department projects – the FBI's Sentinel Project to develop a case management information system, the Justice Management Division's Litigation Case Management System (LCMS) project to develop a case management information system for all seven of the Department's litigating divisions, and the FBI's Next Generation Identification (NGI) project to develop a state-of-the-art automated system for sharing fingerprint and other biometric information. We share OMB's concern over these three IT systems.

With regard to Sentinel, when the FBI awarded a contract to Lockheed Martin to develop the system in March 2006 the FBI estimated that it would cost a total of \$425 million and be completed by December 2009. Following the June 2007 completion of the first phase of Sentinel, the FBI revised its project estimations, increasing the budget to \$451 million for a completion in June 2010. In a report issued in October 2010 the seventh of our reports on the development of Sentinel, we found that Sentinel is at least 2 years behind schedule and at least \$100 million over budget. According to its original plan, Sentinel was to be fully completed by now. However, after spending about \$405 million of the \$451 million budgeted for the Sentinel project, the FBI has delivered only two of Sentinel's four phases to its agents and analysts. Moreover, we believe that the most challenging development work for Sentinel still remains.

In September 2010 the FBI briefed us on the FBI's new approach for completing the Sentinel project using an "agile methodology" whereby it would assume direct management of Sentinel development and reduce the role of Lockheed Martin as the prime contractor. Significant concerns relating to the cost, schedule, functionality, and amount of work necessary to complete Sentinel remain under this new approach. We are monitoring the progress of the Sentinel project and will continue to report on its status.

The second high risk Department project identified by OMB, the LCMS project, had been under development since 2004. LCMS, which was intended to be a centralized IT case management system for approximately 14,500 authorized users in seven of the Department's litigating components, was originally estimated to cost about \$42 million and to be completed by December 2010. Yet, in an audit report issued in March 2009 we found that the LCMS project 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. In September 2010 the Department decided to terminate the LCMS project. As a result, millions of dollars in development of this IT system were spent in an unsuccessful attempt

to develop a consolidated system, and the Department still struggles with decentralized, disparate litigation case management systems.

The reasons for the delays, cost overruns, and failure in LCMS were similar to problems we have identified with the implementation of other Department IT systems. Specifically, we found ineffective requirements planning processes, requirements being modified after much work had been done, defects identified in system integration and user acceptance that were costly to correct, and the failure to adequately address in a timely fashion the difficulties the contractor was having in meeting schedule and cost requirements.

The third Department high-risk project identified by OMB is the FBI's Next Generation Identification (NGI) project, which is intended to enhance the existing capabilities of the FBI's current fingerprint identification system and provide searching capability for other types of biometric identification, such as palm prints, iris scans, and tattoos. According to the OMB's "Federal IT Dashboard," the total cost of NGI is expected to be \$3.4 billion through its completion in Fiscal Year (FY) 2017. One of the key challenges for this high-dollar project is to contain its cost while implementing a design that can accommodate new types of biometric evidence as they become available.

Another example of a difficult major IT development project is the Department's Integrated Wireless Network (IWN), a joint project with the Department of Homeland Security (DHS) and the Department of Treasury (Treasury) that is intended to allow federal law enforcement agents to communicate across agencies. This project is seeking to permit interoperability with state and local law enforcement partners and meet mandates to use federal radio frequency spectrum more efficiently. We are currently conducting a follow-up to our March 2007 audit of this project. In our prior audit, the OIG reported that the project, which at that time had a budgeted cost of \$5 billion split among the Department, DHS, and Treasury, was at high risk for failure due to weaknesses in the program's governing structure and the uncertain and inconsistent funding mechanisms that allowed the participating agencies to pursue separate solutions.

In sum, developing IT systems in a timely, cost-effective, and secure way remains a major challenge for the Department. The difficulties the Department is facing are similar to the problems in other federal agencies, and there are no quick and easy solutions. But the Department's track record in this area is uneven, and we believe the Department must focus on this increasingly important challenge.

6. Violent and Organized Crime

While focusing on counterterrorism, the Department must also continue to address violent and organized crime. Organized crime in particular presents challenges for the Department because it is responsible for a wide range of criminal activity, such as manipulation of financial markets, drug trafficking, prostitution and human trafficking, and has taken on an increasingly transnational nature. In addition, gang-related crime has increased in prevalence and scope according to recent assessments by the Department.

To combat violent gangs, among other measures, the Department established the National Gang Intelligence Center (NGIC) and the National Gang Targeting, Enforcement and Coordination Center (GangTECC). In a review we conducted last year, the OIG concluded that these two gang intelligence and coordination centers did not significantly improve the coordination and execution of the Department's anti-gang initiatives. We recommended the Department ensure that their activities are better integrated for both law enforcement and cost efficiencies.

In response to our review, the Department established a partnership of GangTECC and NGIC with the DEA's Special Operations Division and the Organized Crime Drug Enforcement Task Force Fusion Center. GangTECC has relocated to the Special Operations Division and is now operating as the gang section at the Division. In early September 2010 NGIC detailed two full-time analysts to the Fusion Center to function as NGIC's operational intelligence unit. In addition, the Department has proposed merging three Criminal Division sections, including GangTECC and the Criminal Division's Gang Unit, to form the Organized Crime and Gang Section.

While the Department's has shown progress in addressing violent crime, many challenges remain. For example, the FBI Laboratory analyzes forensic DNA from crime scenes, which can provide critical evidence in identifying and prosecuting violent criminals. The OIG examined the FBI Laboratory's growing backlog of forensic DNA cases. This backlog and delay in receiving results can postpone legal proceedings that are waiting on the results of forensic DNA analysis, prevent the timely capture of criminals, prolong the incarceration of innocent people who could be exonerated by DNA evidence, and adversely affect families of missing persons waiting for positive identification of remains. The OIG report noted that the FBI is pursuing various strategies to reduce the forensic DNA case backlog and minimize workflow bottlenecks, such as implementing a laboratory information management system, strategic management of cases, and human resource initiatives.

The FBI is implementing the recommendations we made in our report to help improve the FBI Laboratory's DNA case backlog, and we intend to conduct a follow-up audit in the coming year to determine the FBI's progress in this

area. In addition, we currently are auditing the FBI's progress in addressing the backlog of known DNA samples from federal arrestees, non-U.S. detainees, and convicted offenders.

ATF also plays an important role in combating violent crime by ensuring that federal laws are followed during the sale of guns. For example, ATF conducts regulatory inspections of Federal Firearms Licensees (FFLs) to determine whether FFLs are taking appropriate measures to avoid selling firearms to prohibited persons. In a 2004 review, we found that ATF's inspection program was not fully effective for ensuring that FFLs comply with federal firearms laws because inspections were infrequent and of inconsistent quality, and follow-up inspections and adverse actions were sporadic even when numerous or serious violations were identified. We recommended that ATF improve its inspection program by developing a standard inspection process, revising staffing requirements, improving the comprehensiveness of crime gun tracing by law enforcement agencies, and creating a tracking system to monitor the progress and timeliness of FFL denials and revocations. We are now conducting a follow-up review to assess the changes ATF has made to the gun dealer inspection program since 2004.

7. Financial Crimes and Cyber Crimes

The need to aggressively combat financial crimes and cyber crimes is an increasing challenge for the Department. Financial fraud continues to negatively affect the economy, and the increased use of computers and the Internet in furtherance of financial crimes, as well as the international scope of these criminal activities, has exacerbated the challenge of cyber crime.

In November 2009 a presidential Executive Order created the Financial Fraud Enforcement Task Force (Task Force). The Department described the Task Force as the "cornerstone" of its work in the financial fraud area. Led by the Department, the Task Force combines the work of several agencies to focus on mortgage crime, securities fraud, *American Recovery and Reinvestment Act* (Recovery Act) and rescue fraud, and discrimination against borrowers and consumers. Among other things, the Department is seeking OIG assistance in providing training to federal grantees and contractors on ways to prevent and detect such fraud.

Closely related to the challenge of financial crimes is cyber crime. Rapid technological advances and the widespread use of the Internet make cyber crime an increasing challenge for the Department. The broad range of cyber crime includes intrusions, online fraud, identity theft, and child pornography. Cyber crimes can threaten national security and also result in serious financial consequences for individuals, businesses, and government institutions. Cyber

crime is of particular concern because it can be committed remotely and anonymously, across state and international borders.

Identity theft is a major cause of financial and cyber crime. According to the Department, identity theft was the fastest growing crime in 2008, victimizing more than 10 million Americans. Yet, a March 2010 OIG audit report found that the Department had not developed a comprehensive strategy to combat identity theft. We also determined that the Department had not implemented several of the recommendations stemming from a 2008 follow-up report issued by the President's Identity Theft Task Force. We recommended the Department ensure that its efforts to combat identity theft are better coordinated and are given sufficient priority. Since we issued our audit, the Department has designated a senior official to coordinate the Department's identity theft enforcement efforts, and all relevant DOJ components have designated an official to oversee their components' identity theft enforcement efforts. These officials are working to expand available training and ensure consistency in addressing identity theft victims.

The Department must also focus attention on cyber crime that can threaten national security. The OIG is examining the development and operation of the FBI's National Cyber Investigative Joint Task Force, as well as the capabilities of FBI field offices to investigate national security cyber cases. In addition, we are conducting a separate review on the Department's Justice Security Operations Center, which helps protect the Department's information technology infrastructure and sensitive data from cyber attacks.

8. Detention and Incarceration

Safely, securely, and economically handling the large federal inmate and detainee populations is a difficult challenge for the Department. The Federal Bureau of Prisons (BOP) must contend with overcrowded and aging facilities, higher inmate to staff ratios, the need to address staff sexual abuse of inmates and other types of staff misconduct, and providing jobs and training programs for inmates while they are incarcerated. At the same time, the USMS must find cost-effective detention space in state and local facilities to house tens of thousands of federal detainees awaiting trial or sentencing.

One factor that can affect the safety of inmates and staff is misconduct by correctional officers. In September 2009 the OIG issued a report on the Department's efforts to prevent staff sexual abuse of inmates. Since then, we have continued to assess the BOP's progress in preventing sexual abuse of inmates and providing services to inmate victims. We found that BOP's procedures for safeguarding inmate victims of sexual abuse continue to present concern. As protective measures, the BOP typically isolates inmate victims in special housing units and transfers victims to other institutions. Yet, these measures may further traumatize victims and move them further away from

family members. The BOP stated that as of November 2010 Wardens have been instructed to document the consideration of alternative safeguarding methods for inmate victims of sexual abuse and their rationale if they choose not to use the alternative method. We believe it is important that the BOP review this documentation and provide adequate oversight of the Wardens to ensure that Wardens are using alternative safeguarding methods when possible.

Under the *Prison Rape Elimination Act of 2003*, the Department is responsible for reviewing the proposed standards issued by the National Prison Rape Elimination Commission and issuing national standards to enhance the detection, prevention, reduction, and punishment of prison rape. The Act mandated that the Attorney General publish a final rule adopting national standards by June 2010 one year from the date of the Commission's recommendations. The Department has not yet met this statutory requirement. On February 3, 2011, the Department published its proposed National Standards and requested comments by April 4, 2011. We believe it is essential that the Department move quickly after it receives these comments to implement a final rule to help protect inmates from sexual abuse in prison.

Federal Prison Industries, called "UNICOR," is a government corporation within the BOP that provides employment to staff and inmates at federal prisons throughout the United States. In addition to the challenge of ensuring that UNICOR is financially self-sustaining, the BOP also must ensure that UNICOR facilities provide a safe work environment for inmates and staff. The OIG released a report in October 2010 that found workers and inmates at several BOP institutions were exposed to toxic metals, such as cadmium and lead, and other hazards while working in electronic waste (e-waste) recycling plants operated by UNICOR. Our report, which was completed with the assistance of four federal agencies with expertise in health, safety, and environmental matters, found that UNICOR had significant problems with its e-waste program and exhibited a troubling lack of attention to the safety of staff and inmates who participated in the e-waste recycling operations. However, we found that UNICOR began to implement significant health and safety improvements to its e-waste recycling operations starting in June 2003 that by 2009, with limited exceptions, UNICOR's e-waste operations were being operated safely. The BOP is beginning to implement recommendations in our report that will help UNICOR further improve its compliance with applicable health, safety, and environmental requirements.

The OIG also recently reviewed the BOP's furlough program, which allows BOP inmates authorized absences from institutions without escort. Our review found that the BOP's furlough policy has not been updated since 1998 and does not, for example, require BOP staff to notify victims and witnesses when an inmate is released on a medical furlough. In 2003, the BOP drafted a new furlough policy, but had not implemented it, because the BOP

believed it must negotiate these changes in the policy with the BOP union. The BOP initially estimated that the negotiation and implementation of such a policy would not be finalized until December 2017 a 14-year time lag from 2003 when BOP first drafted its revised policy. The OIG report included seven recommendations to the BOP, including that the BOP develop a more effective mechanism for negotiating with the union on required policy changes.

Since issuance of the report, the BOP has reached an agreement with its union on a new furlough policy. However, BOP has failed to implement some outstanding recommendations from other OIG reports, and BOP attributes its failure to implement these recommendations on the lack of an effective mechanism for negotiating policy changes with the union. The OIG believes the BOP needs to continue to seek improvement in this area.

In addition to incarcerating sentenced inmates at BOP facilities, the Department also must provide safe and affordable detention space for nearly 60,000 federal detainees awaiting trial or sentencing. The USMS is responsible for housing these detainees, and the Department's Office of the Federal Detention Trustee (OFDT) oversees an annual budget of approximately \$1 billion for housing federal detainees. The USMS houses 80 percent of its detainees in non-federal detention space by negotiating contracts, known as Intergovernmental Agreements (IGA), with approximately 1,800 state and local governments.

Over the years, we have expressed concerns that the Department was not effectively negotiating the rates it pays to state and local entities for housing these federal detainees. In FY 2008, the OFDT and USMS made changes in the way they establish jail-day rates with state and local detention facilities. One change involves OFDT using an econometric statistical model, known as eIGA, for estimating a fixed-price range for the jail-day rate for federal detainees housed at state and local facilities. However, negotiated jail-day rates under the new approach appear to give some state and local facilities a large profit to house the detainees. We are conducting an audit reviewing the Department's use of the eIGA process to determine whether it is economically and efficiently setting the jail-day rates. This issue could have significant consequences for the total budget required to house detainees.

We are now completing a review of the Department's implementation of the International Prison Transfer Program, in which inmates who are citizens of treaty nations may be returned to their home countries to serve their sentences closer to their families. We are examining several ways that implementation of the transfer program can be improved to increase the number of participants and reduce delays, which we believe may result in significant cost savings.

9. Grant Management

Grant management has long been a challenge for the Department. Beginning in 2009, the Department faced heightened challenges in grant management, because it was required to award \$4 billion in grants under the Recovery Act at the same time that it had to award the \$3 billion in grant funding contained in the Department's annual appropriations.

As of the end of August 2010, the Department had expended about 52 percent of its Recovery Act funds. The Department handled this increased grant workload without any significant increase in staff. Our reviews have found that, in general, the Department's grant management staff made extraordinary efforts to implement the Recovery Act programs and generally issued the Recovery Act grant funds in a timely, fair, and objective manner.

At the same time, the Department has sought to improve its regular grant management practices. In 2009, shortly after the passage of the Recovery Act, the OIG developed a document, entitled *Improving the Grants Management Process*, which contains a series of recommendations and best practices in grant management that federal agencies should consider implementing. In response, the Department has implemented changes in its grant management practices, including expanding the use of online training opportunities among grant recipients and assisting grantees in determining the appropriate performance information to collect.

At the same time, the Department's Office of Justice Programs' (OJP) Office of Audit, Assessment, and Management has increased its staff and improved its monitoring and oversight of grants. While we believe the Department has taken positive steps toward improving its grant management practices, these changes will take time to fully implement and to incorporate into the Department's regular practices. Moreover, our audit work has continued to identify areas where the Department could further improve its management of grants.

For example, our audit of the Department of Justice Byrne Justice Assistance Grants found that the Department treated competitive grant applicants inconsistently, allowing some grant applications to continue through the competitive process even though they did not meet one or more of the solicitation requirements, while denying other applicants further consideration for the same deficiencies. In addition, we identified some deficiencies in the peer review processes for evaluating grant applications and in documenting the basis for award recommendations. As a result of our recommendations, the Department is revising its procedures to address these deficiencies and to strengthen its oversight of grantees.

We also found that the Department needs to implement better controls to ensure that it correctly scores grant applications. Our audit of the \$1 billion Office of Community Oriented Policing Services (COPS) Hiring Recovery Program found that COPS had used some inaccurate scoring formulas to select grantees, which resulted in grant awards to 45 agencies that should not have received grants, while another 34 agencies that should have received grants did not. In response to the inaccuracies we identified, COPS corrected the scoring formulas so that the correct formulas will be used in the future when making grant awards. Similarly, in our audit of the Office on Violence Against Women's (OVW) administration of \$225 million in grant funding, we found several instances where OVW staff made errors while tabulating peer review scores of individual applications.

We also found in our Recovery Act audits that the Department was not consistently documenting its reasons for making discretionary awards and was not explaining why some applications that were ranked lower by peer reviewers were awarded grants over applications that peer reviewers had ranked higher. Although the Department is not required to follow the rankings of peer reviewers in awarding grants, we believe that the Department should document its rationale for award decisions that deviate from peer review results.

In sum, while the Department has demonstrated a commitment to improving its grant management process, considerable work remains before managing the billions of dollars the Department awards annually in grants is no longer a top challenge for the Department.

10. Financial Management

Financial management has been a top management challenge for the Department since 2003. It is important to recognize that the Department has made significant improvements in its internal controls over financial reporting and management. Yet, we believe the need for accurate, near real-time financial information continues to present management challenges for the Department.

For FY 2010, the Department again earned an unqualified opinion and improved its financial reporting. For the fourth straight year the financial statement auditors did not identify any material weaknesses at the consolidated level. Department components also reduced component significant deficiencies from eight in FY 2009 to four in FY 2010.

As in past years, however, much of this success was achieved through heavy reliance on contractor assistance, manual processes, and protracted reconciliations, primarily as a result of the Department's decentralized structure. This 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 five major accounting systems that are not integrated with each other. In some cases, the components' outdated financial management systems are not integrated with all of their own subsidiary systems and therefore do not provide automated financial transaction processing activities necessary to support management's need for timely and accurate financial information throughout the year. We remain concerned about the sustainability and cost of these ad hoc and labor-intensive efforts, which are often overlooked in measuring the true costs of maintaining the current financial management systems.

The Department has long recognized the need for a Department-wide financial management system and has sought to implement a Unified Financial Management System (UFMS) to replace the disparate major accounting systems currently used throughout the Department. 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.

Yet, only the DEA and ATF have fully implemented the UFMS. While that is a significant achievement, both of those organizations had the Department's most modern legacy financial management systems. Therefore, the central issue to this challenge remains largely unaddressed because the Department's other components, particularly the USMS and FBI, continue to use non-integrated and, in some cases, antiquated financial management systems. Implementation at the USMS began in FY 2010 and will continue through FY 2012, and implementation planning for the FBI began in FY 2011.

Conclusion

In sum, the Department has made progress in addressing many of its top management challenges, but improvements are needed in important areas. These challenges are not easily resolved and will 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.