OIG Top Management and Performance Challenges in the Department of Justice

November 13, 2009

MEMORANDUM FOR THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management and Performance Challenges in the Department of Justice

Attached to this memorandum is the Office of the Inspector General's (OIG) 2009 list of top management and performance challenges facing the Department of Justice (Department). We have prepared similar lists since 1998. By statute, this list is required to be included in the Department's annual Performance and Accountability Report.

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

Attachment

This page intentionally left blank.

Top Management and Performance Challenges in the Department of Justice – 2009

1. Counterterrorism: Counterterrorism remains the highest priority of the Department of Justice (Department or DOJ). While recent terrorism arrests demonstrate the Department's focus on and progress in its counterterrorism efforts, the Department in general and the Federal Bureau of Investigation (FBI) in particular still face significant challenges in fully performing this critical mission.

For example, in May 2009 the Office of the Inspector General (OIG) issued an audit that examined the FBI's practices for making nominations to the consolidated terrorist watchlist. The 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. The 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. However, the OIG audit concluded that the FBI did not consistently nominate known or suspected terrorists to the consolidated terrorist watchlist in accordance with FBI policy and did not update or remove watchlist records as required.

The deficiencies identified in this audit followed our findings in a March 2008 audit report that watchlist nominations from FBI field offices often were incomplete or contained inaccuracies, which caused delays in the nominations process. Although the FBI agreed with our March 2008 recommendations and began taking corrective actions, our May 2009 audit report identified continued internal control weaknesses that contributed to incomplete and inaccurate watchlist records. In the May 2009 report, the OIG made 16 new recommendations to the FBI regarding nominations to, modifications of, and removal of identities from the consolidated terrorist watchlist, and the FBI agreed to implement all of these recommendations.

In another follow-up review, the OIG examined the FBI's Foreign Language Translation Program. The FBI's ability to timely translate the large amount of foreign language materials it regularly collects is critical to national security. OIG audits in 2004 and 2005 found significant deficiencies in the FBI's Foreign Language Translation Program. The OIG's October 2009 audit found that many of these deficiencies have not been fully corrected. Specifically, we found that the FBI continued to have significant amounts of unreviewed foreign language materials in counterterrorism and counter intelligence, the FBI's highest priority investigative areas. Moreover, the FBI still does not have an automated means for assessing the amount of material it collects for translation. In addition, while the FBI has improved its compliance with quality control requirements and begun requiring experienced linguists to have a formal quality control review performed once every four quarters, we identified numerous linguists who have not had the quality of their work reviewed for over 3 years. Moreover, the FBI continues to fall short in meeting its linguist hiring goals, resulting in a decrease in the number of linguists since 2005 at the same time there has been an increase in the amount of material for translation. The OIG

made 24 new recommendations to assist the FBI in improving the management of its Foreign Language Translation Program.

As Attorney General Holder noted in his congressional testimony, communication and information sharing are critical to the Department's counterterrorism strategy. However, in a recent audit the OIG found that the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are not adequately coordinating their explosives-related operations. The OIG audit found that jurisdictional disputes occur between the FBI and ATF, delaying explosives investigations and resulting in a disjointed federal response to explosives incidents, some of which involve terrorist incidents. Despite an Attorney General memorandum in August 2004 and a 2008 Memorandum of Understanding between the FBI and ATF, allocation of investigative authority between the two agencies is unclear, and disputes between the agencies have continued regarding lead agency authority for federal explosives investigations.

The FBI's development of an automated system to track terrorist threats and suspicious incidents was intended to disseminate immediate threat information to the FBI's law enforcement and intelligence partners. An OIG November 2008 report examining the FBI's Guardian Threat Tracking System (Guardian) revealed shortcomings in the accuracy, timeliness, and completeness of the information entered in Guardian. The deficiencies identified by this audit resulted in threat information not being made available to all Guardian users. The FBI has recently developed E-Guardian, a companion system to provide state and local law enforcement with the capability to share local terrorism incident information with the FBI and to receive nationwide unclassified terrorism incident information from the FBI. Following our review, the FBI officially launched E-Guardian in January 2009.

In accord with the *National Strategy for Combating Terrorist Use of Explosives in the United States*, the OIG evaluated the FBI's efforts to prepare for weapons of mass destruction (WMD) threats, including how the FBI ensures that WMD Coordinators in FBI field divisions identify WMD threats and attacks. Our audit found that although the FBI has established a WMD Coordinator position in each of its field divisions to serve as the point-person on WMD matters, the WMD Coordinators need to be more involved in the process used by each field office to identify and forecast WMD threats and vulnerabilities. We also recommended that the FBI enhance day-to-day coordination between WMD Coordinators and field office Intelligence Analysts. Additionally, we found that the FBI needs to develop qualification standards and training plans for field division personnel charged with preventing and detecting WMD threats. The OIG made 13 recommendations for the FBI to enhance the responsibilities and training of its WMD Coordinators and to help improve field division WMD-related efforts.

The OIG is currently evaluating the FBI's efforts to investigate national security cyber intrusion cases. We are assessing the efforts of the FBI National Cyber Investigative Task Force to address potential national security cyber intrusion threats. In addition, our audit is examining the FBI field offices' capabilities to investigate national security cyber intrusion cases.

Another recent OIG review determined that the Department had failed to appropriately perform its critical legal function during the early phases of a controversial intelligence gathering activity. In the weeks following the terrorist attacks of September 11, 2001, the President authorized the

National Security Agency (NSA) to conduct a classified program to detect and prevent further attacks in the United States. The program was reauthorized by the President every 45 days, with certain modifications. The activities carried out under these authorizations were referred to as the President's Surveillance Program (PSP). In July 2009, the OIG completed a 407-page classified report that examined the Department's controls over and use of information related to the PSP and the Department's compliance with legal requirements governing the PSP. The OIG report focused in particular on the Department's role in providing legal advice concerning the Program and on the FBI's role as a consumer of information from the Program. In conjunction with four other Intelligence Community OIGs, we also issued a 40-page summary of the unclassified material from the OIG reports.

In our review, we found that only one Office of Legal Counsel (OLC) attorney was read into the PSP during its first year and a half of operation. The OIG concluded that it was extraordinary and inappropriate that a single attorney was relied upon to conduct the initial legal assessment of the PSP, and that the lack of oversight and review of his work, as customarily is the practice of OLC, contributed to a legal analysis of the PSP that at a minimum was factually flawed. The OIG also concluded that the limited access to PSP information also undermined the Department's ability to perform its critical legal function during the PSP's early phase of operation.

The OIG also sought as part of its review to assess the role of PSP-derived information and its value to the FBI's overall counterterrorism efforts. Our interviews with FBI agents and analysts responsible for handling PSP information generally were supportive of the program as "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward," although most PSP leads were determined not to have any connection to terrorism. The OIG concluded that although PSP-derived information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts.

In sum, while the Department continues to make counterterrorism its top priority, recent OIG reviews have highlighted the continuing challenge for the Department in addressing this critical area.

DOJ RESPONSE:

The Department of Justice's highest priority and most important responsibility is to protect our national security. To fulfill that responsibility effectively and efficiently, the Department's leadership has identified several areas of potential improvement in this field, many of which were identified in the Inspector General's recommendations. The Department has already begun implementation of these new procedures and policies where appropriate.

The Department leadership and the FBI are on track to resolve all 24 OIG report recommendations directed to the FBI. In fact, many of OIG's recommendations are consistent with measures already taken by the Department as part of its overall strategic plan for improving the Departments overall management and efficiency. For instance, the FBI has successfully closed four of the seven recommendations in the OIG's February 2008 report and nine out of sixteen recommendations in the May 2009 report. Of particular

note, the Department and the FBI agree that the appropriate handling of watchlists is an important responsibility that must be addressed effectively and consistent with the law. As such, the FBI has reorganized the Terrorist Review and Examination Unit, which has oversight responsibility for watchlisting of FBI investigative subjects. To streamline the process and establish internal controls, the Unit was divided into teams to provide for more effective overall management. Similarly, a Metrics Team and Quality Assurance Team now formally identify watchlisting problems and ensure each issue is corrected in a timely manner. Compliance with watchlisting policy is now measured and reported on a monthly basis, which includes current trends and best practices observed across the FBI. The results continue to improve with compliance rates rising from 56 percent to 86 percent for timely case openings, and 64 percent to 89 percent for timely case closings. After a problem is identified, direct follow-up now ensures 100 percent of these issues are tracked and resolved. In addition, the FBI's draft watchlisting policy is nearly complete; it incorporates clear guidance for watchlisting FBI investigative subjects, non-investigative subjects, and those identified via our foreign partners. Once the policy is approved, an additional seven recommendations will be ready for closure. This review is ongoing and requires examination of approximately 80,000 records with completion expected by the end of the 2009 calendar year.

The FBI is encouraged by the progress made in collecting material for timely counterterrorism translation. In fact, the OIG's report on the FBI's Foreign Language Translation Program documents the significant improvements the FBI has made in the past four years in this program. That said, we take the OIG's concerns about this program very seriously, and it recognizes that much work is needed to improve the FBI's foreign language translation programs. The Department is fully committed to undertaking this effort. With regard to counterintelligence collections, the Department and the FBI will continue to carefully prioritize and monitor the most important material. Overall, the Department is confident that its language translation capabilities, including recruiting, hiring, training, and retaining effective linguists, have substantially improved.

The FBI is also working to decrease its audio backlog. The FBI is currently procuring and testing a new system that will facilitate the centralized management of this data. This system will enable the FBI to gather accurate statistics on audio backlog, which may demonstrate that the backlog is significantly less than that reported in the OIG report. With respect to unreviewed electronic files, moreover, the FBI takes an analytic approach to handling these files and uses advanced technology to assist in the identification and prioritization of those electronic files that are most relevant to the FBI's mission. To further improve upon this approach, the FBI is developing new technological and management tools that will reduce the volume of electronic files requiring review and translation.

In addition, the Department is working to resolve any residual challenges to coordination of explosives investigations. The Department agrees with OIG that this is an important concern. Indeed, the Department recognizes the critical importance of a well-coordinated and effective response to explosives incidents. Equally important is the need to adequately train our personnel and ensure effective information sharing with all

appropriate components and law enforcement partners. The OIG Report documents the Department's challenges concerning the most efficient application and balance of its explosives enforcement assets and responsibilities and offers some specific remedies to those challenges. The Department agrees with the recommendations that are reflected in the body of the Report and is currently taking steps to address each of those recommendations. While we may modify the ways in which we implement some of those recommendations in order to achieve the most successful and efficient resolution to the matters under review, the Department is committed to taking specific, effective, and measurable actions that address the concerns identified by OIG, including: coordinating efforts; determining roles and responsibilities during a federal response to an explosives incident (such as determining lead agency jurisdiction); and managing shared responsibilities such as information sharing, explosives training, research and technology development, outreach to the public and industry, and use of certain laboratory resources.

Furthermore, the Department remains committed to sharing terrorism information with federal, state, local, and tribal law enforcement partners. To that end, the FBI has created an unclassified version of its Guardian program called eGuardian. The eGuardian system will facilitate situational awareness with respect to potential terrorism threats and activity by providing law enforcement partners with a suspicious activity reporting (SAR) system accessible via Law Enforcement Online. Sharing information within the eGuardian network should eliminate the jurisdictional and bureaucratic impediments that otherwise delay communication and dissemination of information that could potentially affect the nation's security posture. Indeed, the eGuardian system will offer the United States law enforcement community a previously unrealized degree of connectivity with regard to the collection and dissemination of suspicious activity and threat reporting. The eGuardian system also will provide state and local users a uniform platform to cause actionable information with a potential terrorism nexus to be analyzed at the state Fusion Center level and reported to the Joint Terrorism Task Forces via the classified Guardian system.

Consistent with the OIG report entitled, "The Federal Bureau of Investigation's Weapons of Mass Destruction Coordinator Program," the FBI has made strides to professionalize and increase the competency of our WMD Coordinators and Intelligence Analysts through a formalized training curriculum and select performance requirements. These improvements build on the many strengths that the OIG report identified in this area. That said, the Department concurs with the thirteen recommendations in the OIG's report, and are in the process of creating increased professional opportunities and development for WMD Coordinators and Intelligence Analysts who prioritize WMD threats and coordinate activities within their respective domains. Through collaboration with the FBI's Directorate of Intelligence, the WMD Directorate will implement procedures and practices to address intelligence exchange, performance, tracking, and training relevant to effective domain management.

Finally, the Department adheres to longstanding OLC practice requiring that legal questions are fully and appropriately examined by more than one OLC attorney and that all written legal advice is approved by at least two senior-level attorneys. All opinions and other signed memoranda containing legal advice are now written or approved by the head

of the Office and at least one Deputy Assistant Attorney General. Indeed, in almost all cases, such documents are reviewed by the head of the Office and at least *two* Deputy Assistant Attorneys General. Accordingly, OLC regularly insists that, wherever possible, the head of the Office and at least one Deputy Assistant Attorney General are cleared into compartmented national security programs about which OLC is asked to provide legal advice.

2. Restoring Confidence in the Department of Justice: In the past several years, the Department of Justice has faced criticism for politicization in the hiring of career officials, dismissal of U.S. Attorneys, and alleged misconduct in several prosecutions. These issues involve a small number of the many important responsibilities the Department handles and also involve only a small percentage of the Department's dedicated work force. Yet, these issues can affect confidence in the objectivity and non-partisanship of the Department of Justice as a whole and can undermine the confidence in the many critical decisions the Department makes. Consequently, restoring confidence in the Department is an important and ongoing challenge.

In 2008, the OIG and the Department's Office of Professional Responsibility (OPR) issued two joint reports which substantiated serious allegations of improper politicized hiring practices in the hiring processes for career attorney positions in the Department's Honors Program and Summer Law Intern Program and in hiring for career positions by staff in the Office of the Attorney General.

Another joint OIG/OPR report issued in 2008 concluded that partisan political considerations played a part in the Department's removal of U.S. Attorneys in 2006. We concluded that the process used to select the U.S. Attorneys for removal was fundamentally flawed, and the oversight and implementation of the removal process by the Department's most senior leaders was significantly lacking. The Department's removal of the U.S. Attorneys and the controversy it created severely damaged the credibility of the Department and raised doubts about the integrity of Department prosecutorial decisions.

In January 2009, the OIG and OPR issued another joint report which found that Bradley Schlozman, the former Acting Assistant Attorney General (AAG) for the Civil Rights Division, had hired lawyers for career positions in the Division and had made personnel decisions based on attorneys' political or ideological affiliations. Our investigation concluded that in doing so Schlozman violated federal law (the *Civil Service Reform Act)* and Department policy, both of which prohibit discrimination in federal employment based on political affiliations.

As noted in our 2008 analysis of the Department's top management challenges, the Department has taken significant steps to correct problems we found in these four reviews. For example, the Department returned the responsibility for hiring career employees from politically appointed officials to career employees, and the Department provided training for these selecting officials. The Department also developed new briefing and training materials for Department political appointees that stresses that the process for hiring career employees must be merit based, and that ideological affiliations may not be used as a screening device for discriminating on the basis of political affiliations. In addition, the former Attorney General appointed a special counsel to

investigate whether any crime was committed related to removal of the U.S. Attorneys, and that investigation is ongoing.

However, the Department has still not responded to the OIG's recommendation that the Department clarify its policies regarding the use of political or ideological affiliations to select career attorney candidates for temporary details within the Department. The Department's guidance on this issue is inconsistent, and we recommend that the Department clarify the circumstances under which political considerations may and may not be considered when assessing career candidates for details to various Department positions.

While the Department has taken important steps on the issues of politicized hiring and firing that we identified in our reports, the Department is also faced with significant issues arising from several recent prosecutions, including the prosecution of former Alaska Senator Ted Stevens. In April, after a jury trial, the Department moved to dismiss the indictment charging Stevens with violating government ethics laws. According to the Department, it dismissed the indictment after trial because it concluded that certain information should have been provided to the defense for use at trial. The Department's handling of this case created concern about the prosecutors' adherence to professional standards of conduct. 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. For example, judges in the District of Massachusetts, the Northern District of Alabama, and elsewhere have questioned the professional conduct of Department prosecutors. The judges expressed concerns primarily about prosecutors failing to disclose exculpatory or impeachment information to the defense and the manner in which prosecutors handled certain informants and witnesses.

Other issues regarding the professional responsibility of the Department's attorneys have also been reported on during the past year, including the OIG report about the President's Surveillance Program, which is discussed in the previous management challenge. In another matter involving national security issues, allegations have arisen concerning the role Department attorneys played in providing legal advice relating to enhanced interrogation techniques. A report by OPR on this issue is pending.

In response to these concerns about prosecutorial conduct, the Department has taken a variety of actions. For example, in August 2009 the Department created a working group to consider best practices for prosecutors in fulfilling their disclosure obligations. The Department also announced a new training program in which all United States Attorneys' Offices have been directed to appoint a Discovery Trainer who will be required to attend a training conference, which will focus on discovery issues, including Brady-Giglio, Rule 16, Jencks, informants, and agent and attorney notes. The Discovery Trainers will then present mandatory training to all Assistant U.S. Attorneys in their districts by the end of the year. In addition, the Department plans to hire an official to oversee this training process, assess the need for additional improvements, and ensure continued implementation of the reforms.

In short, we believe that restoring confidence in the professionalism of the Department is a continuing challenge. 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, it must remain focused on this critical issue.

DOJ RESPONSE:

As noted by the OIG, the Department already has taken substantial steps to restore confidence in the professionalism and integrity of its work. Attorney General Holder has repeatedly said that "we must restore the credibility of this Department, which has been so badly shaken by allegations of improper political interference." The Department has maintained a singular focus on ensuring that its work is done without regard to political party or ideology. Indeed, the Attorney General explained on the day he was sworn into office, "We must fulfill our duties faithfully, and apply the law evenhandedly, without regard to politics, party or personal interest." In short, the Department of Justice is fully committed to restoring confidence in its work and reputation by upholding its vital traditions of independence, non-partisanship, transparency, and fealty to the law.

To that end, the Department has re-established its commitment to non-partisan hiring and enforcement. For instance, as part of its continuing effort to address hiring concerns, the Department invited attorneys who applied to the Department's Honors Program in 2006 (and may have been excluded for reasons of political affiliation) to apply again. Of the 167 attorneys who were offered this opportunity, 63 accepted interviews, 54 actually interviewed (9 withdrew prior to or after interviewing), and 15 were hired. Two candidates declined offers of employment. In addition, the Department is working through the legal issues regarding implementation of a policy concerning the selection of career attorney candidates for temporary details to confidential, policy-determining, policy-making, or policy-advocating positions within the Department and expects to clarify the policy in the current fiscal year.

The Department has taken various measures to help ensure that its attorneys are aware of, and act in accordance with, their professional obligations. The Department remains committed to meeting the highest standards during discovery—as in every stage of litigation—in its criminal and civil cases alike. In addition to the prosecutorial working group noted by the OIG, a parallel working group is examining the Department's civil discovery practices and capabilities. These working groups will clearly demonstrate that the goal of the United States Justice Department is not to keep count of convictions or civil judgments, but rather to be accountable for justice.

The Department is devoting significant resources to build on the training programs already in place to ensure our attorneys are the best trained in the field. As noted by the OIG, we are developing a comprehensive discovery curriculum for prosecutors, and we plan to provide discovery training to federal prosecutors, paralegals, and law enforcement agents. The Department recently convened a three-day discovery and case management course at the National Advocacy Center in Columbia, South Carolina, to train the "discovery experts" from all 93 U.S. Attorneys offices and the Department's litigating

components. Now that we have "trained the trainers," they will go back to their respective offices and provide in-depth training for new and current prosecutors.

Additionally, based on the Working Group's recommendations, the Department has designated "discovery experts" in all 93 United States Attorney's offices and in all the criminal litigating components of the Department. These discovery experts are senior members of their offices who have received additional training and will be an invaluable resource to their colleagues to address individual discovery issues and providing training to new prosecutors on an ongoing basis.

The Department also is creating an Intranet site that will serve as a central repository for discovery materials, including recent court decisions, training materials, sample case management tools and other materials to help prosecutors comply with their obligations to the defense and the court. The Computer Forensics Working Group will be reconvened to address the problem of properly cataloging electronically stored information recovered as part of federal investigations as well as the adequacy of computer forensic resources that support federal criminal investigations. In addition to those improvements we have already begun to implement, we agree with the OIG in the importance of this mission, and will continue to dedicate the Department's effort and resources to affirm the public's confidence in Department's integrity and professionalism.

3. Recovery Act Funding and Oversight: In addition to the traditional challenge the Department faces each year in managing more than $3 billion in grant funds, the Department has received additional grant funds from the *American Recovery and Reinvestment Act of 2009* (Recovery Act). The Recovery Act, which provides $787 billion in total funding intended to provide a stimulus to the economy, includes $4 billion in Department grant funding to enhance state, local, and tribal law enforcement; to combat violence against women; and to fight Internet crimes against children. The distribution of Recovery Act Funding among the various Department grant programs is shown in the chart below.

RECOVERY ACT-FUNDED PROGRAMS

Appropriations Title	Department Component	Total Funding	Allocation to Component Programs and Purpose
State and Local Law Enforcement Assistance, Recovery Act	Office of Justice Programs (OJP)	$2.765 billion	**$2 billion** – Edward Byrne Memorial Justice Assistance Grant (JAG) Program funding for a broad range of activities to prevent and control crime and improve the criminal justice system.
			$225 million – Edward Byrne Competitive Grant Program funding to help communities address targeted needs.
			$225 million – Grant funding for construction/renovation of correctional facilities on tribal lands.
			$125 million – Grant funding for rural law enforcement activities related to preventing and combating drug-related crime.
			$40 million – Grant funding for law enforcement activities along the southern border and in high-intensity drug trafficking areas (includes $10 million of pass-through funding for ATF).
			$50 million – Grant funding for initiatives related to Internet crimes against children.
			$100 million – Grant funding for victim compensation and assistance.
Community Oriented Policing Services, Recovery Act	Office of Community Oriented Policing Services (COPS)	$1 billion	**$1 billion** – Grant funding for the COPS Hiring Recovery Program (CHRP) to hire and rehire additional career law enforcement officers.
Violence Against Women Prevention and Prosecution, Recovery Act	Office on Violence Against Women (OVW)	$225 million	**$175 million** – Grant funding to support the work of state, local, and tribal governments and domestic violence and sexual assault coalitions.
			$50 million – Transitional Housing Assistance Grant Program funding to provide victims of crimes against women with transitional housing services and to move such individuals into permanent housing.
Salaries and Expenses, Office of Justice Programs, Recovery Act	OJP	$10 million	**$10 million** – Administrative funding to OJP, further allocated as follows: OJP $7.0 million COPS $2.5 million OVW $ .5 million
Salaries and Expenses, Recovery Act	Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)	(Funding received through OJP)	**$10 million** – Funding to support Project Gunrunner for the Southwest Border Initiative to reduce cross-border drug and weapons trafficking and violence on the border.
Office of the Inspector General, Recovery Act	Office of the Inspector General (OIG)	$2 million	**$2 million** – Funding for oversight activities and functions related to Recovery Act funding.
Totals	**Five Components**	**$4.002 billion**	**($3.990 billion or 99.7 percent is for grants)**

Source: U.S. Department of Justice Draft Agency Plan for Management of Recovery Act Funds

The management and oversight of Recovery Act funds is a significant challenge for the Department because the Department 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. For example, the Department's Edward Byrne Memorial Grant Program Justice Assistance Grant Program (JAG Program) received $2 billion in Recovery Act funds to be awarded to state and local governments to support a broad range of activities aimed at preventing and controlling crime and improving the criminal justice system. This money is approximately 4 to 18 times more than the annual funding that the Department awards through the JAG Program each year ($496 million in fiscal year (FY) 2005, $202 million in FY 2006, $305 million in FY 2007, and $108 million in FY 2008).

Yet, despite the significant influx of Recovery Act money that the Department must oversee, the number of grant administrators who award and oversee these grant programs has not significantly increased. Therefore, these same grant administrators who already were challenged to provide adequate oversight of annual JAG grant funds face additional challenges in overseeing the Recovery Act funding.

The Department plans to monitor grant recipients through a combination of oversight methods, including on-site program and financial reviews, desk reviews of recipient reports, and analyses of single audit results. Effective monitoring by each of the Department's three grant-making agencies is crucial to the early identification and correction of problems among the Recovery Act grant recipients. As discussed in more detail in the management challenge on grant management, the Office of Justice Programs (OJP) has taken steps to improve its monitoring efforts by strengthening its Office of Audit, Assessment, and Management (OAAM). The OIG will be assessing the effectiveness of these improvements as we audit the Department's oversight of Recovery Act awards.

In another example of the Recovery Act challenge, the Department's Office of Community Oriented Policing Services (COPS) received an additional $1 billion in Recovery Act funds in 2009 for the hiring of career law enforcement officers. This is approximately three times larger than the average annual appropriations for COPS grants over the past 5 years. In addition, the focus of COPS grants in recent years had shifted from hiring police officers to providing funds for law enforcement equipment and technology. The result is that COPS must now manage a $1 billion Recovery Act hiring program with staff that may need to be retrained and refocused in overseeing a significantly larger number of hiring grants. Yet, the COPS' staff to administer its grant programs has declined from 214 in 1999 to 116 in October 2009. While COPS has recently increased its staffing in response to the Recovery Act challenges, as of September 2009 only eight grant monitors were on board in the COPS Grant Monitoring Division. Consequently, we are concerned with COPS' ability to provide effective grant management over thousands of grants with such a limited number of staff.

To address the management challenges presented by the infusion of Recovery Act funding, the Department has taken important steps. These steps include:

- OJP has implemented a High Risk Grantee Designation program to assess a grantee's risk before awards are made and to strengthen its monitoring of these grantees.

- COPS created the 2009 COPS Hiring Recovery Program Grant Owner's Manual to assist grantees with the administrative and financial matters associated with the grant.

- COPS plans to offer free access to interactive online training courses and resources to help grantees manage their grants and implement their community policing plans under the Recovery Act.

- The Office on Violence Against Women (OVW) held several pre-award conference calls with potential applicants to clarify Recovery Act solicitation requirements, and OVW is developing a monitoring plan for Recovery Act awards.

At the same time, the OIG has taken proactive steps to help the Department in its oversight of Recovery Act money. For example, the OIG has provided Department officials and grant administrators with training on the grant management process in an effort to prevent fraud or misuse of the funds. Since enactment of the Recovery Act in February 2009, the OIG has trained over 800 Department grant officials in order to raise awareness of the specific fraud, waste, and misuse risks related to Recovery Act and other grant funding.

The OIG also has reviewed draft documents prepared by the Department, including both pre-award documents for grant applicants and post-award guidance for grant recipients, and provided advice to Department officials regarding these documents. We have also provided guidance to the Department regarding appropriate internal controls and best practices when awarding and overseeing Recovery Act funds.

In addition, the OIG prepared a document, entitled *Improving the Grant Management Process*, which contains recommendations and best practices that OIG auditors and investigators have identified which granting agencies should consider adopting to reduce waste, fraud, and abuse in grants. We distributed this document to Department grant managers and posted it on our website, and we also provided it to other Departments involved in grant activities.

The OIG also has initiated several reviews to examining DOJ's management of Recovery Act funds. For example, we have ongoing audits on the the Byrne formula and competitive grant programs; OJP's grants for correctional facilities on tribal lands; COPS Hiring Recovery Program; OVW's Recovery Act programs; and ATF's use of Recovery Act funds for Project Gunrunner, a national initiative to reduce firearms trafficking to Mexico. In our initial report on ATF's Project Gunrunner, we concluded that some of ATF's planned activities do not appear to represent the best use of Recovery Act resources to reduce firearms trafficking.

In addition to our reviews of the Department's management and oversight of Recovery Act funds, we also are auditing samples of individual grantees that received Recovery Act awards. Our audit work is being performed in phases, and we are providing grant administrators significant findings from our work as quickly as possible so that these issues can be promptly addressed.

Special agents from the OIG Investigations Division field offices and auditors from our regional audit offices have reached out to state administering and oversight agencies regarding DOJ

Recovery Act funds. In these meetings, we discuss our work and encourage these officials to report to us any evidence of potential waste, fraud, or abuse in the use of Department funds. In sum, grant management has been a long-standing challenge for the Department, and this year even more so when the Department must award and oversee an extra $4 billion in grant funds under the Recovery Act. While the Department has taken positive steps on oversight of Recovery Act funds, it must continue to focus on the challenge of protecting these funds from fraud, waste, and abuse.

DOJ RESPONSE:

The Department has taken several proactive steps to ensure sufficient monitoring of the Recovery Act grants and contracts. Having recognized the same management challenges identified by the IG, the Department has put into place substantial monitoring measures to ensure effective distribution of these grant funds.

For example, shortly after the Recovery Act was enacted, the Department directed our OJP bureaus and program offices, the Office of the Chief Financial Officer, and the OAAM to conduct programmatic, financial, and administrative monitoring of Recovery Act grants and contracts from award through the close-out of program activity. The Department will conduct on-site programmatic monitoring of 30 percent of the Recovery Act grant funding during the life of the Recovery Act awards. To ensure that the 30 percent threshold results in on-site monitoring for an adequate number of Recovery Act grants, we will also conduct on-site monitoring for at least 10 percent of the number of open awards by program until all Recovery Act grants are closed, with the exception of the Byrne Justice Assistance Grant Program, which will be at five percent due to the large volume of awards. The Department has directed the OAAM to then assess the level, quality, and completeness of monitoring conducted by the OJP bureaus and program offices, as well as the COPS Office.

In addition, since the enactment of the Recovery Act, OJP has been working closely with the OIG. The Department has a risk management plan in place, which includes identifying and closely monitoring high-risk grantees. We have proactively engaged the OIG to consult on methods to prevent the risk of waste, fraud, and abuse in the grant application and award process. For the duration of the Recovery Act post-award period, OJP and Department leadership will continue to meet routinely with the OIG to discuss programmatic progress and implementation issues, as well as to discuss strategies for improving grant program management across the Department.

The Department also has engaged OAAM to conduct program assessments of Recovery Act grant programs to measure performance against intended outcomes and assess compliance with Recovery Act requirements and guidelines. Using existing processes and procedures, program assessments will be designed to examine measures implemented by program offices and/or grantees to aid in enhanced transparency and accountability (e.g., performance measures tracking, compliance with grant requirements). In FY 2010, OAAM will review two Recovery Act programs, the Bureau of Justice Assistance's (BJA) Assistance to Rural Law Enforcement to Combat Crime and Drugs

Program and State and Local Law Enforcement Assistance Program for Combating Criminal Narcotics Activity Stemming from the Southern Border of the United States. These were selected after consultation with the DOJ OIG to avoid duplication of program reviews.

The Department leadership has also tasked the Antitrust Division to launch an "Economic Recovery Initiative" to assist federal, state, and local agencies receiving Recovery Act funds. This Initiative will help ensure that measures are in place to protect procurement and program funding processes from bid-rigging and other fraudulent conduct, as well as ensure that those who seek to corrupt the competitive bidding process are prosecuted to the fullest extent of the law. A principle aim of the Initiative is training government officials to prevent, detect, and report efforts by parties to unlawfully profit from stimulus awards before those awards are made and taxpayer money is wasted.

In addition, DOJ has implemented the following improvements to its grant management: The High Risk Grantee Designation program employed through OJP is being applied to grants awarded by both OJP and OVW. COPS is incorporating OJP's High Risk Grantee Designation program into its grant process as well. All three grant-making components have developed plans to implement the OIG's suggestions for improving the grant management process contained in the February 2009 report entitled, "Improving the Grant Management Process." Moreover, Department leadership now requires periodic reports from the grant components to assess their progress in implementing the suggestions in the OIG's report, and status reports on open OIG audits.

Finally, ATF has been able to expand Project Gunrunner through the financial support of the Recovery Act and other recent appropriations. ATF has taken a series of steps to identify new locations for Gunrunner teams. These include creating a new staffing structure, ensuring Spanish proficiency in more staff along the southwest border, and establishing program methodologies to evaluate the impact of these resources. ATF has considered the recommendations in OIG's Interim Review of ATF's Project Gunrunner and, for each one, has either created an action plan to address the noted deficiencies, or has studied the issue in light of the OIG's concern and provided further justification for its approach. In one instance, ATF is still considering the best approach to address the OIG's concern. Overall, however, these recommendations are consistent with the Department's planned improvements, which we intend to implement with these recent Recovery Act appropriations.

4. Civil Rights and Civil Liberties: Meeting the Department's counterterrorism and law enforcement responsibilities presents a variety of substantial challenges, but the Department must protect individual civil rights and civil liberties while pursuing these responsibilities.

The need for an appropriate balance was highlighted by our reviews of the FBI's misuse of national security letters (NSL), which the OIG first reported on in March 2007. As a follow-up to our reviews of the FBI's use of NSLs and Section 215 orders for business records, the OIG is completing a review of the FBI's use of exigent letters and other improper requests to obtain telephone records. In our March 2007 NSL report, we discovered a practice by which the FBI

used over 700 exigent letters rather than NSLs to obtain telephone toll billing records. We determined that by issuing exigent letters, the FBI circumvented the NSL statutes and violated the Attorney General's Guidelines and internal FBI policy. Our ongoing review is examining in greater detail the FBI's use of exigent letters and is assessing accountability for the FBI's improper use of these letters and other informal requests for telephone records.

The Department and the FBI have taken steps to improve their use and oversight of intelligence authorities such as national security letters. In the OIG's March 2008 follow-up report on NSLs, we found that the FBI and the Department had made significant progress in implementing the recommendations contained in our first report and in adopting additional corrective measures to address the serious problems in NSL usage and oversight we had identified. We also found that the FBI had devoted substantial time and resources to ensure that its field managers and agents understood the seriousness of the FBI's shortcomings in its use of NSLs and their responsibility for correcting these deficiencies.

Yet, while we found that the FBI and the Department have taken positive steps to address the issues that contributed to the serious misuse of NSL authorities, significant additional work remains to be done. First, it remains to be seen how effectively the FBI's Office of Integrity and Compliance – established after issuance of the OIG's March 2007 NSL report – will be able to detect and correct non-compliance with the rules governing the intrusive investigative techniques available to the FBI. In the coming year, the OIG will review the work of the FBI's Office of Integrity and Compliance to determine the effectiveness of this new office.

In addition, the Department has yet to issue final minimization procedures concerning the retention of NSL-derived information. A Department Working Group has developed recommendations for NSL minimization procedures, which are still being considered within the Department and have not yet been issued. We believe that the Department should promptly issue final minimization procedures for NSLs that address the collection of information through NSLs, how the FBI can upload NSL information into FBI databases, the dissemination of NSL information, the appropriate tagging and tracking of NSL-derived information in FBI databases and files, and the time period for retention of NSL-obtained information. At this point, more than 2 years have elapsed since our first report was issued recommending such procedures, and final guidance is needed and overdue.

In addition, the *USA PATRIOT Reauthorization Act of 2005* (Reauthorization Act) required the Department to implement minimization procedures for business records obtained pursuant to Section 215 orders. The Reauthorization Act required that specific procedures be designed for Section 215 material that would minimize the retention and prohibit the dissemination of non-publicly available information concerning United States persons consistent with national security interests. The Reauthorization Act required that these procedures be adopted by September 5, 2006.

However, there was disagreement between the Department and the FBI regarding the definitions and scope of minimization procedures in general, including the time period for retention of Section 215 records, and whether to include procedures for addressing information received in response to but beyond the scope of a Section 215 order. To meet the statutory deadline, the

Department adopted sections of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection of October 31, 2003 (Guidelines) as "interim" minimization procedures for business records.

We concluded that these interim minimization procedures were deficient because the interim procedures were not specific to Section 215 records - in fact, compliance with the Guidelines was already a prerequisite to obtaining a Section 215 order. We therefore recommended again that the Department continue to work to develop appropriate standard minimization procedures for Section 215 records. According to the FBI, the Department has drafted new minimization procedures for business records. However, these procedures have not been issued.

Other OIG reports issued during the past year raise additional concerns about the need to balance aggressive law enforcement with protection of civil rights and civil liberties. As noted in the counterterrorism challenge, the OIG examined the FBI's management of the consolidated terrorist watchlist and raised a concern that while it is important to place names on the watchlist when appropriate, it is also important to remove names from the list when they no longer should be there. We found in our March 2008 audit that FBI case agents did not consistently update watchlist records when new information became known and that in many instances the FBI did not remove watchlist records when appropriate. In a follow-up audit issued in May 2009, the OIG similarly concluded that the internal controls over the processes used to nominate individuals to the terrorist watchlist are weak or nonexistent and that, similar to findings in our previous review, did not update or remove watchlist records as required.

In sum, while its 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 our nation's security.

DOJ RESPONSE*:*

The Attorney General has repeatedly observed that "there simply is no tension between an effective fight against those who have sworn to do us harm, and a respect for the most honored civil liberties that have made us who we are." Each day, this Department works to ensure vigilance in protecting our national security while doing so consistently with the rule of law, civil rights, and civil liberties. We cannot afford to relax our guard in the fight against terrorism and those who threaten our national security, but the Department of Justice is committed to doing so while upholding our fundamental individual rights and liberties. For example, as the Inspector General acknowledged, the Department has made significant progress in developing procedures for handling information derived from national security letters. The Department will finalize and announce these procedures after resolution of Patriot Act reauthorization legislation later this year, which could address this issue. In the meantime, however, the FBI has already adopted many of the new procedures.

For instance, the FBI's Office of Integrity and Compliance (OIC) has implemented (and is now overseeing) a program that facilitates the FBI's ability to comply with both the letter and the spirit of all applicable laws, regulations, rules, and policies. OIC also has

implemented a process for identifying and addressing issues which warrant attention based on the applicable compliance risk. Once the OIG initiates the above-mentioned audit, the FBI will work with the OIG to make relevant personnel available for interviews and to provide relevant documents.

The Department will continue to work with the FBI to finalize the NSL Working Group's recommendations. In addition to directly responding to the OIG's recommendations, we have implemented an automated NSL creation system which will not permit an NSL to be created if required information and approvals are not input. The use of this system should mitigate many of the common errors discussed in the OIG's previous reports on NSL usage. This system, along with changes to FBI policy and enhanced internal reviews of NSL usage, has helped to substantially address the issues raised by the OIG and will result in greater accountability in the future.

The Department also continues to work to finalize minimization procedures for business records. As that work continues apace, it is important to underscore that the FBI Domestic Investigations and Operations Guide addresses many of the issues raised by the OIG.

5. Financial Crimes: While the Department has recognized the need to aggressively investigate and prosecute financial crimes, this challenge has been exacerbated recently. With the downturn in the economy, the Department is facing a significant increase in various types of economic crimes, including mortgage fraud, white collar crimes, health care fraud, and grant and procurement fraud. The Department's challenge involves addressing these crimes with limited resources that are also focused on counterterrorism, violent crimes, and other pressing issues.

While many types of financial crimes have been increasing in recent years, mortgage fraud has seen a dramatic spike, with the FBI reporting more than double the number of criminal mortgage fraud investigations over the past 3 years. Congress recently passed the *Fraud Enforcement and Recovery Act of 2009,* which authorizes a significant increase in the FBI's mortgage and financial fraud investigative program. In addition, this Act gives the Department new authority to prosecute fraud occurring in private institutions that generated many of the subprime mortgages but were previously not covered under federal criminal bank fraud statutes.

The Department also has seen significant growth in corporate fraud and misconduct in the securities and commodities markets at the institutional, corporate, and private investor levels. The FBI reports that it is currently investigating over 189 major corporate frauds, 18 of which have losses over $1 billion. The most recent high-profile case that exemplifies this trend is the investigation in which Bernard L. Madoff pled guilty in March 2009 to 11 felony charges of securities fraud and related charges and was sentenced in June 2009 to 150 years in prison. In addition to prosecuting white collar criminals, a major challenge for the Department will be to aggressively pursue the recovery of the remaining assets through asset forfeiture laws to restore funds to the victims of financial crime.

The Department also recently announced its intention to combat health care fraud by joining with the Department of Health and Human Services (HHS) to create a taskforce called the Health

Care Fraud Prevention and Enforcement Action Team. Health care fraud has been a long-standing challenge for the federal government, with the FBI estimating that losses in the United States exceed $50 billion annually. As health care spending continues to increase, the FBI estimates that health care fraud will show a corresponding increase.

The DOJ-HHS task force is intended to increase coordination, intelligence sharing, and training among HHS, DOJ, and other law enforcement agencies to address health care fraud. During the past year, the Department had one particularly notable success when it announced a $2.3 billion settlement with American pharmaceutical company, Pfizer Inc., to resolve criminal and civil liability arising from the illegal promotion of certain pharmaceutical products.

At the same time, the Department continues to focus on procurement and grant fraud. In 2006, the Department created the National Procurement Fraud Task Force to promote the prevention, early detection, and prosecution of procurement fraud. This task force focuses on civil and criminal enforcement of defective pricing, product substitution, misuse of classified and procurement-sensitive information, false claims, grant fraud, labor mischarging, fraud involving foreign military sales, ethics and conflict of interest violations, and public corruption associated with procurement fraud. As described above, the need to prevent, detect, and deter procurement and grant fraud became even more acute during this past year with enactment of the Recovery Act.

While the Department is investing increased resources in combating financial crime, one of its major challenges will be to ensure that its various components that address financial crimes – including the Criminal Division, the Civil Division, the Antitrust Division, the U.S. Attorneys' Offices, and the FBI – effectively share information and collaborate on the investigation and prosecution of these offenses. In addition, the Department also needs to ensure effective collaboration with other federal agencies, with state and local law enforcement partners, with private industry, and with consumers.

In sum, deterring, investigating, and prosecuting financial crimes is a challenge that has grown significantly more complex. While the Department has undertaken initiatives to help address this problem, it must continue to focus its efforts on meeting this heightened challenge.

DOJ RESPONSE:

The Department is fully committed as one of its top priorities to aggressively investigate and prosecute financial crimes. To do this most effectively, the Department recognizes that it must coordinate its efforts internally and with its partner agencies across the federal, state, local, and tribal governments. As such, the Department's leadership has formed working groups and task forces to coordinate its white collar enforcement efforts among DOJ components, with federal regulatory agencies, and with our state and local partners. For example, as the OIG notes, the Department is actively engaged in a partnership at the senior leadership level with the Department of Health and Human Services to combat health care fraud through the HEAT initiative. The HEAT initiative includes leadership from all of the relevant DOJ components (United States Attorney's Offices, Criminal Division, Civil Division, and the FBI), as well as the Office of Inspector

General at HHS. This interagency effort is already paying dividends in terms of increased recoveries and indictments, information sharing, and coordinated use of resources. In particular, for the first time, the two agencies have submitted a joint budget request to the Office of Management and Budget for FY2011 that reflects the joint resource needs for the initiative.

The Department has also developed a plan for coordination across the government in the area of financial fraud enforcement, including mortgage fraud, securities and commodities fraud, and fraud relating to the use of government economic recovery funds. The Department expects this interagency effort to yield similar dividends in coordination, intelligence sharing, training and enhanced enforcement. In the meantime, the Department has been actively engaged in outreach and coordination with our State and local partners on mortgage fraud matters and emerging mortgage rescue scams. The Attorney General recently joined Treasury Secretary Geithner, Housing and Urban Development Secretary Donovan, Federal Trade Commission Chairman Leibowitz and a group of State attorneys general to announce the creation of four State/Federal mortgage fraud working groups that will be focused on information-sharing, criminal enforcement, civil enforcement and civil rights enforcement in combating mortgage fraud, including foreclosure and rescue scams and lending discrimination. These working groups are each co-chaired by a State Attorney General and an Assistant Attorney General from the Department of Justice, and include high-level participants from Treasury, HUD, the FTC, the FBI and State banking authorities. These developments will both address concerns raised by the OIG, and better protect our citizens, assets, and financial system against criminal schemes and activity.

6. Sharing of Intelligence and Law Enforcement Information: The need to effectively share law enforcement and intelligence information remains a high priority for the Department in meeting many of its critical missions.

Over the past several years, the Department has made significant improvements in its sharing of information. For example, the FBI has improved the sharing of intelligence information with other members of the intelligence community and enhancing its role in joint operations and analytic centers. In addition, the National Security Division has played an important role in improving coordination between law enforcement and intelligence personnel within the Department.

However, the Department faces continuing and substantial challenges in this area. For example, a September 2009 OIG report evaluated the United States National Central Bureau (USNCB), the U.S. representative to the International Criminal Police Organization (INTERPOL). INTERPOL assists in the exchange of information among law enforcement agencies in the United States and throughout the world to detect and deter international crime and terrorism through a network of 187 member countries. Our audit found that the USNCB has not made critical international criminal information, such as information regarding some international fugitives and habitual criminals, available to law enforcement agencies in the United States. In addition, the USNCB has not implemented processes to ensure that the INTERPOL information it makes available to U.S. law enforcement agencies is current, accurate, complete, and timely. The OIG made 27 recommendations to the Department to improve the sharing of INTERPOL

information among U.S. law enforcement agencies. The Department agreed with the recommendations and has begun taking actions to address them.

Domestically, participation by the FBI and other Department components in state "fusion centers" is a key element of the *National Strategy for Information Sharing* (Strategy), which established a framework for information sharing among federal, state, and local government agencies. In addition, the Department operates or participates in several intelligence centers designed to ensure broad dissemination of critical law enforcement and intelligence information.

In November 2009, the OIG issued a report that examined the operations of two such intelligence centers that are central to the Department's sharing of law enforcement information in support of its anti-gang effort: the National Gang Intelligence Center (NGIC) and the National Gang Targeting, Enforcement, and Coordination Center (GangTECC). In NGIC, intelligence analysts from the federal, state, and local law enforcement provide a centralized intelligence resource of information for law enforcement agencies conducting gang investigations. GangTECC is intended to serve as a central coordinating and deconfliction center for multi-jurisdictional gang investigations involving federal law enforcement agencies.

However, our review found that NGIC and GangTECC have not been effective in meeting their fundamental mission of sharing information about gangs. For example, we found that, 3 years after its creation, NGIC still has not established a gang information database as directed by law. Such a database was mandated to ensure that law enforcement agencies nationwide had access to information about gangs. In addition, while GangTECC developed a list of high priority violent gangs, it did not disseminate this information widely in the law enforcement community. The OIG concluded that GangTECC has not established an effective program for coordinating gang investigations and prosecutions.

In another ongoing review, the OIG is examining the Drug Enforcement Administration's (DEA) El Paso Intelligence Center (EPIC), including its intelligence coordination role. EPIC has evolved from a drug intelligence center to an all-threats national tactical intelligence center that manages and provides information to a wide range of federal, state, and local law enforcement agencies. While EPIC's focus is along the Southwest border, EPIC provides information and services to a growing number of users (over 19,000 as of June 2009) across the United States and abroad.

Law enforcement agencies and the intelligence community increasingly rely upon common access to information systems within and across agencies. The capabilities of these systems and the ease of access to stored information are critical to the effectiveness of the information sharing systems. During the past year, the OIG assessed the status of various projects involving enhancement of information sharing systems within the Department and found their progress to be mixed. For example, our reviews of the FBI's efforts to upgrade its information technology (IT) systems determined that the FBI is making progress in addressing deficiencies in its information sharing capabilities. However, the successful completion of the FBI's Sentinel case management system remains a continuing challenge, with the most difficult phases of the project yet to come.

In addition, as noted in the counterterrorism challenge, in November 2008 the OIG reported on its review of the FBI's terrorist threat tracking system known as Guardian. Guardian provides the FBI with the ability to share investigative data about terrorist threats within the FBI, as well as with other government agencies to enhance analysis of the information, to better identify patterns and trends, and to inform development of proactive investigative activities. The OIG found that the Guardian system represents a significant improvement in how the FBI previously tracked and handled threat information. However, the Guardian system needs improvements to address shortcomings in the accuracy, timeliness, and completeness of its information. The FBI generally requires that all threat information obtained from ongoing counterterrorism investigations be entered in Guardian. Our audit found that in almost half of the cases tested, threat information was not entered in Guardian, thereby preventing such information from being readily available to all Guardian users, including the FBI's law enforcement and intelligence partners. The OIG made seven recommendations to improve the FBI's tracking of terrorist threats and suspicious incidents.

The OIG's September 2009 audit of the FBI's and ATF's coordination of explosives investigations, also described in greater detail in the counterterrorism challenge, found that the ongoing lack of coordination between these two components has impeded information sharing on explosives investigations. In particular, the agencies have failed to develop a single-search explosive-incident database and do not participate widely in interagency task forces as required by the Implementation Plan for the *National Strategy for Combating Terrorist Use of Explosives in the United States*.

In sum, while the Department has made progress on improving its ability to share a greater range of law enforcement and intelligence information, it continues to face a variety of operational, technical, and coordination challenges to fully address this critical need.

DOJ RESPONSE:

The Department is keenly aware that it cannot meet its many law enforcement and national security responsibilities without clear and direct communication of information and intelligence across components and agencies. Mindful of this, the Department has greatly improved its information-sharing capabilities in recent years, as the IG has noted. Building on those successes, the Department intends to take additional steps to improve these functions going forward.

For example, the Department, in coordination with the USNCB, is working to improve both the management and functioning of USNCB in order to achieve improved accessibility and utility of INTERPOL's international information sharing systems. In the past, the USNCB entered foreign-issued green notices (i.e., INTERPOL bulletins alerting member countries to career criminals or habitual offenders such as child molesters and violent gang members) into TECS, a law enforcement database administered by the Department of Homeland Security. The USNCB is now exploring the possibility of entering these notices into the NCIC (National Crime Information Center) Sexual Offender and Gang Member Files, an FBI administered database with much wider accessibility within the U.S. law enforcement community, including state, local, and tribal police

authorities. Additionally, the USNCB is entering subjects of foreign countries' fugitive "diffusion" messages into the NCIC Foreign Fugitive File when entry criteria are met. Both measures will greatly expand the availability of this information to U.S. law enforcement agencies, and will correspond with the OIG recommendations.

USNCB also reintroduced greater accountability and stricter oversight of its casework, with the aim of ensuring timely review and updating of INTERPOL case data. Accordingly, the USNCB's Compliance Review Program was recently updated and re-instituted. Each USNCB Division now undergoes an annual self-inspection with compliance oversight and review. We have mandated additional supervisory review of outgoing work products and added staff to support the Compliance Program. USNCB is also implementing several data integrity and file review projects to ensure adherence to case management procedures.

Moreover, in order to ensure that the USNCB meets NCIC's deadlines for entry, applicable NCIC entries are now made by the INTERPOL Operations and Command Center (IOCC) at case opening. This practice also ensures that information is available to U.S. law enforcement as soon as it is received. USNCB now monitors this practice to ensure periodic supervisory review and approval of the entries. We are currently exploring the possibility of establishing a 24-hour Notice Section to better manage the near-constant intake of notices and diffusions from foreign countries, and to combat the recurring backlogs in this area.

USNCB also is studying the technical feasibility of providing all domestic law enforcement agencies with direct query access to INTERPOL data through a consolidated query of NCIC. Although a number of states currently have access to INTERPOL data through International Justice & Public Safety Network (Nlets) queries, a query of NCIC would exponentially expand the access to, and use of, INTERPOL data. In addition, the Department has engaged CJIS in discussions to expand INTERPOL member countries' access to U.S. stolen motor vehicle data. Further, the Department is exploring the idea of retaining outside contractors to conduct comprehensive human capital and information technology studies. These studies will guide our effective planning for future systems and automation projects and determination of appropriate staffing levels across the agency.

The OIG Report also documents USNCB's challenges in providing investigators and prosecutors with one integrated source for gang information and assistance. USNCB has started to address these challenges, which will enhance the overall effectiveness of the Department's anti-gang intelligence and coordination centers, and increase their impact on the gang problem in this country. USNCB also has discussed with OIG staff organizational changes that might modify how the recommendations are implemented, in an effort achieve maximum effectiveness.

As to the SENTINEL Program, the Department and FBI leadership are fully aware of the challenges it poses. Indeed, senior officials are diligently working to monitor SENTINEL's implementation and ensure its success by way of: bi-weekly status updates for the FBI Director; weekly updates for the FBI Finance Division Officer by the

SENTINEL Program Manger (PM); monthly briefings for a joint meeting of DOJ, OMB, and the Office of the Director of National Intelligence; and quarterly briefings for DOJ's Department Investment Review Board (DIRB), at which the DIRB certifies the activities and the progress of the SENTINEL Program. What is more, the DOJ OIG and the Government Accountability Office (GAO) have conducted nine audits (in total) of the SENTINEL Program to date. The Department continues to address the findings of the reports and has incorporated these points into program policies and processes. In fact, 30 of the 31 recommendations are now closed. The Department will, however, continue to work with the GAO and OIG to finalize implementation of the recommendations and other planned improvements.

The Department also employed an Independent Verification & Validation (IV&V) contractor to audit the SENTINEL Program. The IV&V contractor provides monthly reports to the Executive Assistant Director of the Information and Technology Branch within the office of the FBI Chief Information Officer and briefs the SENTINEL PM. Additionally, Congressional staff members of eight Congressional committees and/or subcommittees are briefed on this program, as requested.

Likewise, the SENTINEL Program Management Office (PMO) is actively managing risks through its Risk Review Board process and maintains a risk register which tracks progress of mitigation strategies. Accordingly, SENTINEL's progress and its risks are transparent and monitored—both inside the FBI and outside to many of the oversight entities who conduct audits of the SENTINEL Program.

Finally, the Department continues to work with its prime contractor to ensure that the industry's best practices are followed. We will incorporate the feedback from all of the oversight entities to ensure the program's success.

7. Grant Management: The OIG has identified grant management as a significant challenge for the Department since inception of this list, not only in terms of making timely awards of billions of dollars of grant funds but also in maintaining proper oversight over grantees to ensure the funds are used as intended. This challenge is particularly acute for the Department in 2009 because in addition to managing over $3 billion in grant funding from its regular fiscal year appropriation, the same grant administrators also must oversee disbursement and oversight of $4 billion in grants under the Recovery Act. The challenges the Department faces in ensuring the integrity of Recovery Act funds are described in a separate challenge, while this section focuses on the continuing challenge the Department faces in ensuring the overall efficiency and integrity of its grant programs.

Several OIG reviews completed during this past year demonstrate the significant difficulties the Department has faced in the past in ensuring proper management of its grant funds. For example, in September 2009 the OIG released 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 in FY 2005 through FY 2007. Our audit, which was requested by Congress had 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 with grantees receiving awards but nevertheless participated in the approval process for the grants in question. We also found that the NIJ did not adequately justify the sole-source basis for some non-competitively awarded contracts and could not demonstrate that these contract awards were properly exempt from the competitive process required by government contracting regulations. The Department agreed with the nine recommendations we made in this report and has begun taking corrective actions to address each of the audit recommendations.

In April 2009**,** the OIG released a report which also found significant deficiencies in how OJP's Office of Juvenile Justice and Delinquency Prevention (OJJDP) awarded over $113 million in discretionary grants in FY 2007. Our review found that OJJDP allocated $74 million of the $113 million it awarded that year for non-competitive grants or "invitational awards" to 17 organizations after officials from the Office of the Attorney General, the White House, and Congress contacted OJP to lobby for non-competitive awards to certain organizations. Yet, the OJP Director stated that she could not remember who specifically had contacted OJP to request funding for specific applicants, nor could OJP provide us with any documents showing that it made merit-based assessments for these invitational grants. Because OJP lacked such evidence, we could not determine if the awarding of these invitational grants without competition was appropriate and whether it was the best allocation of OJJDP funds.

With respect to the competitive awards OJJDP made in FY 2007, we also found that OJJDP skipped several steps in its peer review process that are critical to ensuring that objective criteria are applied uniformly to all the applicants during the peer review process. In addition, our audit found that the OJJDP Director recommended, and the OJP Assistant Attorney General approved, awards to several organizations whose proposals received peer review scores that were lower than applications submitted by other organizations that did not receive award recommendations. We concluded that OJP and OJJDP decision makers should have justified and documented the rationale for award recommendations that deviated significantly from peer review results.

In March 2009, the OIG examined the Department's Convicted Offender DNA Backlog Reduction Program (Backlog Reduction Program), a grant program that provides funding to help states reduce the backlog of convicted offender DNA samples. We found that the Backlog Reduction Program has contributed to the decrease in the national backlog of convicted offender DNA samples awaiting analysis, although the overall nationwide backlog may continue to grow because of recent legislation that increases the number of offenses for which DNA samples of arrestees can be collected. However, we identified deficiencies in the Department's handling of the program, such as a failure to provide adequate guidance to the state laboratories on collecting and reporting performance information. We also found significant delays in starting several Backlog Reduction Program awards, which caused over 180,000 convicted offender DNA samples to not be uploaded in a timely manner to the Combined DNA Index System (CODIS), a national DNA-profile matching service maintained by the FBI. In addition, the Department continued to award funding to several state laboratories that had not utilized previous award funding.

Recent OIG audits and investigations of grant recipients have also resulted in civil or criminal actions, reflecting the continuing need for close grant oversight by the Department. For example, the National Training and Information Center, a national organizing, policy, research and training center for grassroots community organizations, agreed in June 2009 to repay $550,000 to settle a lawsuit alleging that it improperly used Department grant money to lobby Congress regarding the award of future grants. In another OIG investigation, a tribal leader pled guilty to falsely stating that she had hired three police officers after receiving $225,000 in grant funding from the Department's Office of Community Oriented Policing Services when in fact she spent the money on personal items and did not hire any officers.

Recognizing the important management challenge it faces, the Department has taken significant steps toward improving its grant management process during the past 18 months. In May 2008, the Associate Attorney General issued a memorandum directing the OJP Assistant Attorney General to document all discretionary funding recommendations and decisions. Under this policy, future award recommendations must contain a list of all applications received that includes the lowest scoring application funded as well as every application scoring higher, regardless of whether it was selected for funding, and a brief explanation of why a listed application was not recommended for funding.

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 across OJP. OAAM also has worked more closely with the OIG during the past year to improve grant management processes, and it now meets with the OIG on a quarterly basis to discuss grant issues. OAAM also plans to strengthen its grant monitoring processes by ensuring it reviews a minimum of 10 percent of active awards, performs quality reviews of granting agencies' site visit reports, and conducts program assessments of grant programs. OAAM also implemented the OJP High Risk Grantee Designation program to identify high-risk grantees in order to impose special conditions on and increase its monitoring of those grantees.

The Department has taken other responsive measures during recent months in response to a document we issued entitled, *"Improving the Grants Management Process."* Shortly after passage of the Recovery Act, the OIG surveyed its staff and reviewed prior audit reports to identify significant grants management issues. Based on this review, we drafted a document that 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 report. For example, OJP stated that it will now apply program-specific audit recommendations by the OIG to all applicable programs, rather than to just the specific program the OIG audited. OJP is also conducting OJP-wide assessments to improve internal controls and identify opportunities for improvement. In addition, 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.

We believe that through these recent actions and other planned improvements, the Department is demonstrating a commitment to improving the grant management process, and we have seen significant signs of improvement. However, considerable work remains before grant management of the billions of dollars awarded annually in Department grants is no longer considered a top Department challenge.

DOJ RESPONSE:

The OIG is entirely correct that the Department of Justice is fully committed to ensuring that its grant programs are effectively managed and that the grants it distributes are adequately monitored and used by grantees as intended. Indeed, the values of transparency and oversight are vital to the Department's approach to grant management.

Each day, the Office of Justice Programs (OJP) works to ensure that its grant-making decisions are transparent, and that it can be held accountable for its grant management performance. To that end, in FY 2009, OJP has posted all of its award decisions on the OJP website, including the type of award, the recipient, and the award amount. Similarly, OJP is dedicated to continuously improving its oversight and monitoring of grantees and grant programs. OJP has established common procedures and guidance to improve the quality and completeness of monitoring across OJP, as well as provided effective tools to its grants managers to properly document desk reviews and on-site monitoring, formally communicate with grantees through the system, and track the resolution of open issues. As part of its oversight responsibilities, moreover, the OJP OAAM will continue to evaluate the quality and level of monitoring of OJP grants and conduct OJP-wide assessments of program initiatives and operations to measure performance, enhance internal controls, and identify opportunities for improvement.

OJP also has embraced the OIG's February 2009 report entitled "Improving the Grant Management Process" and implemented many of its recommendations. In particular, OJP has implemented those recommendations relating to grant program development, application, and award processes. At every possible opportunity, OJP is implementing corrective actions to respond to OIG grant-related and program-specific audit recommendations.

OJP and Department leadership have been working very closely with the OIG in addressing grantee issues identified by the OIG in grant audits conducted by the OIG and audits conducted in accordance with OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations. OJP has streamlined audit follow-up activities to ensure that outstanding audit recommendations are tracked and promptly addressed, which has lead to faster closure of a significant number of grant and single audit reports. OJP and Department leadership will continue to meet routinely with the OIG and will continue to work closely with grantees to ensure that issues identified by the OIG are timely resolved by either repaying unallowable grant expenditures, providing further support that substantiates the grantees' expenditures, or developing appropriate procedures to ensure future compliance.

OJP has worked quickly to implement appropriate corrective actions in response to the OIG's review of the Backlog Reduction Program. As of July 2009, based on the corrective actions implemented by NIJ, the OIG had closed 10 of the 11 report recommendations. NIJ anticipates fully implementing the remaining open recommendation by December 2009.

8. Detention and Incarceration: The Department continues to face a significant challenge in safely and economically managing the federal inmate and detainee populations, particularly in light of the rise in the number of inmates and detainees and the increasing costs needed for this purpose.

The federal inmate population has dramatically increased over the past 30 years, rising from fewer than 25,000 inmates in the Federal Bureau of Prisons' (BOP) custody in 1980 to more than 209,000 inmates in 2009. 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. The majority of growth in recent years has been in the numbers of medium and high security inmates who cannot be housed in contract facilities. They therefore must be housed either by adding beds to existing BOP institutions or by building new institutions. System-wide overcrowding continues to be a serious issue with BOP facilities at 37 percent above rated capacity as of April 2009.

In addition to safety issues presented by overcrowding, the BOP also must address other threats to inmates' safety, including sexual abuse in prisons. 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.

This year the OIG examined in-depth the Department's efforts to prevent sexual abuse of federal inmates by correctional staff. Our September 2009 report found that allegations of criminal sexual abuse and non-criminal sexual misconduct at BOP institutions more than doubled from FY 2001 through FY 2008. BOP officials told us they believe this increase is due to the BOP's efforts during this time period to educate and encourage staff and inmates to report abuse. However, our review found that while the Department's progress in implementing staff sexual abuse prevention programs has improved since 2001, the Department needs to take additional steps to effectively deter, detect, investigate, and prosecute staff sexual abuse of federal prisoners.

For example, we found that BOP officials at some prisons – in an effort to protect alleged inmate victims – automatically isolate and segregate the victims and subsequently transfer them to another federal prison without first considering less restrictive options for safeguarding them from further harm. Inmates often view such actions as punitive and may be reluctant to report their sexual abuse or cooperate with investigators if they are automatically isolated or moved to another institution. Additionally, BOP officials could not verify that alleged inmate victims had received appropriate victim services, such as psychological assessments and medical treatment. The OIG also identified improvements that should be made in staff training, inmate education, and oversight of the BOP's program to reduce staff sexual abuse of inmates.

We also analyzed the prosecution of staff sexual abuse of inmates. Since 2006 when the law changed sexual abuse of inmates from misdemeanor to felony crimes, the percentage of cases accepted for prosecution by Department prosecutors has increased from 37 percent under the old law to 49 percent under the new law. We also found that the prosecutors who accepted these cases had a very high success rate, with all but 7 of the 90 prosecutions resolved during the period of our review resulting in convictions. However, some prosecutors continued to express a general reluctance to prosecute these cases. 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 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. One OIG review 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.

With approximately one-third of BOP's 115 institutions 50 years or older, the increasing prison population also exacerbates a challenge for the BOP in repairing failing infrastructure at these institutions. While the BOP prioritizes facilities that need the most attention, significant additional money is needed to address what can become, at its most serious, a safety and health-related issue.

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 United States Marshals Service (USMS). Approximately 56,000 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) provides oversight of the USMS's detention activities and manages the budget for housing USMS detainees, a budget which in FY 2009 totaled more than $1.2 billion.

The USMS houses 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 these detainees. Over the years we have found problems with the manner in which the per diem charges the Department pays for each detainee (also known as a jail-day rate) are determined and with the Department's monitoring of the charges. We are initiating another audit of the Department's process for identifying and negotiating fair and reasonable per diem rates.

In sum, the Department's detention and incarceration responsibilities continue to pose prisoner safety and financial challenges that have intensified in recent years due to rising federal prisoner and detainee populations.

DOJ RESPONSE:

One of the Department of Justice's most important responsibilities is to house federal prisoners and detainees safely and humanely. The Department remains committed to fulfilling this responsibility, despite the increasing prison and detainee populations and mounting resource challenges noted by the Inspector General. To that end, the Department's FY 2010 and outyear budget requests are structured to address the BOP's long-term capacity needs in the most cost effective manner possible. BOP will continue to structure budget requests to address capacity needs in the most cost effective manner possible.

Sexual abuse—including staff sexual abuse—must not be tolerated in federal prisons. Any allegations of abuse are treated as serious by the Department of Justice. Indeed, the Department has established a high-level working group to address the recent recommendations of the National Prison Rape Elimination Commission. This group will examine these recommendations and prepare a regulation adopting national standards for the detection, prevention, reduction, and punishment of prison rape, as required by the Prison Rape Elimination Act. The Department expects that the working group's review will lead to further improvements in BOP's efforts to combat staff sexual abuse. Even as this work is ongoing, however, BOP continues to have a zero tolerance policy for staff sexual abuse and takes extremely seriously any allegation of sexual abuse in its facilities. The Deputy Attorney General recently convened a meeting with BOP, EOUSA, and OIG to discuss the findings of OIG's September 2009 report on the Department's efforts to prevent staff sexual abuse of inmates.

As the OIG notes, moreover, the Department has increased its prosecutions of staff sexual abuse in recent years. EOUSA's Office of Legal Education has sponsored classroom training on Prosecution of Criminal Cases in Federal Prisons, including presentations on Investigation and Prosecution of Sexual Abuse and Other Crimes Committed by BOP Employees. EOUSA is currently in the process of developing and providing additional training to AUSAs.

Furthermore, BOP agrees with the OIG that wardens should consider methods to protect victims short of isolation or segregation, although at times such steps may be necessary. In addition, the BOP is committed to ensuring that victims of sexual assault receive appropriate medical and psychological assessments and if necessary, treatment. In some cases, there may be a need for an alternative means of providing such services other than established protocol. Such alternate means are necessary to prevent wider dissemination of information to staff other than the warden and investigative staff, which might compromise the integrity of an ongoing investigation.

Finally, in November 2007, the OFDT implemented a new pricing model for the government to negotiate a fair and reasonable per diem rate and built a tool, called eIGA, to assist in collecting jail cost information and maintaining negotiation records. The eIGA model uses operating cost information gathered from detention facilities across the nation as an element in developing the core rate that officials apply as the government's estimate

of services being offered by the local jail. Based on recommendations and input by the OIG and the Department, OFDT adjusted eIGA to collect additional cost information that is calculated as a separate cost-based rate that is also available during the negotiation process.

9. Information Technology Systems Planning, Implementation, and Security: Like other government organizations and private corporations, the Department faces an ongoing challenge managing the more than $2 billion it annually spends on information technology (IT) systems – and ensuring that its decisions in IT planning, development, and security maximize the impact of these expenditures.

The Department has had mixed results in successfully meeting this challenge. Although the Department has made progress in planning for new IT systems, the Department still faces delayed implementation, deficient functionality, and cost overruns of some IT systems. In addition, while the Department has developed sound processes and procedures for identifying IT vulnerabilities, it has been slow to implement systems to address the vulnerabilities.

The OIG continues to be concerned that the Department does not exercise direct control over IT projects among Department components. 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 have identified continuing concerns about the development of critical Department IT systems. For example, a March 2009 OIG audit report examined progress toward developing a Department-wide 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. However, 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 recommended that the Department reevaluate the viability of implementing the LCMS in litigating divisions other than the Executive Office for United States Attorneys and United States Attorneys' Offices, including an assessment of whether there is a commitment and adequate funding to continue development of the system. We also urged better oversight of this project to minimize or avoid further schedule and cost overruns.

In August 2009, subsequent to the issuance of our report, we met with senior Department managers to discuss the Department's response to our recommendations. The Department expressed a strong commitment to meeting the need for the LCMS and to fully implementing our recommendations. We agree with the need for such a system, and we believe that with adequate

funding, commitment from the litigating divisions, improved planning and development, and better controls, the Department can complete the LCMS system successfully. However, the Department must be vigilant in its oversight of this project and should carefully monitor its progress.

Another example of the challenge the Department faces in this area is the FBI's ongoing effort to upgrade its case management system, known as the Sentinel project. In March 2006, the FBI awarded a contract to Lockheed Martin to develop Sentinel in four phases. At that time, the FBI estimated that Sentinel would cost a total of $425 million and be completed by December 2009.

In October 2009, the OIG completed its fifth report on the progress of Sentinel. Sentinel appears generally to be on track, but we identified several areas of concern. For example, we found that the newly delivered portions of Sentinel did not provide significant additional functionality to users as initially planned. We also determined that the FBI and Lockheed Martin agreed to delay the projected completion date until September 2010, 9 months later than originally planned. Moreover, the FBI and Lockheed Martin agreed that Lockheed Martin's costs to complete Phase 2 of the project have increased by $18 million. We also raised concerns that an increase in turnover and unfilled staff vacancies on the Sentinel project management team left it without enough staff with the appropriate skill level. We made six new recommendations to assist the FBI in addressing these and other issues.

As the Department develops new IT systems, it also must ensure the security of those systems and the information they contain. Specifically, 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.

We have found that the Department has made significant progress in the area of IT security and has developed sound processes and procedures for identifying IT vulnerabilities. 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 Department has established the Justice Security Operations Center (JSOC), which provides real-time monitoring of the Department's networks to detect vulnerabilities and threats. 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.

Portable IT media pose significant IT security risks in the Department and across government. As an initial step in assessing the Department's efforts to safeguard information stored on portable devices, the OIG reviewed the Civil Division's laptop computer encryption program and practices. In a report issued in July 2009, we found that all the Civil Division's laptops were encrypted and compliant with the Department's requirements, but we identified a serious vulnerability in that a large percentage of the laptops used by Civil Division contractors to process data on behalf of the Civil Division were not encrypted. The Civil Division relies on

contractors for assistance in various aspects of sensitive litigation involving national security, banking, and insurance. We found that this information security lapse resulted from the Civil Division's failure to provide its contractors with security instructions for protecting Department data.

The OIG is now auditing the Criminal Division's laptop computer security programs and practices. In addition, we are evaluating whether the Department has communicated to all components the national strategy to combat identity theft, and whether it has developed the infrastructure to implement its responsibilities under the strategy.

In sum, if the Department is to build on the advances it has made in IT systems planning, implementation, and security, it must closely manage its IT projects to ensure the systems are cost-effective, well-run, secure, and able to achieve their objectives.

DOJ RESPONSE:

The Department is committed managing its Information Technology (IT) systems efficiently, cost-effectively, and securely. Indeed, the Department already has made significant progress in planning and implementing new IT systems, and its future projects and efforts will continue to build on that existing success.

To that end, while the Department CIO still does not have authority over the various components' IT budgets, he does have insight into—and oversight of—their IT priorities through the annual budget process. During that process, each component's CIO presents his IT priorities to the Department CIO, who then prioritizes all submissions to ensure overall compliance with the Department's mission, the Attorney General's priorities, and the Department's strategic plan. In addition, all components must ensure that any new project—regardless of size— meets the requirements of the Department's reference architecture and that the program uses sound program management methodology. Programs that have a total development and implementation cost in excess of $100 million require regular review by the Department's Investment Review Board, which is chaired by the Deputy Attorney General. These reviews provide senior management with an in-depth view of the program, including its schedule, cost, and any potential issues. This process ensures that issues are surfaced and addressed before they can have a significant impact or become critical to the program's overall success.

Consistent with its general effort to ensure effective IT management, the Department fully supports and places a high priority on the continued development of LCMS. The IG is correct to note that the senior Department management is strongly committed to implementing LCMS. The Department believes that the information processing services that will be delivered through the LCMS Program are paramount to the efficient and effective operation of DOJ and its litigating components. The OIG report raised constructive recommendations with which to improve the Program implementation. The Department has responded to all of the recommendations both verbally and in writing, and it will continue to work toward final closure. Most important, additional internal, management, and contract controls have been added to mitigate the risk of future cost and

schedule overruns. Likewise, a detailed implementation plan for deploying LCMS to the remaining litigating components will be developed

As the Inspector General notes, the SENTINEL Project remains on track. The OIG recently issued its fifth audit report on the progress of Sentinel in early November 2009. The Department has reviewed the report. To the extent that there are any areas of concern, the Department continues to closely monitor the Project so that it will be completed in the fall of 2010.

Phase 1 was successfully deployed throughout the FBI in June 2007. It provided a user-friendly, web-based interface to access information currently in the FBI's Automated Case Support (ACS) system. Through this web-based interface users have easier access to investigative and administrative case information. Phase 1 also introduced Personal Workboxes which summarize a user's cases and leads, and Squad Workboxes that enable supervisors to better manage their resources and assign leads with the click of a mouse. These capabilities placed more investigative and administrative case information at the employees' fingertips and began moving employees away from a dependence on paper-based files.

Based on lessons learned from Phase 1, the PMO adopted an incremental development strategy to more rapidly develop and deploy capabilities to users in the remaining phases. This approach reduces the task of creating costly custom, throwaway code needed for ACS and SENTINEL to interact simultaneously while SENTINEL steadily assumes ACS services. As a result of the development of a strategic plan associated with the incremental development strategy at the beginning of Phase 2, the cap for the program was raised $26 million, increasing the budget to $451 million, and the overall program length was extended 6 months. The program had expended $282.2 million as of October 8, 2009. The total program cost of $451 million is unchanged since the start of Phase 2.

Segments 1, 2, and 3 of Phase 2 were successfully delivered. Segment 4—the final Segment of Phase 2—is currently nearing completion. Segment 4 will provide three forms and a new electronic workflow tool with digital signature. It will also migrate administrative case data from the legacy system and introduce new case management functionality for administrative cases in SENTINEL. Phase 3 began in August 2009. SENTINEL is scheduled to be completed in the fall of 2010.

Finally, ensuring information technology security is of critical importance to the Department of Justice. Consistent with the priority that the Department places on IT security, it has devoted valuable resources and attention to ensuring that its IT systems as a protected as possible. For instance, as acknowledged by the IG, the Department has made significant progress in the area of IT security and has developed sound processes and procedures for identifying IT vulnerabilities. The Department will continue to build on this success going forward. To that end, the Civil Division is implementing the necessary actions to ensure that all non-Civil Division laptop computers used to process DOJ data are encrypted or require contactors to use encrypted Civil Division provided hardware. OIG's

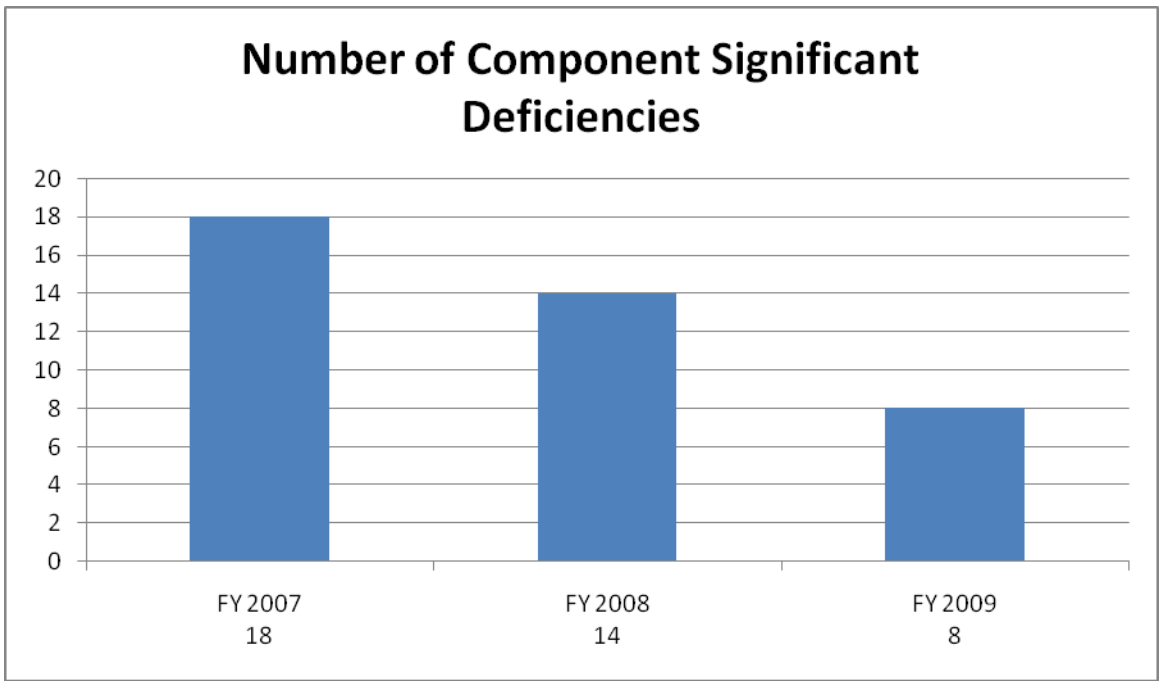
recommendation in this area has been implemented for contractors under the Mega-3 contract.

Implementing this recommendation for contractors hired under an OBD-47 will require a comprehensive set of new procedures, including changes in contract language, technical support resources, additional hardware acquisition, additional personnel, and training. It is likely that some OBD-47 contractors will have the resources to comply with this requirement. For others who may lack the technical sophistication to comply with the requirement, the Civil Division is planning to provide some limited support or encrypted hardware. To implement this change, hardware must be identified, tested, procured, and deployed. The Division has identified the requirements for hardware, software, and additional personnel, and has begun crafting procedures and planning the procurement. Following procurement of the hardware and software, it will construct a training program for attorneys and other staff members acting as points of contact on OBD-47 contacts. The Division anticipates it will take 9 to 12 months to fully implement this recommendation.

The Division also is taking steps to ensure that all contract support providers are aware of security information procedures for handling DOJ data in accordance with DOJ policy. All Mega-3 contractors have been provided this information and are required to pass it through to sub-contractors. OBD-47 contractors will be part of the comprehensive program outlined in the paragraphs above. To ensure security awareness, the Civil Division will conduct periodic spot-checks of contract support providers.

10. Financial Management and Systems: While financial management and systems has been identified as a top management challenge for the Department since 2003, the Department has made significant improvements in its financial reporting. At the same time, there has been an increasing demand for accountability and transparency throughout the federal government, and this need for accurate, near real-time financial information continues to present a significant management challenge for the Department.

For 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 at the Department consolidated level. Additionally, Department components reduced component significant deficiencies from 14 in FY 2008 to 8 in FY 2009.



Similar to past years, 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 data. The Department currently uses six 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 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 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 solve 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.

Yet, the Department's efforts over the past several years to implement the UFMS have been subject to fits and starts, primarily because of problems obtaining sufficient funding for the project, staff turnover, and other competing priorities. Despite the fact the Department selected the vendor 5 years ago for the unified system and selected an integrator to implement the unified system 3 years ago, full implementation of the UFMS has occurred at only one component, the DEA. While successfully implementing the UFMS at the DEA is a significant achievement, the DEA's legacy system was one of the most modern financial management systems within the Department. Thus, the central issue to this challenge remains largely unaddressed because the Department's other components continue to use five major, unintegrated and, in some cases, antiquated financial accounting systems.

Implementation of the UFMS is not projected to be completed in all Department components until FY 2013 at the earliest. Until that time, Department-wide accounting information will continue to be produced manually, a costly and time consuming process that undermines the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles, as well as the ability to provide detailed financial information for newly emerging requirements.

However, the Department, by achieving another year of overall positive financial statement audit results, has made progress in its overall financial management. Nevertheless, we remain concerned that the Department has not yet been able to replace its legacy financial systems with a single integrated financial management system. Implementation of the UFMS is critical for the Department to meet the need for accurate, timely financial information.

DOJ RESPONSE:

We agree with the importance of modernizing the financial management infrastructure of the Department through the implementation of the Unified Financial Management System (UFMS). We are also committed to continuing to strengthen our financial operations, our internal controls, and our review and evaluation procedures.

We are hopeful we are overcoming the concern that the UFMS project has moved only in fits and starts. In 2009, the Drug Enforcement Administration successfully migrated to UFMS, and, importantly, obtained an unqualified audit opinion on its financial statements produced from UFMS. As expected, the DEA project was a large, complex, and difficult migration, but one which helps lay the foundation for the upcoming FY 2010/2011 migration of ATF to UFMS. ATF set the stage for its full migration by implementing a Momentum upgrade during FY 2009. Additionally, other notable progress was made on UFMS during FY 2009: the BOP completely moved its procurement workforce and transactions onto the UFMS acquisitions module, a significant precursor to future use of UFMS; the FBI began headquarters use of the UFMS contract writing tool; and now USMS, with the close support and assistance of BOP, is beginning to plan a migration to the UFMS acquisition module.

UFMS is an extremely complex project which needs to be carefully implemented over several years. Lessons learned from the DEA implementation will be used in the next component projects. We are already working to strengthen the hardware and application stability of UFMS based on our experience with DEA operations. Finally, major efforts were made in FY 2009, and are continuing in FY 2010, to secure funding for the next phases of the project.

During FY 2009, the Department continued to emphasize the importance of improving component financial management operations and accountability. We successfully conducted a one day intensive fraud prevention seminar for financial managers from across the Department. The seminar put particular emphasis on preventing and detecting insider fraud threats faced by federal agencies. Two components this year, FBI and ATF, successfully completed their component-level financial audits without any material weaknesses or significant deficiencies, and a major reduction in significant deficiencies was made across the DOJ components. We were again pleased that the hard work of the DOJ financial management community achieved an unqualified opinion on the FY 2009 financial statements. We believe the emphasis placed in prior years on improving our operations can be seen from our audit results.

Despite the FY 2009 accomplishments, the Department's financial improvement work must continue. Financial management expertise and routine reliance on controls is uneven across the Department, and we agree we need to strengthen our operations in several components. To improve our reporting integrity and accountability, we plan to do management-directed testing of selected subsidiary systems in FY 2010. Finally, we will continue to push to strengthen our budget execution oversight, and better train our staff, and to improve the IT security controls over our financial systems and networks.