DOJ Management's Response to the Office of Inspector General's Top Management and Performance Challenges

1. Counterterrorism

Issue: The FBI has reallocated significant agent and analyst resources from traditional criminal investigations to counterterrorism and counterintelligence matters. These shifts of resources have presented challenges not only for the FBI, but also for other federal, State, and local law enforcement organizations affected by the FBI's reduced involvement in certain criminal investigations. The greatest reduction of FBI resources has occurred in drug-related investigations.

Action: The FBI continues to contribute to the overall counter-drug effort by participating on joint task forces designed to maximize investigative results by combining resources, expertise, and jurisdiction of federal, State, and local agencies.

Since September 11, 2001, DEA has steadily increased its agent investigative work hours to focus on the priority mission of the DEA, which is to disrupt and dismantle Priority Target Organizations (PTOs) and CPOTs – the "Most Wanted" drug trafficking and money laundering organizations believed to be primarily responsible for the Nation's illicit drug supply. Since 2001, DEA has continued to increase its PTO investigations and has repeatedly exceeded established targets for disrupting and dismantling those organizations, which includes the removal of ill-gotten revenues from trafficking drugs. In 2001, DEA disrupted or dismantled 94 PTOs; in FY 2006, DEA disrupted or dismantled 1,305 PTOs, an increase of 1,288% over 2001. Following 9/11 and the FBI's resulting reallocation of drug enforcement resources, DOJ, with Congressional support, has been restoring the drug agent level within DEA. The FY 2007 Congressional Budget provides 6,080 total DOJ Drug Agents, maintaining the pre-September 11, 2001, level.

Issue: The Department's newly created National Security Division and the FBI's National Security Branch require implementing new reporting structures and developing new relationships with other federal, State, and local agencies.

Action: In March 2006, Congress re-authorized the USA PATRIOT Act which, among other things, established an Assistant Attorney General position to head DOJ's National Security Division (NSD). Under the direction of the Assistant Attorney General for Administration (AAG/A) (with direct oversight provided by the Office of the Deputy Attorney General), working groups were formed to identify and implement immediate and long-term administrative actions that needed to be accomplished. In addition to helping prepare the organizational structure and budget reprogramming documents that were submitted for review and approval by OMB and Congress, Justice Management Division performed much of the behind-the-scenes work so that NSD's personnel would have all the necessary administrative infrastructure in place and functioning when its new AAG was confirmed by the Senate.

Action: The National Security Branch (NSB) combines the FBI's national security workforce and mission under one leadership umbrella. This structure enhances communication capability within the Intelligence Community (IC), and with federal, State, local, and tribal law enforcement partners.

The head of the NSB serves as the FBI's lead intelligence official and routinely communicates with the DOJ National Security Division (NSD). Additionally, NSB representatives have well-established relationships with personnel in the Office of Intelligence Policy Review, Counterterrorism Section, and Counterespionage Section, all of which are now located within the NSD.

Issue: The FBI needs to better support and integrate non-agent and non-lawyer staff with technical skills into its counterterrorism effort.

Action: The NSB is developing an integrated FBI intelligence workforce consisting of agents, analysts, linguists, and surveillance specialists with deep investigative and intelligence expertise in national security and criminal tools. To build this, the NSB is creating an environment that will attract and retain intelligence personnel. The FBI refined its recruitment strategy to target and provide incentives to applicants with critical skills in intelligence, foreign languages, technology, area studies, and other specialties. For example, to staff the Weapons of Mass Destruction Directorate's

(WMDD) new Intelligence Analysis Section, the WMDD worked with the Directorate of Intelligence (DI) to establish an aggressive hiring strategy to identify individuals with experience in biological, chemical, or nuclear sciences.

Career paths that reward and develop technical experts in intelligence operations are essential to the FBI's ability to retain a world-class national intelligence workforce. Recently, the FBI implemented a national security career path, allowing analysts, agents, linguists and surveillance specialists to develop specialized skills and experience in priority areas. It is developing career paths for Intelligence Analysts (IAs) that will allow them to pursue technical, as well as management, paths in their chosen jobs. The FBI has achieved a key milestone by extending the IA career path in field office from the GS-12 level to the GS-14 level in field offices.

The DI training management has been included in the New Agents and National Academy Curriculum Committees. The DI also controls the curriculum for the intelligence career services (ICS) Cohort Program. The Training and Development Division is scheduling ICS Cohort Program and New Agent classes to start on the same days in FY 2007 so that some of the in-processing and administrative matters may be covered jointly. Throughout FY 2006, NSB supported 11 joint exercises for new agents and IAs, offering analysts and agents an opportunity to work together on simulated cases while learning each other's roles in the investigative process and the intelligence cycle. This initiative is a derivative of the interaction between New Agent Training and the ICS Cohort Program.

Issue: The effectiveness of the FBI – in particular the FBI's leadership in various areas including counterterrorism – has suffered because of a lack of continuity due to frequent turnover among all levels of management at headquarters and in the field.

Action: FBI special agents join the bureau at an average age of 30, and are eligible for retirement at age 50 with 20 years of service. These agents are most valuable to the FBI at the very stage when they are eligible to retire, when many are highly marketable in the private sector as well. Even the most dedicated agents may find it difficult to remain with the FBI after they are eligible for retirement, particularly when faced with the prospect of transferring to a high-cost area to advance their FBI career. Further, family and education obligations also may be at the highest levels at this point.

To address this issue, the FBI has launched a number of initiatives. Representatives of the FBI's Executive Development and Selection Program (EDSP) are developing a database designed to assist in Senior Executive Service (SES) succession planning. The FBI's Training and Development Division is formulating an "FBI Leadership Training Framework" that will provide the basis for a comprehensive leadership development program. The Strategic Leadership Development Plan will provide techniques for identifying leadership needs and problems; articulate a program designed to enhance leadership knowledge, skills, and abilities throughout an employee's career; and relate leadership development to the FBI's strategic mission in its top priority programs. The FBI is evaluating several possible measures to lengthen tenure in SES positions, particularly at FBI Headquarters, including the increased use of retention bonuses and other incentives. The FBI will continue to explore options for retention, including the enhanced use of a variety of financial incentives and staffing flexibility in order to help the FBI cope with these factors.

Issue: Although the FBI recently has made progress in improving its management of IT upgrades, agents and analysts will not benefit from a fully functional case management system for several more years.

Action: The FBI has established a realistic timetable to incrementally design, develop, integrate, test, and implement SENTINEL in four phases. Each phase will introduce new capabilities and provide greater access to existing information, while easing user transition, training, deployment, and support. Phase 1 is scheduled for delivery in April 2007, and will provide immediate benefits to agents, analysts, and supervisors by providing a web-based interface to legacy data. It also will allow users to better manage their workload by pushing their cases, leads, and action items to their personal workboxes. Phase 2, scheduled for May 2008, will provide greater document management and will automate workflow.

Issue: The FBI does not always allocate agents responsible for maritime security according to the threat and risk of a terrorist attack on a given seaport.

Action: The FBI's Counterterrorism Division is in the process of reformulating a previously submitted answer to this issue, which will be forwarded to FBI Inspection Division and subsequently to DOJ OIG by an 11/06/2006 deadline.

2. Sharing of Intelligence and Law Enforcement Information

Challenges to sharing information are addressed under Challenge 3, "Information Technology Systems Planning, Implementation, and Security," and Challenge 9, "Civil Rights and Civil Liberties."

3. Information Technology, Planning, Implementation, and Security

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

Action: The DOJ traditionally has followed a de-centralized management approach, which is not conducive to intense control over component programs and systems. In the last four years, however, the Department has put some mechanisms in place to help the Deputy Attorney General (DAG) and the CIO provide better oversight of high risk or problem projects. One such mechanism, the Department Investment Review Board, chaired by the DAG with the CIO as Deputy Chair, meets approximately twice a month to review progress and issues related to major Department IT programs.

The CIO will put forward a recommendation to the DAG for improving the control, management, and oversight of large, expensive IT projects at both the Department and the component levels. For the Department to gain more control of high risk functions, there would need to be significant structural changes made to its budgeting, hiring, and contracting processes. Fundamental changes internally, with the components, and on the Hill are needed to help persuade the components to act more like a single organization and use "corporate assets" rather than expand their own infrastructure and support systems for their IT needs.

Issue: The FBI has not yet fully staffed the SENTINEL Program Management Office, and there is still uncertainty over risk mitigation, contingency planning, and total project costs of SENTINEL.

Action: The SENTINEL Project Management Office (PMO) has adjusted its staffing level to be funded for 73 positions. Currently, it has a staff of 65 persons, and has been actively recruiting an intelligence analyst and a training planner. Six Operations and Maintenance positions are being actively recruited. The PMO reviews staffing on a weekly basis and has successfully filled what it considers to be normal attrition since the inception of the project.

The FBI has instituted a risk management process to identify and mitigate the risks associated with the SENTINEL project. The process is managed by the SENTINEL Program Manager and a Risk Review Board that meets biweekly. The most significant risks identified are examined at monthly Program Management Review sessions and other SENTINEL oversight meetings, in accordance with the FBI's Life Cycle Management Directive. In addition, the risks, along with other significant program information, are presented to the FBI Director and his senior leadership team weekly; to a combined senior review team from DOJ, OMB, and DNI monthly; to the CIO Advisory Council on a bimonthly basis; to the FBI Director's Advisory Board when called on; and quarterly to any/all of the eight Congressional oversight committees that review the progress of SENTINEL. The PMO currently is developing contingency plans for all medium and high risks, in accordance with the FBI's risk management plan.

The FBI is committed to delivering SENTINEL on schedule and within budget. The Independent Government Cost Estimate is an estimate showing realism for proposal evaluation purposes. Market changes in labor and rapid changes in commercial off-the-shelf (COTS) technology are the prime reasons for variances. The PMO has been updating the OMB300 and the annual budget request with actual costs as they are known to ensure the most accurate reflection of total project costs. The PMO is confident that it will be able to effectively monitor and manage SENTINEL resources.

Issue: The Department's current wireless capabilities do not provide law enforcement officers and agents with the support they need because the 15- to 20-year-old communications systems infrastructure results in degraded coverage, reliability, and usability. Further, antiquated, stove-piped,

land mobile radio systems provide only limited federal-to-federal and federal-to-State and local interoperability.

Action: Through the Integrated Wireless Network (IWN), DOJ will replace the aging wireless systems of the ATF, DEA, FBI, USMS and OIG with a consolidated set of communications services that support DOJ's tactical law enforcement and counterterrorism missions. In the second quarter of FY 2007, the Department expects to procure the services of a systems integrator to develop and deploy the IWN. Meanwhile, DOJ has implemented a pilot system in the State of Washington and has taken several interim steps to consolidate and mitigate problems incumbent with the legacy systems.

Issue: The Department has some weaknesses in its management, operational, and technical controls for sensitive but unclassified and classified systems, as well as in its oversight program and related management controls. Components are not being held accountable for completing documentation and testing systems, and stronger monitoring of the Department's certification and accreditation process could identify and correct many of the reported system weaknesses.

Action: In 2005, the OCIO developed an oversight program and methodology for monitoring IT performance, including IT security. The Department's IT security methodology is closely aligned with the control requirements in the DOJ IT Standards, FISCAM, and existing automated tools used to support the FISMA requirements within the Department. In FY 2007, DOJ will continue to implement corrective actions for identified weaknesses in the areas of access controls, patch management, and baseline secure configurations, as well as improve overall testing of controls to ensure they are effectively designed and functioning properly. The DOJ IT Security Staff (ITSS) will accelerate the review of certification and accreditation documentation and control implementation for adequacy, completeness, and quality. Quality reviews will ensure that controls are adequately implemented; that implementation is adequately documented (e.g., control compliance descriptions and actual results in the system security plan); and that, where weaknesses are found in control implementation, plans of action and milestones (POA&Ms) are created, funded, and managed. Lastly, the OCIO will provide additional training to components in all areas of certification and accreditation, self assessments, control validation, and POA&M management.

The Department will continue to monitor progress through the IT Security Dashboard and the IT Management Scorecard. The ITSS and the Department's IT Security Council will continue to monitor IT security problem areas to identify systemic issues and formulate recommended solutions. For components with significant deficiencies, the CIO will continue its practice of monthly progress review meetings and, where appropriate, apply additional resources to bring about desired results.

The Department will initiate a CIO/CIO Council-sponsored assessment of the DOJ IT Security Program that will focus on priorities and program planning, implementation, and management. Furthermore, to bolster senior program official commitment to IT security implementation in the components, CIO performance work plans will include elements for IT security.

Issue: It is not clear what procedures the components follow internally when responding to data breaches or losses. A significant challenge many components face is the ability to identify the specific information contained on lost or stolen laptop computers and other IT equipment.

Action: The DOJ Computer Emergency Readiness Team (DOJCERT), the central organization within the Department to which components report data loss and computer security incidents, is in the process of establishing clearly defined guidance, comprehensive training, and regular meetings with component incident response teams (IRTs).

At the beginning of each FY, DOJCERT updates the Incident Response Plan (IRP) template that components follow in developing or updating their system IRPs. In this year's update, DOJCERT has added a new section focusing specifically on data loss reporting. It aligns with requirements set forth by OMB and US-CERT and defines specifically the information components need to gather when a data breach or loss occurs.

In addition, during FY 2007, DOJCERT will develop an Incident Response (IR) Handbook components can use when investigating incidents. It will identify the information to be gathered during and following an incident and techniques to compile all essential information, including the type of data included on lost equipment. It will also describe a method for identifying the level of residual risk associated with each incident as it is resolved. This will align with a new field in the DOJCERT Incident Reporting Database that will be used to measure the residual risk assigned to each incident.

To reinforce this written guidance, DOJCERT is incorporating it into the DOJ employees' annual training. Within the Department's annual Computer Security Awareness Training, DOJCERT has created a section addressing IR and discussing specifically the need to report lost or stolen IT equipment. Additionally, DOJCERT is working with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University to develop an IR training course within the virtual training environment. A section of the course will address data loss incidents. Component IRT members will complete the web-based course as part of their annual training requirement.

4. Violent Crime

Issue: The FBI's prioritization of counterintelligence and counterterrorism has resulted in shifting agents, analysts, and other resources from traditional criminal investigations to counterterrorism and counterintelligence activities. As a result, the Department is investigating and prosecuting significantly fewer traditional criminal matters than it did prior to September 11, 2001. State and local law enforcement officials have indicated that their investigative caseloads have increased following the FBI's post-September 11 reprioritization. Approximately 50 percent of respondents to an OIG survey of State and local law enforcement agencies indicated that the overall crime rate in their agencies' jurisdiction had increased during the 5-year period from FY 2000 - FY 2004: 41 percent of respondents said violent crime against persons had increased; 24 percent said gang-related crimes had increased; and 17 percent cited a rise in bank robberies. Many of these State and local officials have expressed concern about their agencies' ability to handle the increased workload and that the complex crimes that the FBI previously had handled often exceeded their departments' resources, expertise, and jurisdiction. In contrast, other local representatives said they did not believe the FBI's reduced involvement in these areas had negatively impacted their agencies' operations.

Action: Although the FBI has attained significant statistical accomplishments in the Violent Crimes Program, the number of agents it has dedicated to violent crimes has been significantly reduced. The FBI has offset these losses, in part, by aggressively combating violent crimes through the development of new violent crime task forces and leading nationwide initiatives such as the Innocence Lost child prostitution initiative, Project Welcome Home international fugitive return initiative, the Indian Gaming Working Group, and the creation of Child Abduction Rapid Deployment Teams. The FBI is leading the way in technological and intelligence innovations that will greatly assist all federal, State, and local law enforcement agencies in identifying crime trends, distributing law enforcement resources, and locating and apprehending perpetrators. Some of these innovations include the integration of fugitives into the Department of State passport lookout system, the Project Pinpoint intelligence mapping tool, the Choice Point Registered Sex Offender Locator Tool, and Violent Crime-Wireless Intercept Tracking Teams.

Issue: The Department has allocated less money to State and local governments for crime prevention. Several local leaders have noted that the shift of federal priorities to terrorism prevention has resulted in less federal funding to combat domestic crime, reductions in police department staffing levels, and more strain on the courts and corrections components of local criminal justice systems.

Action: OJP focuses its limited resources on those priorities and locations that can have the greatest impact. Its Strategic Plan, covering FY 2007 through FY 2012, provides a framework to focus funding to optimize the return on investment of taxpayer dollars.

The COPS Office, through its consistent interaction with law enforcement professionals, is aware of the needs of local law enforcement. As a result, COPS directs its limited funding to key areas. For example, in FY 2006, COPS funded a Tribal initiative that focused on the creation of various training and knowledge products aimed at addressing chronic public safety issues. The COPS Office will continue to focus its resources to maximize the impact of grant funding for State, local, and tribal law enforcement.

Issue: An OIG review determined that while the ATF's Violent Crime Impact Teams (VCIT) strategy may be an effective tool to reduce violent crime in targeted areas, there is inconsistent application by local VCITs of key elements of the strategy. The OIG also found that ATF's claim in January 2006 that it had met its stated goal was based on insufficient data. In light of the ATF's plans to expand the VCIT program to 15 additional cities in 2007, the Department must consistently implement and evaluate the VCIT strategy in these cities in order to improve the effectiveness of the ATF's efforts to target gun violence in specified urban areas.

Action: To address the OIG recommendation that "the Department must consistently implement and evaluate the VCIT strategy in these cities in order to improve effectiveness of the ATF's efforts to target gun violence in specified urban areas," ATF is issuing guidance to its Field Divisions directing VCITs to tailor the ten best practices – identified during ATF's evaluation of the program – to local conditions. Additionally, ATF will use a survey to assess the intensity with which each of the best practices is being used.

Issue: There is a need for BOP, as well as State and local corrections facilities, to prepare inmates for life after prison. Studies show that more than half of all offenders are re-arrested within 3 years after release. According to reports from the Bureau of Justice Statistics, "The reentry of serious high-risk offenders into communities across the country has long been the source of violent crime in the United States."

Action: The BOP has an active and evolving release preparation program to assist prisoners in reentering the community successfully. This program targets specific inmate needs and focuses on skills acquisition. Reentry skills are a point of focus from initial designation to the successful transition back to the community.

5. Financial Management and Systems

Issue: While the Department's goal is to move to more of a year-round versus a year-end financial reporting effort, most components are still hobbled in meeting that goal by the lack of automated financial accounting processes. To address this issue, the Department has placed great reliance on the planned Unified Financial Management System (UFMS) as the fix for many of these automation issues. The UFMS would standardize and integrate financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes. However, the Department's efforts over the past few years to implement the UFMS to replace the seven major accounting systems currently used throughout the Department have been subject to fits and starts.

Action: During FY 2006, the Department continued to demonstrate progress to remediate internal control weaknesses, which included corrective actions for tracking and measuring timely compliance and resolution. Departmental progress was demonstrated within the internal control framework, accrual accounting methodology, grant accounting and monitoring, and through establishment of financial management policies and procedures to enhance controls over financial reporting. A major key to the plan for improving audit performance is the development and deployment of a core financial system, the Unified Financial Management System (UFMS), throughout the Department. The UFMS will enhance financial management and program performance reporting by making financial and program information more timely, relevant, and accessible.

6. Detention and Incarceration

Issue: An OIG review found that BOP's monitoring procedures, intelligence analysis, and foreign language capabilities were deficient. It found that BOP does not adequately read the mail or listen to the telephone calls, visitor communications, or cellblock conversations of terrorists or other high risk inmates. The review also found that BOP does not have sufficient resources to translate inmate communications in foreign languages and lacks staff adequately trained in intelligence analysis techniques to properly assess terrorist communications. Also, BOP is not screening for terrorist connections in organizations that assist it with recruiting religious services providers.

Action: The BOP's response to the OIG's report issued September 27, 2006, detailed its intended corrective action. The thirteen recommendations have been resolved and BOP is in the process of implementing the actions identified.

Issue: The Department must try to keep drugs out of federal prisons and rehabilitate drug-addicted inmates. In January 2003, the OIG issued a review that found the BOP did not search visitors or monitor visiting rooms adequately, did not search staff or take sufficient measures to prevent drug and other contraband smuggling by BOP staff, and did not provide adequate non-residential drug treatment to inmates.

Action: The BOP has implemented corrective action to resolve and close seven of the thirteen recommendations identified in the OIG's report. The BOP is currently working on implementing corrective action on the six remaining resolved recommendations, all of which require changes to rules language and/or policy revisions.

Issue: The OIG believes the Department could realize significant cost savings if it addressed deficiencies in how prices are set in individual Intergovernmental Agreements (IGAs) with State and local agencies for detention bed space. It appears that the OFDT's revamping of the IGA pricing process through a statistical pricing model known as eIGA may result in the Department paying higher jail-day rates than necessary. Also, the OIG believes that the USMS needs to improve its procedures for establishing and monitoring IGAs. The OIG has encouraged the Department to attempt to recover overpayments made to State and local jails.

Action: OFDT does not agree that the electronic Intergovernmental Agreements (eIGA) process will lead to an unwarranted increase in rates. Under the current system, only the actual or allowable costs of individual jails are examined, so the reasonableness of costs is never challenged. However, under the eIGA approach, a price analysis is conducted using comparisons to similar jails with similar operations to determine a fair and reasonable jail rate without requiring an evaluation of individual cost elements. A price analysis supports a negotiation position that permits the Government and the jailer an opportunity to reach agreement on a fair and reasonable price that provides the greatest incentive for efficient and economical performance. (A fair and reasonable price does not require that agreement be reached on every element of cost.) In the eIGA process, federal government negotiators establish a fair and reasonable price by evaluating the offered rate through comparison to the eIGA Core Rate (government estimate); rates at other federal, State and/or local facilities; previously proposed rates; and previous Government private jail contract prices.

The current method of determining the rate – and rate increases – on the basis of cost provides an incentive to jailers to increase cost elements that are allowable federal prisoner housing costs in order to receive higher jail rates. The eIGA method provides maximum incentive for the jailer to control costs and perform effectively and imposes a minimum administrative burden upon each party.

With regard to "overpayments made to State and local jails," the OFDT maintains that the agreements incorporated a "fixed rate" and, accordingly, the agreements with the State and local governments were negotiated, fixed-price agreements for the period in question, and the parties were bound. OFDT believes that, in the absence of fraud, the agreements are not subject to retroactive adjustment.

To enforce the need for districts to comply with established IGA management policy, USMS has initiated regular communication to the districts via telephonic and written methods. It has developed a much enhanced Justice Detainee Information System upgrade, which will provide reports designed to better track IGA information. In turn, using these reports, USMS can evaluate the effectiveness and efficiency of the program and make adjustments and corrections to problem areas. The IGA Branch is increasing its staffing to meet the substantial workload of the IGA program, and, in FY 2007, it expects funding for training, allowing IGA Branch staff to gain additional knowledge in areas such as price/cost analysis and negotiation techniques.

7. Supply and Demand for Drugs

Issue: For the second consecutive year, more State and local law enforcement agencies nationwide identified methamphetamine as the drug that poses the greatest threat in their area.

Action: DEA is very aggressive in training drug law enforcement counterparts with respect to methamphetamine investigations. Since FY 1999, DEA has trained a total of 9,704 State and local law enforcement officers in identifying and cleaning up clandestine laboratories. To expand and improve its efforts, DEA is beginning the construction of a new state-of-the-art clandestine lab training facility at the DEA Academy in Quantico, Virginia in the fall of 2006.

The DEA has redirected the focus of its Mobile Enforcement Teams to prioritize deployments to assist with methamphetamine investigations. Currently, the teams are focusing on targeting methamphetamine PTOs and clandestine laboratory operators in areas of the United States that have a limited DEA presence.

With the significant reduction in the number of domestic small toxic labs, DEA's Clandestine Laboratory Enforcement Teams will expand their efforts beyond dismantling methamphetamine labs to include the targeting of Mexican methamphetamine trafficking organizations. Current drug and lab seizure data suggests that roughly 80 percent of the methamphetamine used in the United States comes from larger labs, increasingly in Mexico, and that approximately 20 percent comes from small toxic laboratories. Since 2001, DEA has disrupted or dismantled in excess of 500 Priority Targets where methamphetamine was the primary drug involved.

The DEA, with the support of the Department of State and other U.S. law enforcement agencies, has provided or sponsored training to over 450 Mexican students since 2001 in the areas of clandestine laboratories, chemical training, and related prosecutions. Training has been provided both to officials who regulate precursor chemicals and pharmaceuticals at the State and Federal level within Mexico, as well as agents from the Agencia Federal de Investigaciones and a number of prosecutors within the Mexican Organized Crime Unit.

In response to the FY 2006 Department of Justice Appropriations Act, DEA established a Methamphetamine Task Force (MTF). The MTF is comprised of three DEA special agents, two diversion investigators, three attorneys, and one program analyst. The purpose of the Task Force is to improve and target the federal government's policies with respect to the production and trafficking of methamphetamine.

Issue: In recent years, there has been a dramatic increase in the diversion of controlled pharmaceuticals. Although the need for special agent assistance in diversion investigations has increased significantly since a previous review, the OIG found that the time spent by special agents assisting diversion investigations still constitutes a small share of their total investigative effort. Also, the Department has not provided law enforcement authority for its diversion investigators. Further, the support that intelligence analysts provide to diversion groups in the field has continued to be limited, and intelligence analysts and special agents still receive minimal diversion control training.

Action: The Department's Office of Personnel approved law enforcement authority for DEA diversion investigators on 8/30/06, and the Office of Personnel Management is reviewing the matter.

DEA has taken action to update its diversion control training for special agents and intelligence analysts to improve the support of diversion investigations. In addition, DEA is implementing an Action Plan that includes:

1. providing diversion investigators with adequate special agent support until the DEA diversion investigator position is converted to a position with law enforcement authority;
2. ensuring that DEA special agents who frequently assist with diversion investigations attend the week-long diversion training school;
3. providing training to intelligence analysts on topics that would effectively support diversion investigations;
4. updating the diversion control training video used in the special agent and intelligence analyst training academies to include current issues such as diversion using the Internet;
5. ensuring that diversion investigators receive training in skills necessary for conducting Internet investigations, such as financial investigations; and
6. fully implementing the program to provide undercover credit cards to diversion investigators.

8. Grant Management

Issue: The Department needs to improve its overall oversight of the grant process, including closeout. The creation of the Office of Audit, Assessment, and Management within OJP got off to a slow start during the past year.

Action: During FY 2006, OJP implemented significant changes to improve oversight of the grant process, including updating its grant monitoring requirements in the Grant Managers' Manual, automating the Grant Adjustment Notice (GAN) process, modifying its business policy for when grants are considered overdue for closure, and addressing the backlog of grants overdue for closure. During FY 2006, OJP modified its business policy to count grants as overdue for closure 120 days after the end of the project period, rather than 180 days after. By automating the GAN process, OJP reduced the time to respond to grant adjustment requests by 10 days and was able to notify grantees of decisions regarding grant adjustment requests via the Grants Management System (GMS). During FY 2007, OJP will automate the grant closeout process and implement a requirement that all programmatic monitoring efforts be conducted and documented in GMS.

The statutory provision that created the new Office of Audit, Assessment, and Management (OAAM) was signed into law on January 5, 2006, and generally was not effective until 90 days later, with certain portions not effective until October 1, 2006. The proposed new organization chart for OJP is being reviewed by the Department.

In FY 2006, the COPS Office began conducting a comprehensive grant-related business process review. It developed business process maps depicting the "as-is" processes for the entire grant management lifecycle, including application

review, grant maintenance, grant monitoring, and grant closeout. After capturing "as-is" business processes, staff members identified potential gaps in the processes as well as candidate ideas for improvement. A comprehensive set of improvement recommendations was made, and, as a result, the COPS Office Executive Management prioritized five improvement projects for FY 2007.

A number of institutional structures ensure that OVW funds are spent for their intended purposes. First, internal and external peer reviews ensure that all grant applications meet solicitation requirements. Second, OVW, in conjunction with OJP's Office of the Comptroller, monitors "draw down" and expenditure of awarded funds. Financial status reports from recipients are closely examined to ensure that funds are being spent as scheduled; are dedicated to costs allowable by program objectives, the terms of the agreement, and DOJ fiscal requirements; and are in compliance with Federal cash management regulations and OMB A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, as appropriate. Third, the OIG and OJP's Office of the Comptroller conduct on-site reviews to determine whether: (1) grantees are properly accounting for the receipt and expenditure of federal funds, and (2) expenditures are in compliance with federal requirements and award special conditions. Fourth, OVW program specialists closely review financial reports and progress reports to ensure that funds are being spent for program purposes. Finally, OVW management rigorously assesses requests for no-cost extensions and changes to grant budgets. OVW will be implementing changes and additional policies and practices to improve their handling of closeouts.

Issue: The Department lacks performance standards, measures, and data to determine what its grants accomplish.

Action: The OJP Strategic Plan for FY 2007-FY 2012 includes performance measures that represent a cross section of OJP's key programs. The measures will be used to gauge the progress in achieving OJP's four strategic goals. In its annual budget submission, OJP will report specific baseline and target values to OMB for programs that are subject to Program Assessment Rating Tool (PART) assessments. To strengthen performance standards, measures, and data that support grant accomplishments, OJP will conduct "mini-PART" assessments of its programs during FY 2007.

In FY 2006, the COPS Office received approval from OMB on a new set of annual and long term performance measures focusing on the Office's performance in meeting its mission to advance community policing. The performance measures will assess the impact of COPS grant resources and knowledge products (training/technical assistance and publications) on increasing the capacity of grantees and knowledge resource recipients to implement community policing strategies.

The OVW collects data from multiple measures for each of its 12 grant programs. A key outcome-focused performance measure is the percent of victims requesting services who received them. Other performance data collected by OVW focuses on apparent outputs rather than long-term outcomes. However, such measures reflect whether grantees are implementing promising approaches that have a demonstrated impact on victim safety and offender accountability. The OVW has baseline data for all of its annual performance measures.

In 2001, OVW, with the help of the Muskie School of Public Service, University of Southern Maine, established the VAWA Measuring Effectiveness Initiative and has developed semi-annual progress report forms for each of its discretionary grant programs. (The STOP formula program requires State administrators to report annually on their awards and provide detailed annual sub-grantee data.) These reports request specific data on grantee activities, from victim services to training to criminal justice functions. They are designed to require input from all project partners who receive funding. Each grantee must complete these progress reports and include performance data that relate to the annual performance measures.

Issue: The Department does not exercise its full authority to monitor grants, and it has failed to implement simple requirements that could provide greater assurances that the grantees are compliant with grant requirements.

Action: With respect to OJP, the OIG provides as an example only NIJ's Coverdell program, suggesting that "NIJ did not effectively implement a statutory [certification] requirement" in that it did not give applicants certain "necessary guidance" and also "did not require grant recipients to name the entity" described in the statutory requirement to which the OIG refers. The OJP notes that, although nothing in the Coverdell statute requires guidance along the lines the OIG suggests , NIJ actually did provide such guidance to applicants (and required new certifications) before making awards for FY 2005. Also, NIJ included such guidance in its program announcement for FY 2006. (The OIG recently has indicated, in fact, that it intends to "close" its recommendation to OJP with respect to the provision of guidance.)

Regarding the OIG's criticism that, in FY 2005, NIJ "did not require grant recipients to name the entity" referred to in the certification requirement, OJP notes that, while the OIG for some time disputed OJP's position on the requirements imposed on it, the OIG's General Counsel, in August 2006, agreed with OJP that the law does not obligate OJP or NIJ to require grant recipients to name the entity. As documented in a letter from the Department's Office of Legal Counsel (OLC) to OJP's General Counsel, dated August 3, 2006, "the General Counsel for OIG has informed [OLC] that the OIG, like OJP, believes that the [statutory certification requirement to which OIG refers] is satisfied as a legal matter when OJP receives a basic certification from an applicant that replicates the language of [the certification requirement]." Moreover, OLC has taken the position (consistent with OJP's in connection with the OIG review), that "there is a significant legal question whether in FY 2005 OJP had authority under the Coverdell program to impose additional requirements" such as a requirement to "name the entity" with a process in place to conduct independent, external investigations. We also note that a recent change in the law gives OJP express legal authority to require that Coverdell applicants "name the entity." The OJP has agreed to do so beginning with the FY 2007 Coverdell program announcement.

In FY 2006, the COPS Office developed a risk-based approach to monitoring that will allow it to increase its oversight of grantees by better targeting site visits and office-based grant reviews (OBGRs) to those grantees at highest risk of performance problems and non-compliance with grant requirements. In FY 2007, COPS will focus resources toward targeting 100% of those grantees classified at the highest risk. The COPS Office will continue its financial monitoring activities by focusing on data discrepancies, delinquent reporting, excess cash reconciliation, review of grantees' 269A submissions, matching drawdowns to expenditures, and reviewing grantee final reports. Finally, COPS plans to increase efforts and resources toward resolving existing non-compliance issues generated from past on-site visits and OBGRs.

All OVW program specialists, who are responsible for managing 99% of its grants and cooperative agreements, are subject to performance work plans that hold them accountable and require them to monitor grantee "progress and compliance with applicable guidelines and regulations."

All OVW grant program specialists are required to conduct a number of grant monitoring activities, including: reviewing grantee progress reports, conducting on-site monitoring visits for a minimum of 10% of their grantees each fiscal year, conducting at least one desk audit for each grant during a 24 month cycle, and reviewing all grantee semi-annual progress reports. The latter are submitted through an on-line system which OVW implemented as part of its Measuring Effectiveness Initiative. The on-line system has greatly enhanced OVW tracking of both the timely submission of progress reports by grantees and the review of the progress reports by program staff. This improved review process has afforded OVW a greater opportunity to identify grantees who may be performing outside the scope of their grant award.

For grantees, program partners, and sub-grantees, OVW enforces the guidelines in OJP's Office of the Comptroller's Financial Guide. Further, OVW holds grantees and program partners accountable for costs through an internal and external peer review process, conducted on a pre-award basis. As part of this process, reviewers assess the cost effectiveness of proposed projects and evaluate whether the individuals and organizations involved are qualified to implement each project. OVW may request that successful applicants revise their grant budgets based on this review process.

Finally, each year, OVW reviews and revises its solicitations to reflect the current statutory purpose areas and eligibility requirements and to ensure that OVW funds will reach the intended beneficiaries. In a clear, specific, and uniform manner, solicitations for all OVW grant programs outline eligible applicants, certification requirements, activities within the scope of the program, program priority areas and, if relevant, special conditions for funding, as well as activities that may compromise victim safety.

Issue: In its review of the COPS Office's administration of the methamphetamine grant program, the OIG found a lack of coordination among COPS officials, weaknesses in the database used to manage and track grants, and insufficient and inconsistent monitoring of grantees.

Action: The COPS Office has formalized and re-structured its Meth Team to include key staff from all grant-making divisions. The new interdivisional structure of the Team includes regular participation and meetings on a weekly basis to discuss the latest actions and share upcoming activities. This restructuring has promoted communication and more consistent oversight among divisions responsible for methamphetamine projects. The Office is ensuring that staff involved with data entry of methamphetamine grants are fully trained and is conducting quality control checks of the COPS Management System (CMS) on a regular basis. The COPS has updated the CMS user manual to specifically include the Methamphetamine Training Module and has notified staff members of its posting on the COPS Intranet.

9. Civil Rights and Civil Liberties

Issue: The Department must integrate its new Office of Privacy and Civil Liberties (OPCL) in the work of the Department so that office can play a meaningful role in the development and implementation of Department policy that may affect civil rights and civil liberties issues.

Action: In addition to creating the Privacy and Civil Liberties Board, the Chief Privacy and Civil Liberties Officer (CPCLO) meets on a weekly basis with the FBI's Chief Privacy Officer, and on a monthly basis with privacy officers for ATF, DEA, and USMS, to address privacy and civil liberties issues. The CPCLO has appointed the Deputy Chief Privacy and Civil Liberties Officer (DCPCLO) to be OPCL's main interface with the new National Security Division.

Issue: The OIG has recommended that the Department and DHS enter into a memorandum of understanding (MOU) to formalize policies, responsibilities, and procedures for managing a national emergency that involves alien detainees. Both the Department and DHS agreed with the recommendation and began negotiating language for the MOU, but it still has not been finalized.

Action: The OPCL will work with the component responsible for coordinating with DHS to complete the MOU.

Issue: The Department's efforts to collect and share information with its law enforcement and intelligence partners present a significant challenge to its efforts to protect civil rights and civil liberties. The Department has a need for effective intelligence tools and, at the same time, must observe existing legal, operational, and administrative constraints on these potentially intrusive authorities.

Action: The CPCLO co-chairs the President's Information Sharing Environment Guideline 5 Working Group, along with the Civil Liberties Protection Officer for the Office of the Director of National Intelligence. The Guideline 5 Working Group has drafted Guidelines for Protecting the Privacy and Other Legal Rights in the Information Sharing Environment. In addition, the OPCL has been engaged in launching the "One-DOJ" environment, which facilitates the sharing of departmental information with regional partners through the Department's Regional Data Exchange System. The OPCL will continue to advise the Department on all of its information sharing initiatives.

Issue: Investigative and intelligence authorities enacted or expanded in the Patriot Act and the Patriot Improvement and Reauthorization Act invest broad new information-gathering powers in FBI agents and their supervisors, often permitting these tools to be approved at the field office level on a minimal evidentiary predicate. This means that the FBI – and other law enforcement or intelligence community agencies with access to FBI databases – is able to review and store information about American citizens and others in the United States who are not subjects of FBI foreign counterintelligence investigations and about whom the FBI has no individualized suspicion of illegal activity. Consequently, the Department – and the FBI, in particular – need to be mindful of the potential for any abuse of these authorities and the need for aggressive oversight by first-line supervisors, field office and headquarters managers, legal counsel, and established internal and external oversight mechanisms.

Action: The Congress, the President, the Attorney General, and the Director of National Intelligence have mandated that the FBI give the highest priority to countering terrorist activities against the territory, people, and interests of the United States. At the same time, the FBI fully appreciates its obligation to protect the legal rights of all Americans, including freedoms, civil liberties, information privacy, and others guaranteed by Federal law. Even for the areas of its highest priorities, the FBI must operate only in a manner consistent with the Constitution, applicable laws, Executive Orders, regulations, and other authorities to which it is subject. The FBI completely concurs that this is an important issue requiring that it be ever mindful of the potential for abuse and aggressively vigilant in guarding against any abuse. A 2004 internal communication from the Director to all FBI personnel emphasized this balance.

In 2005 the FBI again emphasized to all FBI personnel that, while information that has insufficient value to justify further investigative activity (at least at the time it is obtained) might legitimately be acquired during threat assessments, such information is often sensitive personal information, and measures should be taken to properly characterize its nature, protect it from inadvertent disclosure, and only use it as may be authorized by applicable policies and regulations.

FBI special agents and intelligence analysts receive job-specific privacy and civil liberties training, including an overview of the Attorney General's Guidelines, first amendment issues, the Privacy Act, and the protection of civil liberties. In 2006, all FBI employees received training on the U.S. Constitution and the protections in the Bill of Rights.

Further, in 2006 the FBI restructured the previously established position of FBI Senior Privacy Official to that of FBI Privacy and Civil Liberties Officer (PCLO) and created a new Privacy and Civil Liberties Unit (PCLU). Among its responsibilities, the PCLO/PCLU reviews FBI Privacy Impact Assessments (PIAs) for identification and appropriate resolution of privacy/civil liberties issues.

The PIA is an excellent tool to determine whether collections of data adequately protect privacy and civil liberties. While the e-Government Act of 2002 excludes national security systems from the PIA requirement, the Department requires that PIAs be prepared for such systems. The OPCL works with all Department components to ensure that their systems protect the privacy and civil liberties of the American people, and the CPCLO is responsible for approving all Department PIAs. Sign-off follows an iterative approval process and occurs only when the OPCL is satisfied that a system maximizes the protection of privacy.

This spring, the OPCL issued official PIA guidance, a Privacy Threshold Analysis to determine whether a PIA is required, and a new PIA Template. Recently, the OPCL completed a half-day training session on drafting a PIA and complying with the Privacy Act. The OPCL is considering developing a "CLIA," a Civil Liberties Impact Assessment.

10. Cybercrime

Issue: The Department has created or expanded several organizations to focus on cybercrime, including the Internet Crime Complaint Center [FBI], the FBI's Cyber Division and its National Strategy, and the Criminal Division's Child Exploitation and Obscenity Section and the Computer Crime and Intellectual Property Section. Department initiatives to combat aspects of cybercrime include the Task Force on Intellectual Property, expansion of the Computer Hacking and Intellectual Property Program, and Project Safe Childhood. Although the Department has established a good foundation for fighting cybercrime, it must continue to build upon these initiatives to respond to the growing challenge.

Action: With the ever-increasing growth of the Internet, along with its chat rooms, file sharing, and illicit websites, it is important to fully protect against the online sexual exploitation of children. A prime example of FBI success in this area is the Innocent Images National Initiative. This program has expanded from 113 cases opened in 1996 to 2,135 cases opened in 2006. The FBI will continue to share its success with the media, with the hope of using the publicity as a deterrent to online predators. New technology and tools have improved the FBI's ability to track down these criminals and bring them to prosecution. The FBI will continue to work with the National Center for Missing and Exploited Children, the Office of Juvenile Justice and Delinquency Prevention's Internet Crimes Against Children task forces, and other public interest groups to improve outreach and education to parents and children through their local schools. The FBI also will continue to produce materials and web content to help educate teachers, parents, and children.

Theft of Intellectual Property Rights (IPR) is a rapidly growing occurrence, perpetrated by groups and individuals located in the United States and abroad. Intellectual property represents not only a serious economic asset, but many times is tied directly to national security. The FBI recognizes the importance of identifying and neutralizing operations targeting U.S. intellectual property in order to reduce the impact on the nation's security and economy. In 2006, the FBI opened 316 cases involving intellectual property violations, convicted 179 individuals, and collected over $111 million dollars in restitutions, recoveries, fines, seizures, and forfeitures. The FBI plans to expand its capabilities to address the needs of the future. Through its liaison with various associations, including the Motion Picture Association of America, the Recording Industry Association of America, the Business Software Alliance, and the Electronic Software Association, the FBI has obtained information that has populated a database of Warez sites, which is used to target egregious theft of intellectual property over the Internet. Information obtained from IPR liaison contacts continues to track Warez sites and other IPR targets that have direct impacts against the U.S. economy.

The Internet has become increasingly attractive to all segments of the population as a medium for everyday information-gathering, communication, and commercial activity. In recent years, law enforcement has witnessed a substantial growth in online criminal fraud. Valuable intelligence collected from private industry leads to the development of numerous productive FBI initiatives targeting escalating cybercrime trends, including Criminal Spam, International Re-shipping and Phishing/Identity theft. In Operation Web-Snare, a joint law enforcement and industry-driven initiative, more than 155 investigations were advanced, resulting in 115 arrests and millions of dollars in seizures and recoveries. Through this

initiative, more than 870,000 victims were identified with losses exceeding $180 million dollars. Subsequent initiatives where substantial industry-based intelligence was crucial include the SLAM-Spam and Digital Phishnet initiatives. These law enforcement and industry collaborations have led to the initiation of more than 100 additional investigations, while continuing to leverage exponential intelligence and analytical resources from a growing list of key industry partners. These partnerships were quickly re-directed to focus on opportunistic cybercrime scams exploiting publicity and broad public support for victims of last years tsunami, as well as the recent hurricanes impacting the Gulf coast region of the United States. As a result, more than 150 investigations were rapidly developed and referred to law enforcement, domestically and abroad, and more than 2,000 websites have been disabled because of these projects.

The Criminal Division is working with the Department's Identity Theft Task Force to finalize a comprehensive governmentwide strategy to increase safeguards of personal information held by public and private entities, improve public outreach so that individuals can better protect themselves, and investigate and prosecute identity theft crimes when they occur. Also, in September 2006, the Criminal Division participated with the Identity Theft Task Force in developing federal guidance for agencies pertaining to responding to data breaches, developing standard police reports for identity theft, and improving government data security.

In September 2006, the Criminal Division contributed to the ratification of the Convention on Cybercrime, completing a nearly 10-year negotiation and ratification process. This Convention will strengthen the nation's ongoing international leadership role in cybercrime issues and facilitate rapid international cooperation in cybercrime cases.

Lastly, the Criminal Division participated in developing the Progress Report of the DOJ Task Force on Intellectual Property. In June 2006, the Attorney General issued the Report detailing the successful implementation of all 31 recommendations from the Task Force's 2004 report. The implementation of these recommendations represents achievements by the Department in combating intellectual property theft committed over the Internet.

This page intentionally left blank.