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

1. Counterterrorism

1. Counterterrorism: The Department's top priority remains its ongoing effort to detect and deter terrorism.

Issue 1.1: The Federal Bureau of Investigation's (FBI) Foreign Language Services Program has significant deficiencies in its translations of materials it collects in foreign languages. Deficiencies include a continuing backlog of unreviewed foreign language material (in some instances high-priority material is not reviewed within 24 hours in accord with FBI policy), and a lack of full implementation of the quality control program for linguists. The FBI also faces challenges in meeting linguist hiring goals.

Action: In response to the Office of the Inspector General (OIG) audits of 2004 and 2005, the FBI's Language Services Section (LSS) took decisive action and completed each and every one of the 18 OIG recommendations, pertaining to such matters as translation backlog, linguist hiring, linguist training, statistical reporting systems, quality control, and other technical issues that have a bearing on the Foreign Language Program's (FLP) ability to address FBI investigative and intelligence requirements. It has also been demonstrated to OIG that the "requirement" to review high priority material within 24 hours is not and was never intended to be formal FBI policy, but rather a temporary directive issued by the then Deputy Director in the wake of September 11, 2001. Prioritization of foreign language translation support is governed by a five tier Foreign Intelligence Surveillance Act (FISA) prioritization system, and further guidance on the timeliness of translation support has since been promulgated by the LSS. LSS continues an aggressive hiring program, hiring to the extent allowed by congressionally authorized funded staffing levels and non-personnel funding for contract support. Furthermore, LSS's Quality Control Program has trained and certified 328 quality control reviewers who, in FY 2008, reviewed close to 4000 work products as mandated by policy or as selected at random.

LSS actions following the 2004 and 2005 audits brought closure to all 18 OIG recommendations in the original audit. On February 26, 2008, the OIG initiated another follow-up audit to examine LSS's continued progress on these issues, as well as new LSS initiatives that have further enhanced the FLP's effectiveness and efficiency. OIG's final report is expected by the end of calendar year 2008.

Issue 1.2: The Department's counterterrorism responsibilities require close coordination with other Intelligence Community and military organizations. The OIG found that the FBI did not respond fully or in a timely manner to repeated requests from its agents in the military zones for guidance regarding several issues (e.g., circumstances under which FBI agents may participate in interviews of detainees who have previously been subjected to non-FBI interrogation techniques, circumstances under which the FBI may use information obtained from detainees by other agencies through the use of non-FBI techniques, and circumstances under which FBI agents should report the conduct of other agencies' interrogators).

Action: The FBI is in the process of formulating an official response to the OIG's May 2008 report on this issue. The FBI will provide its response to the OIG by November 15, 2008.

Issue 1.3: The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the FBI both have the authority to investigate explosive-related cases, but historically, they have had significant disputes over their respective jurisdictions. Even after ATF's entry into the Department and an Attorney General memorandum addressing several explosive-related jurisdictional issues, disputes between the two agencies have continued.

Action: The FBI and the ATF are working together to address the issues identified in the OIG's ongoing audit regarding coordination of explosive-related activities. The FBI will provide a formal response to the OIG at the conclusion of the audit.

Meanwhile, in July 2008, the Directors of the ATF and the FBI entered into a formal agreement regarding the protocols to be followed in explosives related incidents/investigations. This document is the official position of DOJ, and it recognizes that ATF will be the lead investigatory agency on explosives related incidences which are not acts of terrorism. Similarly, the FBI agrees that ATF is the federal agency charged with investigating acts of explosives related violent crime. Not only are issues relating to incident management covered in the 2008 protocols (e.g., jurisdiction, investigation/leads, resources) but also issues related to initial response (e.g., first responders, joint notification, crime scene processing and laboratory/forensic capabilities) and prosecution. The 2008 protocols are a framework from which the ATF and the FBI will build more specific standards and procedures surrounding all of the issues addressed in the Memorandum of Understanding (MOU). A committee of ATF and FBI Special Agents in Charge (SACs), operating under the joint direction of ATF and FBI leadership, currently is working these issues.

2. Sharing of Intelligence and Law Enforcement Information

2. Sharing of Intelligence and Law Enforcement Information: An essential element in successfully detecting and deterring terrorism and enforcing the law is sharing information with federal, state, and local officials. The implementation of new or upgraded information technology (IT) systems to facilitate information sharing remains a key factor in the Department's ability to meet this challenge.

Issue 2.1: The successful completion of the FBI's SENTINEL system remains a continuing challenge, with the most difficult phases of the project yet to come.

Action: The FBI is fully aware of the challenges that lie ahead and is working hard to ensure that SENTINEL is successful. 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. PMO progress and risks are transparent both inside the FBI and outside to our many oversight entities. The Director and/or his executive staff are briefed weekly on the status of the project. The FBI's Finance Division is also briefed weekly by the PMO. The Department of Justice (DOJ), Office of Management and Budget (OMB), and the Office of the Director of National Intelligence (ODNI) are briefed at a joint monthly meeting. The DOJ's Department Investment Review Board (DIRB) is briefed quarterly by the PMO and the DIRB certifies the activities and progress of the program. The PMO provides monthly Earned Value Management (EVM) data to the DOJ and briefs the DOJ quarterly on its EVM reporting.

The Government Accountability Office (GAO) and the DOJ OIG have performed eight audits of the SENTINEL Program to date. The FBI continues to address the findings of the reports and has incorporated all of the findings into program policies and processes. The FBI will continue to work with the GAO and OIG who will shortly be starting their ninth and tenth audits of the program. The FBI has also hired an Independent Verification & Validation (IV&V) contractor to audit the SENTINEL Program. Monthly IV&V reports are provided to the FBI Chief Information Officer (CIO) and are briefed to the SENTINEL Program Manager. The SENTINEL Program has been asked to resume quarterly staff briefings of eight Congressional committees and/or subcommittees.

The FBI will continue to work with its prime contractor to ensure that the industry's best practices are followed. It also will continue to incorporate feedback from all of the oversight entities in order to ensure the success of the program.

Issue 2.2: In its audit of the FBI's National Name Check Program (NNCP), the OIG found that the name check process used by the FBI has serious deficiencies, including relying on outdated and inefficient technology, personnel with limited training, overburdened supervisors, and inadequate quality assurance measures. Those deficiencies have resulted in large backlogs, with over 327,000 name check requests pending as of March 2008, a backlog that can hamper timely adjudication of immigration applications. Also, security check delays can slow the adjudication and deportation of applicants who may pose a national security threat to the United States.

Action: Since March 2008, the FBI's NNCP has implemented a number of strategies to expedite the elimination of the name check request backlog and maintain a steady state operation. These strategies include:

- Stabilizing the current information technology systems,
- Deploying a metrics based name check management process,
- Implementing formal quality assurance procedures,
- Updating all NNCP training documentation,
- Refreshing all training materials, and
- Conducting mandatory refresher name check training.

Based on these strategies, the NNCP reduced the name check request backlog by 90 percent. As of October 21, 2008, there were 33,018 in process.

Issue 2.3: The FBI's use and maintenance of its Guardian system could be improved in several ways. For example, the FBI needs to better ensure the accuracy, timeliness, and completeness of the information entered in Guardian, as well as provide better oversight. Additionally, the Guardian system requires updates to improve its functionality and value.

Action: Based on a review of the OIG report on this issue, the FBI concurs with the OIG's assessment and seven recommendations. As a result of this report and the September 29, 2008, signing of the new Attorney General Guidelines (AGGs) for Domestic FBI Operations, the FBI will issue updated policy and guidance to all field offices and personnel working counterterrorism matters. This guidance will incorporate the seven recommendations and changes to the FBI Threat Mitigation policy and procedures that are directly affected by the new AGGs. This policy and guidance will be issued prior to the effective date of the new AGGs on December 1, 2008.

The FBI is committed to ensuring appropriate supervisory review of threat and suspicious activity incidents entered into Guardian. To ensure that terrorist threats and suspicious incidents entered in Guardian are closed or forwarded for investigation in a timely manner, existing policy regarding this matter is being reinforced by the FBI's National Threat Center Section (NTCS), Counterterrorism Division (CTD). The Guardian development team is committed to the future enhancement of Guardian. In response to concerns outlined in the OIG report, the FBI has developed and implemented a schedule to ensure technical patches to the Guardian system are completed in a timely manner.

3. Information Technology Systems Planning, Implementation, and Security

3. Information Technology Systems Planning, Implementation, and Security: The Department must ensure that the more than $2 billion it spends on IT systems is being used effectively. The Department must ensure the security of its systems and the information contained in them, balancing the need to share intelligence and law enforcement information with the need to ensure that such information sharing meets appropriate security standards.

Issue 3.1: An OIG audit found that the IT systems cost information the Department provides to Congress, OMB, and senior Department management is unreliable. Specifically, IT systems cost reporting within the Department is fragmented, uses inconsistent methodologies, and lacks control procedures necessary to ensure that cost data is accurate and complete. The OIG concluded that the lack of complete and verifiable cost data undermines the effectiveness of oversight of IT projects by various entities, including the DIRB, Department and component CIOs, Congress, and OMB.

Action: The Department has drafted an IT system cost reporting standard that is in the process of review by Chief Financial Officers (CFOs) and CIOs of major components, following review by the principal OIG auditor for Audit 07-37. The standard contains data definitions that will aid in the consistent reporting of IT systems costs in components' legacy financial systems, and will serve as the basic requirement for tracking and reporting IT costs in the Unified Financial Management System (UFMS).

Issue 3.2: Several major IT projects such as the Unified Financial Management System (UFMS), the Litigation Case Management System, and the Integrated Wireless Network (IWN) project still remain risky in terms of cost, schedule, and performance.

Action: The Department has enhanced its oversight of these programs through more comprehensive program reviews and greater analysis using the Earned Value Management System (EVMS). The results of these reviews are being briefed monthly to senior management and are subject to quarterly reviews by the DIRB to ensure the highest possible level of executive oversight. The Justice Management Division (JMD) agrees that these programs are high risk and has dedicated additional staff to the projects to help minimize exposure.

Issue 3.3: The Department does not exercise direct control over IT projects among Department components. Historically, the components have resisted centralized control or oversight of major IT projects, and the Department's Office of the Chief Information Officer (OCIO) does not have direct operational control of components' IT management.

Action: The CIO has improved oversight of the Departments major IT initiatives and high risk projects in several ways, including conducting a CIO Council that meets every quarter to enhance the understanding of the needs of the various DOJ components. This also has greatly improved the communication between the component CIO community and the JMD staff. In addition, major IT programs are being reviewed by the DIRB which monitors them against their projected costs, schedules, and benefits, and takes corrective action to continue, modify, or terminate them.

Issue 3.4: OIG audits of the Department's information security conducted pursuant to the Federal Information Security Management Act (FISMA) have identified continuing weaknesses with the Department's management, operational, and technical controls for its classified and sensitive but unclassified systems. Specifically, the Department lacks effective methodologies for tracking the remediation of IT vulnerabilities identified in monthly system configuration scans, applying department-wide remedies for known vulnerabilities, and conducting an inventory of devices connected to the Department's various IT networks.

Action: The Department plans to provide a Vulnerability Tracking System that will be operational by January 30, 2009. This system will effectively track the remediation of IT vulnerabilities identified in system configuration scans, apply department-wide remedies for known vulnerabilities, and conduct an inventory of devices connected to the Department's various IT networks. The Vulnerability Tracking System is comprised of two tools. The Foundstone tool will be used to identify the inventory of devices, identify IT vulnerabilities, and identify whether IT vulnerabilities have been resolved through remediation by the DOJ components. Another tool, such as SharePoint or a similar application, will be used for document management and information sharing. Department engineers will research and define the remedies to vulnerabilities, determine the priority, and upload this data to the information sharing application. This application will be used to communicate the information Department-wide, as well as track the status of vulnerability remediation for all systems on a DOJ component by component basis. Each DOJ component would implement vulnerability remediation activities based on their own processes, but in accordance with Department policy and direction.

Issue 3.5: The Executive Office for U.S. Attorneys (EOUSA) has insufficient controls to ensure the accuracy and completeness of its Victim Notification System (VNS) data. Also, there are deficiencies in the security of VNS information, most notably that sensitive crime victim information is not adequately protected.

Action: In June and July 2008, EOUSA met with individual representatives of the investigative agencies that participate in VNS to discuss strategies for improving the accuracy of victim contact information. Additionally, EOUSA conducted five basic VNS courses for victim witness personnel, during which the importance of the accuracy of victim contact information was emphasized. Also, EOUSA will raise this issue again with the investigative agencies at the upcoming VNS Executive Committee Meeting on October 30, 2008.

EOUSA views maintaining the privacy and security of crime victim information as a high priority. EOUSA has taken action based on OIG's security recommendations and has provided evidence to OIG concerning those actions. EOUSA will continue to work with OIG to provide any other evidence required to close the recommendations.

Issue 3.6: The FBI's name check processes rely on outdated and inefficient technology. While the FBI has explored some electronic tools to assist in the name check search process, it has not conducted a technical assessment of its phonetic name-matching algorithm, the key component in the name matching system, which matches names to the FBI's index of names in its investigative files. The OIG concluded that the FBI's algorithm is largely outdated and potentially ineffective, increasing the risk that submitted names are not accurately searched and matched against FBI files. While the FBI told the OIG that it lacked adequate funding to implement technological improvements in its name check process, the OIG noted that the FBI had not raised its name check fees in 17 years and, thus, lost opportunities to enhance its antiquated automated systems.

Action: Currently, the FBI's NNCP is partnered with the FBI's Information Technology Operations Division (ITOD) to conduct phonetic name-matching algorithm testing. The evaluation team currently is evaluating performance and conducting a detailed analysis of the results. The final results and recommendations from this testing process will be published in a formal report, the first draft of which is due in the middle of November 2008. The NNCP adjusted its Name Check fees in FY 2008 to cover its operational costs and to fund technological improvements to its name check process. A new fee study has just concluded and is tracking changes in cost as a result of operational improvements and business process re-engineering.

4. Civil Rights and Civil Liberties

4. Civil Rights and Civil Liberties: Balancing aggressive pursuit of its counterterrorism responsibilities with the protection of individual civil rights and civil liberties is a continuing challenge of the Department.

Issue 4.1: While the FBI and the Department have taken positive steps to address the issues that contributed to the serious misuse of National Security Letter (NSL) authorities, additional work remains to be done. For example, the Department's Chief Privacy and Civil Liberties Officer still has not revised its initial proposal and considered further whether and how to provide additional privacy safeguards and measures for minimizing the retention of NSL-derived information. In addition, it remains to be seen whether the FBI's new Office of Integrity and Compliance (OIC) will be effective in detecting and correcting non-compliance with the rules governing the intrusive techniques available to the FBI.

Action: The NSL Privacy and Civil Liberties Working Group (NSL Working Group) is nearing completion of the revised memorandum concerning enhancements to the safeguards for privacy and civil liberties connected to the FBI's use of National Security Letters. The working group conducted field research to understand the processes associated with the collection, use, and maintenance of NSL-derived records and to support the development of new procedures that seek to clarify and strengthen protections for privacy and civil liberties.

The FBI Integrity and Compliance (I&C) Program is managed by the OIC and was formally established by the Director on June 25, 2007. The program is modeled on corporate-style compliance programs and is geared to identify and mitigate the risk of non-compliance in all aspects of the FBI's day-to-day operations and activities. OIC's mission is "to develop, implement, and oversee a program that ensures that there are processes and procedures in place that promote FBI compliance with both the letter and the spirit of all applicable laws, regulations, rules, and policies ... and to endeavor to protect and enhance the FBI's reputation for integrity."

The OIC has implemented all the elements of a successful I&C program: management "buy-in"; organizational structure; risk assessment methodology and implementation; two-way communications; human resource policies that encourage compliance; audit; and documentation. Implementation highlights include the following: top-level management has demonstrated support for the I&C program as evidenced by the Director's decisions to stand-up the office and to personally lead the Integrity and Compliance Council. FBI executives support the program by leading and participating in executive compliance committees and assigning personnel to analyze and mitigate potential compliance risks. The program organizational structure in Phase I centered on the creation of the Integrity and Compliance Council, chaired by the Director, and the Executive Management Committees, chaired by each of the Executive Assistant Directors. Phase II implementation, which will move the I&C program to the program manager level, has begun. A risk assessment methodology was developed and is used by the compliance committees. Potential risks are identified, prioritized, and analyzed, and mitigation plans are developed and worked. Various lines of communication have been established between the OIC and FBI personnel, including creation of an OIC training video featuring FBI executives, creation of an OIC website, and numerous OIC briefings to various FBI stakeholders. In addition, OIC has established a compliance helpline which allows FBI employees to report compliance concerns anonymously. A non-retaliation policy for reporting compliance concerns was promulgated, compliance awards established, and an explicit compliance element has been incorporated into the performance appraisal plan of FBI employees. Finally, OIC has developed a high level monitoring plan for implementation of the AAGs for Domestic Investigations and the FBI Domestic Investigations and Operations Guide. OIC is working with FBI stakeholders to further define and implement the monitoring plan.

Issue 4.2: FBI case agents do not always update watchlist records when new information becomes known, nor does the FBI always remove watchlist records when it is appropriate to do so.

Action: To address concerns about the maintenance of watchlist records, the FBI Terrorist Review and Examination Unit (TREX) now conducts a bi-monthly scrub of all newly opened and closed international and domestic terrorism cases to ensure an FD-930 form ("Consolidated Watchlist Form for Terrorist Members") is submitted to add or remove individuals from the watchlist in a timely manner. There are several mechanisms currently in place to ensure records are updated as new information becomes available. First, the FBI has an extensive training program required for all agents and support staff who take part in the watchlisting process, which includes details on requirements to modify (i.e., update) records when new information is available. The FBI also conducts a supervisory review every 90 days of open cases on investigative progress. This review now includes a reminder for the case agent to update the FD-930 form with newly acquired information. In addition, when the Terrorist Screening Center (TSC) becomes aware of new information from a separate agency, it notifies the FBI of the record discrepancy and requests a review/update to the FD-930.

5. Restoring Confidence in the Department of Justice

5. Restoring Confidence in the Department of Justice: Restoring public confidence in the integrity of Department operations in light of concerns about politicized hiring is an ongoing challenge facing the Department. Related to this is the need to prepare for an orderly transition to new Department leadership when the Administration changes in early 2009.

Action: The Attorney General agrees that public confidence in the integrity of the Department is essential and that preparing for an orderly transition is an important challenge for the Department. The Attorney General believes that throughout 2008 the Department has taken significant steps and engaged in a sustained effort to address the issues affecting public confidence in the Department and to ensure a smooth transition to new leadership. Many of those actions are described in more detail below.

Issue 5.1: The Department's hiring of career employees was affected by improper political considerations. Committees screening applications inappropriately used political or ideological affiliations to "deselect" candidates, violating Department policy and federal law. At times, this resulted in rejecting high-quality career attorney candidates for important work details in favor of less-qualified candidates. It also affected screening of candidates for immigration judge positions and caused significant delays in appointing immigration judges at a time when the immigration courts were experiencing an increased workload and a high vacancy rate.

Action: As noted by the OIG, the Department has taken many steps to address these issues, both before and after the OIG / OPR reports were released, and has adopted all of the recommendations made by OIG and OPR. For example, the central review process for Honors Program hiring is now handled by career employees. The Department also issued stronger guidance to enforce the use of merit hiring principles and to clarify that political affiliation may not be used to evaluate candidates and that ideological affiliations may not be used as a proxy factor to discriminate on the basis of political affiliation. In addition, all current and new political appointees now receive briefing and training material on the applicability of merit hiring principles and prohibited personnel practices in career attorney hiring.

The July 2008 OIG / OPR report on inappropriate hiring practices also noted that the Department implemented a revised process for selecting Immigration Judges in July 2007. The revised process places the recommendations in the hands of career officials at the Executive Office of Immigration Review and the

Department. Under the revised process, 18 new Immigration Judges have taken the bench and 23 are currently in the hiring process.

Issue 5.2: The immediate challenge for the Current Attorney General and the Department's leadership is to ensure that the serious problems and misconduct the OIG found regarding politicized hiring for career positions and the dismissal of U.S. Attorneys do not recur.

Action: The Attorney General has said repeatedly that it is neither permissible nor acceptable to consider political affiliations of candidates while hiring career Department employees. To ensure this does not happen again, he has instituted remedial and ongoing mandatory training for all political appointees regarding prohibited personnel practices; directed implementation of all the institutional recommendations made in the OIG/OPR reports; appointed an attorney to investigate and determine any wrongdoing that may require legal action; and revised policies and procedures to prevent recurrence of this type of activity. As a result of these reforms, and others, the Attorney General is confident that the Department is on surer footing today than it has ever been before, and that the institutional problems identified in the OIG/OPR reports will not recur.

Issue 5.3: The Department must coordinate effectively with the Department's new leadership to accomplish an orderly and efficient transition.

Action: The Attorney General has said that ensuring an orderly and efficient transition is one of his top priorities during the remainder of his tenure. The Department has been proactive in its preparation and will remain proactive throughout the transition period. The Attorney General designated his Chief of Staff and the Assistant Attorney General for Administration, the senior career management official in the Department, as transition coordinators in April 2008. The coordinators have directed a Department-wide effort and are prepared to work with the incoming administration beginning immediately after the election. Among other things, the Department has:

- Identified career officials to lead each component following the departure of political appointees.
- Along with the FBI, worked with both campaigns to facilitate security clearances for transition team members before election day.
- Prepared briefing materials on Department organization, mission and functions, funding, and major issues to be addressed following inauguration.
- Conducted briefings for outgoing appointees to ensure compliance with applicable law and regulations.
- Prepared to brief incoming appointees on hiring practices, ethics, records responsibilities, and Department organization with particular emphasis on issues raised by OIG / OPR reports.

These proactive efforts will continue throughout the transition period.

6. Violent Crime

6. Violent Crime: While the Department's post-September 11 priorities were reordered to emphasize preventing terrorism, an ongoing challenge has been to maintain an appropriate emphasis on domestic crime. A key element of this is for the Department to effectively coordinate new initiatives to address violent crime with existing operations, including the Department's task forces and partnerships with state and local law enforcement agencies. This approach has yielded positive results. The rate of violent crime reported in the FBI's VCR for 2007 was the second lowest in thirty years. Notwithstanding this historic low, some communities continue to struggle with violent crime problems. The Department's current approach of targeting relief to areas most in need and working with our partners to develop a custom response to the particular challenges faced, is well suited to the crime challenges observed.

Management's Statement: The Department is pleased that the OIG recognizes the important work it is doing to address violent crime, including projects such as the Innocence Lost National Initiative, Internet Crimes Against Children, and Project Safe Childhood. To prevent duplication of effort among these and other task forces, the Department has issued policies aimed at improving coordination among them. The OIG also recognizes the progress the Department has made in implementing the Sex Offender Registration and Notification Act (SORNA), including issuing guidelines on compliance for states, working to make local registries accessible through the Department's National Sex Offender Public Registry web portal, and expanding access to the FBI's National Crime Information Center criminal history database.   Also, the U.S. Marshals Service (USMS) has increased federal investigations and arrests of fugitive sex offenders and has increased the assistance it provides to state agencies with fugitive sex offender investigations.

7. Cybercrime

7. Cybercrime: With the rapid technological advances and the widespread use of the Internet, combating cybercrime is a challenge for the Department and law enforcement nationwide. Cybercrime includes such criminal activities as fraud, identity theft, sexual exploitation of minors, and theft of intellectual property.

Issue 7.1: The FBI's key indicator for identifying the number of child pornography websites and web hosts shut down was not accurate because it used as a surrogate measure the number of subpoenas for subscriber information served on web hosting companies and Internet service providers (ISPs). Counting the number of subpoenas served is not a fully accurate measure of the FBI's activities in shutting down child pornography websites and web hosts because the FBI has no direct technical role in shutting down the websites.

Action: Following the OIG's Key Indicators Audit conducted during FY 2007, the FBI's Innocent Images National Initiative (IINI) reevaluated ways in which to report accomplishments related to investigations of Internet-based child pornography. As approved through the Program Assessment Rating Tool (PART) review conducted by the OMB during spring 2008, in the future the FBI will use a measure that records the number of children rescued as a result of FBI investigations into child pornography.

Issue 7.2: The OIG identified issues with the FBI's timely processing of evidence seized from computers and other electronic devices in investigating cybercrimes against children.

Action: The FBI agrees with the OIG that the expeditious processing of computer child pornography forensic evidence is a priority for its computer forensic examiners. The FBI already has focused personnel enhancements received in FY 2008 on staffing these types of examiners at a special laboratory in Maryland dedicated to supporting the FBI's IINI. The IINI Computer Analysis Response Team (CART) Laboratory will help reduce any existing backlog in processing evidence for top priority IINI investigations. The FBI continues to deploy new technologies as resources become available to help increase the efficiency of its field digital evidence forensic examiners. Deployment of the CART Storage Area Network system (SAN) forensic network, for example, in the majority of large FBI field offices has enabled the FBI to reduce the backlog each year by up to 10 percent despite an increase of seized data per year of up to 40 percent.

The FBI's chief constraints in processing this kind of forensic evidence are the volume of the computer evidence seized and the standards applied to its examination. Most U.S. Attorney's Offices require that the FBI conduct comprehensive forensic examinations on all computer technology-based materials found at a child exploitation crime scene, even if seemingly innocuous (e.g., music compact discs). The high volume of computer evidence seized at these crime scenes creates a huge forensic workload that complicates any attempt at speedy evaluation. In addition, meeting strict quality assurance (QA) standards, such as those established by the American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD-LAB), adds a great deal of time to processing computer evidence, time that is not spent strictly on forensic evaluation of pertinent material.

In the course of a continuing OIG audit on this issue, the FBI pointed out that it would be able to appreciably streamline procedures and reduce backlogs if it could apply the resources currently assigned to QA requirements to the processing of computer forensic evidence. The FBI subsequently made a written request in July 2008 to the OIG requesting clarification on whether or not the emerging digital evidence forensics discipline should, like other forensic disciplines, continue to be subject to ASCLD-LAB and other QA requirements as inferred from earlier publications of the OIG. To date, the OIG has not taken a position on whether digital evidence forensics requires the application of strict QA standards. The FBI does not anticipate the OIG taking a specific position on this question without initiating a much more significant, long term review.

8. Grant Management

8. Grant Management: Management and oversight of the billions of dollars in Department grants awarded annually remains a top Department management challenge.

Issue 8.1: There are problems with the design and management of Office of Justice Program's (OJP's) Human Trafficking grant program, grantees' compliance with essential grant requirements, and OJP's system for monitoring human trafficking service providers and task forces. In particular, the Department's award process resulted in a wide variation in funds awarded compared to the number of victims anticipated to be served. Furthermore, the service providers and task forces significantly overstated the number of victims they served, and the Department included this inaccurate information in its annual reports to Congress.

Action: OJP agreed with the recommendations made in the OIG audit and is fully committed to implementing corrective actions to strengthen the administration of the Human Trafficking grant programs. OJP will develop more comprehensible guidance to all task force grantees regarding best practices in maintaining supporting documentation, tracking data to be reported, and verifying the accuracy of the data.

Applicants will continue to estimate the number of victims that may be served in order to develop their project budgets and itemize projected costs; however, when determining the amount of the awards, OJP considers costs associated with outreach, training, and building community capacity to identify and serve all victims of human trafficking identified within a geographic area.

OJP will continue to ensure that applicant costs are reasonable and strategically sound prior to funds being awarded. OJP plans to employ the practice of special conditions that place financial holds on funds to ensure that the project strategy and budget for each application documented fully comply with essential grant requirements stated in the solicitation.

To further improve the reliability and validity of performance reports and the numbers of victims identified and served through the grants, OJP has initiated several actions, including: (1) greater collaboration among its components to ensure the most effective use of the Bureau of Justice Statistics (BJS) developed Human Trafficking Reporting System; and (2) increased technical assistance to all Office for Victims of Crime (OVC) grantees on the use of the Trafficking Information Management System (TIMS) to ensure consistency of the reporting data, thus enhancing the efficiency and reliability of the data collection process. OVC anticipates that it will provide the enhanced TIMS database to OVC grantees by January 2009.

Issue 8.2: OJP has weaknesses in monitoring and overseeing Southwest Border Prosecution Initiative (SWBPI) funds. Specifically, OJP did not require applicants to provide documentation supporting reimbursement requests and does not review applications for allowability and accuracy. Also, SWBPI reimbursements were not linked to actual costs incurred by the jurisdictions to prosecute federally declined-referred criminal cases. Further, OJP has not taken action to identify potential duplicate funding between the SWBPI program and other federally funded prosecution and pre-trial detention programs. An audit of seven SWBPI recipients identified unallowable and unsupported SWBPI reimbursements of $15.57 million of the $55.11 million awarded in those seven grants, or 28 percent of the total reimbursements.

Action: OJP agreed with the OIG recommendations and is implementing changes to the SWBPI system to ensure that reimbursement requests are limited to eligible, documented cases; linked to actual costs; and adjusted to account for any funds received from other federal prosecution and pre-trial detention programs.

9. Detention and Incarceration

9. Detention and Incarceration: The Department must safely and economically manage increasing federal detainee and inmate populations while facing overcrowding, lack of economical alternative detention space, stresses on prison staffing, and the rising cost of inmate health care.

Issue 9.1: The Department continues to report prison overcrowding as a material weakness in its annual performance and accountability reports, and the Federal Bureau of Prisons (BOP) projects the overcrowding rate to increase to 36 percent by the end of FY 2008 and to 37 percent by the end of FY 2009.

Action: The actual crowding rate for FY 2008 was 36 percent, which was lower than the projected crowding rate of 39 percent for fiscal year end. The current projection for FY 2009 overcrowding is 37 percent over rated capacity.

The FY 2008 targets were established prior to a recent Supreme Court decision regarding sentencing disparities between crack cocaine and powder cocaine. The U.S. Sentencing Commission changed guidelines to retroactively re-sentence inmates convicted of crack cocaine offenses and, in the majority of the cases, issue an order for either immediate release or a sentence reduction. The BOP is still reviewing the effects of this decision, but can report that by fiscal year end approximately 2,400 inmates had received a sentence reduction resulting in immediate release and an additional 9,200 inmates had received a sentence reduction. This resulted in slower than projected growth in the inmate population for FY 2008.

Issue 9.2: The infrastructure at many institutions has reached its limit. Approximately one-third of BOP's 114 institutions are more than 50 years old and renovation or expansion of these older facilities is not economically feasible because their infrastructure (including basic utilities) is designed for significantly smaller inmate populations. Further, according to BOP officials, overcrowding at all medium and high security facilities has accelerated the facilities' deterioration and need for renovations.

Action: Faced with limited funding to meet the increasing needs to repair failing infrastructure, the BOP continues to use available Modernization and Repair (M&R) funds to the fullest extent possible. An internal prioritization method is used to identify and fund the most urgent needs. This has resulted in the funding of 33 major projects over the past 2 fiscal years totaling $44 million. With this plan and the effective use of all M&R funds received, the BOP has reduced the M&R unobligated balance to the lowest levels ever in the past 2 fiscal years: $23.5 million in FY 2007 and $21.4 million in FY 2008. In addition, the BOP completed 435 projects in FY 2007 and 438 projects in FY 2008.

When M&R funding was at a greater level, the BOP implemented the Long Range Master Plan Program (LRMP). This program was developed to address the large inventory of needs in older facilities and provide the BOP with a survey that determines the extent of renovations required to bring the facilities to an adequate state of repair. From these surveys, the BOP completed 25 LRMP surveys and identified numerous projects that require funding. Additionally, from FY 2000 through FY 2008, the BOP funded 33 LRMP projects totaling $118 million. In order to operate within available resources, the BOP focuses on only the highest priority M&R projects in critical need of repairs. Thus, these LRMP projects could continue if the BOP receives increased levels of M&R funds.

Issue 9.3: In addition to the challenge that overcrowding presents in terms of confinement space, it also affects the safety and security of the federal prison system. In recent years, there have been several significant incidents of inmate violence at BOP institutions. BOP staff members have claimed that staffing shortages and prison overcrowding, complicated by gang rivalries, led to the violence.

Action: The BOP understands the challenges of overcrowding and its biggest priority remains filling vacant institutions positions. A BOP study completed in March 2006 found that a one percentage point increase in a Federal prison's crowding (inmate population as a percent of the prison's rated capacity) corresponds with an increase in the prison's annual serious assault rate by 4.09 assaults per 5,000 inmates. In addition, an increase of one inmate in a prison's inmate-to-custody staff ratio increases the prison's annual serious assault rate by 4.5 assaults per 5,000 inmates. This study finds that both the inmate to staff ratio and the rate of crowding at an institution are important factors that affect the rate of serious inmate assaults. The BOP is working with DOJ to increase funding for staffing in its institutions.

Issue 9.4: Regarding USMS Intergovernmental Agreements (IGAs) with state and local facilities to house detainees, there are problems with the manner in which the detainee-per-day charges were determined and with monitoring the charges.

Action: In November 2007, the Office of the Federal Detention Trustee (OFDT) implemented a pricing model, referred to as eIGA, in an attempt to ensure that the rates paid by the federal government are fair and reasonable. The OFDT is attempting to refine the eIGA so that operating cost information gathered from detention facilities is converted into an estimated, reasonable per diem rate that contracting officials can use as a baseline in negotiating the IGA rates. The OFDT is working with the OIG to determine what additional cost information will be collected. This information will be used to calculate a rate used by negotiators as additional information during the negotiation process to establish a fair and reasonable per diem rate.

Issue 9.5: Both BOP and the USMS face challenges in containing health care costs and providing quality health care for inmates and detainees. Although BOP has kept inmate health care costs at a reasonable level over the past 7 years, it could possibly further reduce costs. For example, some BOP institutions fail to review and verify medical bills of health care providers.

Action: On August 1, 2008, the BOP awarded a contract for Medical Claims Adjudication services. The BOP believes that claims review performed by a professionally trained, objective third party is the most effective method for assuring medical claims are processed accurately. The contract consists of a 2-year base period, with three 1-year option periods. The base period will focus on the Federal Correctional Complex (FCC)

Butner, the largest medical correctional complex in the BOP. FCC Butner has the largest volume of medical claims submitted for inmate health care. In the third year (first option year) three BOP regions will begin using the claims adjudication services, with the remaining three regions coming on board in year four (option year two). By year five, all BOP facilities will be using the services. The BOP believes this approach will increase the accuracy of claims review, identify errors in billing, identify potential patterns or trends of errors, and demonstrate that correct payments are being made for the services rendered. BOP will monitor the results of the adjudication services to identify potential changes to future contracting solicitations, improvements in local health services operations, and improvements in the timely processing of payments of medical claims.

10. Financial Management Systems

10. Financial Management and Systems: The Department must successfully implement an integrated financial management system to replace the disparate and, in some cases, antiquated financial systems used by Department components.

Issue 10.1: The Department's FY 2008 unqualified opinion and improved financial reporting, along with a reduction in material weaknesses at the consolidated and component levels was achieved through heavy reliance on contractor assistance, manual processes, and protracted reconciliations. The OIG remains concerned about the sustainability of these ad hoc and costly manual efforts.

Action: The Department continues to reflect improvement in its overall financial management by emphasizing internal controls and documenting processes at all levels of the organization. Progress was made in both general and application controls in FY 2008. One core departmental financial system was eliminated this fiscal year as the OJP converted to the JMD Financial Management Information System (FMIS). This leaves the Department with six core financial systems with the Drug Enforcement Administration (DEA) and the ATF scheduled to migrate to the Department's UFMS in fiscal years 2009 and 2010, respectively. Manual processes and reconciliations exist with any core financial system, but the Department believes that once it has completed the UFMS implementation, it will reduce many of the financial tasks that are performed manually, and the Department will have a standard process for doing business across its components.

Issue 10.2: Four years have passed since the Department selected a vendor for the unified systems, and full implementation of UFMS at the first component, DEA, is not scheduled to begin until FY 2009, more than 1 year behind schedule. Furthermore, implementation of the UFMS is not projected to be completed in all components until FY 2013 at the earliest. Until that time, Department-wide accounting information will continue to be produced manually, a costly process that undermines the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles.

Action: During FY 2008, DOJ continued to demonstrate progress toward development and deployment of a core financial 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.

Deployment of the pilot for the Asset Forfeiture Program was completed in November 2007. The pilot successfully processed transactions for 10 months of FY 2008 and recently completed the first year-end close under UFMS. The go-live for UFMS at the first major component, DEA, is on schedule for the end of December 2008. Training of almost 2,000 DEA end users began in October 2008, and the results of the first operational readiness review indicate all actions are in a green status, meaning completed or on schedule for completion by the required date. In addition, during FY 2008, the FBI continued work on preparation for

UFMS, and the ATF has begun to plan for its UFMS implementation. To help ensure success, the UFMS program receives guidance from the Department's senior leadership and employs an IV&V contractor for consultation. Additionally, the UFMS Project Management Officer briefs and discusses relevant project priorities with OMB on a monthly basis.

Issue 10.3: A January 2008 OIG audit of the FBI's management of confidential case funds to support its undercover activities found that the FBI lacked an adequate financial system necessary to manage these funds effectively. Consequently, FBI employees developed various "work-arounds" in an effort to track confidential case fund requests made by FBI special agents operating in undercover capacities. The review found that the sheer volume of bills, coupled with the inconsistent way various FBI field offices handle confidential case funds, resulted in the FBI routinely paying covert telecommunication costs late, which sometimes resulted in telecommunication carriers terminating FBI telephone lines for non-payment in important cases.

Action: The FBI recognizes the need to improve how it pays its covert telecommunication expenses and is taking several measures to ensure that all covert telecommunication bills are paid on time. It is:

- Mandating the Technical Management Database (TMD)
  - The TMD was created to standardize the tracking and reporting of surveillance techniques, operations, and invoices associated with the Field's Technical Programs. As of April 2008, the FBI mandated the use of TMD in field offices. This mandate brings consistency and transparency to how field offices manage information about their technical programs.

- Mandating Standard Operating Procedures for Paying Telecommunication Costs
  - In the past, FBI field offices have paid covert telecommunication bills in a variety of ways. The FBI is now moving to standardize how field offices pay them. The standard operating procedures are based on best practices in field offices and will involve streamlining the bill paying process, identifying specific roles in the process, and creating transparency and accountability. These standard operating procedures will ensure that all field offices are using best practices for paying covert telecommunication bills and that all bills are paid in a timely manner. The FBI is in the process of mandating these standard operating procedures to the field offices.

- Training FBI Employees
  - The FBI conducted five regional trainings to which all field offices were invited. These trainings covered the use of TMD and the standard operation procedures for paying covert telecommunication bills. Over 120 FBI employees from the field offices attended these trainings. These attendees represented both the financial and technical roles within the field offices.

- Enforcing the New Processes
  - In order to ensure that field offices are implementing the changes, the FBI will send out neutral audit teams to randomly selected field offices. The goal of the audit teams will be to 1) ensure that field offices are complying with all of the mandates concerning the management of covert telecommunication expenses, and 2) provide additional assistance and education if field offices are lacking in any area. In addition, the FBI's Inspection Division will now have responsibility for reviewing how field offices are using TMD and paying covert telecommunication bills. This will ensure that all field offices follow the new mandates consistently.