December 31, 2001

MEMORANDUM FOR THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management Challenges - 2001 List

Attached to this memorandum is the Office of the Inspector General's (OIG) December 2001 list of the Top Management Challenges facing the Department of Justice (Department). We have created this list annually, beginning in 1997 in response to a congressional request. It is our hope that the list will aid Department managers in developing strategies to address what we consider to be the top ten management challenges facing the Department.

As in past years, the challenges are not listed in order of seriousness. However, it is clear that the top challenge facing the Department is its response to terrorism, a challenge that we first placed on the list last year. In addition to updating management challenges that appeared on our list in previous years, this year we have added three new challenges ("Sharing of Intelligence and Law Enforcement Information," "Performance Based Management," and "Department of Justice Organizational Structure"). We combined two challenges from our 2000 submission ("INS Border Strategy" and "Removal of Illegal Aliens" have become "The INS's Enforcement of Immigration Laws") and removed two challenges ("Prison Overcrowding" and "Human Capital"). While the challenges we have removed remain important issues for the Department, we try to keep our list of challenges to ten.

We look forward to working with the Department to address these important management challenges, both by drawing upon findings and recommendations from past OIG reviews and by continuing to conduct reviews in these areas.

Please contact me at 514-3435 if you have any questions or if we can assist in any way.

Attachment

---

1. Counterterrorism: As the events of September 11, 2001, have illustrated, the United States faces grave threats of terrorist attacks. The use of chemical, radiological, and nuclear weapons remains a danger, while the use of biological agents has become a

reality. Terrorists could attempt to attack water supplies, communications, national infrastructure, or government institutions. Advances in computer technology and the Internet have increased the risks of cyber-terrorism. In recognition of these threats, last year we included for the first time the "Departmental Response to Terrorism" as a top management challenge facing the Department of Justice (Department).

This year, as the Department has recognized and as the Attorney General has clearly articulated in response to the attacks of September 11, terrorism is the most important challenge facing the Department. On November 8, 2001, when releasing the Department's Strategic Plan for fiscal years (FY) 2001-2006, the Attorney General stated that the fight against terrorism was now the first and overriding priority of the Department.

Accordingly, the first objective in the Department's Strategic Plan for 2001-2006 is to "Protect America Against the Threat of Terrorism." The three strategic objectives under this goal emphasize prevention and disruption of terrorist operations before an incident occurs, investigation of terrorist incidents to bring perpetrators to justice, and prosecution of individuals who have committed or intend to commit terrorist acts against the United States. The Strategic Plan notes the significant management challenge facing the Department as it seeks to effectively manage its counterterrorism program and avoid potential gaps in coverage or duplicate services provided by state and local governments. In addition, the infusion of billions of dollars into the Department's efforts to combat terrorism presents its own set of challenges.

In FY 2002, the OIG will devote significant resources to reviewing Department programs and operations that affect its ability to respond to the threat of terrorism. For example, we will examine the Federal Bureau of Investigation's (FBI) use of its counterterrorism funds. In separate audits, we will examine the mix of cases investigated by the FBI, as well as the FBI's management of its information technology (IT) projects.

The OIG is currently conducting an audit that relates to the government's ability to respond to terrorism. Our audit reviews domestic preparedness grants that the Office of Justice Programs (OJP) awards to state and local entities for training and equipment to respond to acts of terrorism. We also examine the amount of funding awarded and whether grants are being used for their intended purpose.

The OIG has also undertaken additional program reviews and audits in the Immigration and Naturalization Service (INS), whose work is critical to deterring terrorists from entering or remaining in the United States. For example, we have conducted follow-up reviews on INS programs such as the Visa Waiver Program and the INS's effort to control the Northern Border. We also have begun reviews of how the INS determines whether to send non-immigrants attempting to enter the United States to secondary inspection at air ports of entry, how the INS is handling its responsibilities to implement an automated system to monitor foreign students in the United States, and how the INS uses Advance Passenger Information System data to help deter the entry of terrorists or other criminals into the United States.

2. Sharing of Intelligence and Law Enforcement Information: One of the lessons arising from the September 11 terrorist attacks is the critical importance of sharing intelligence and other law enforcement information among federal, state, and local

agencies. Since September 11, the Attorney General and the Director of the FBI repeatedly have spoken about the importance of this issue, both to the investigation of the terrorist attacks and in ongoing efforts to prevent future attacks.

The Department must ensure that law enforcement agencies on the federal, state, and local levels have access to information that could be important in helping detect and deter terrorist attacks. The Department must also overcome any inclination by law enforcement and intelligence agencies to keep information solely within their agencies rather than sharing it with other law enforcement agencies.

By memorandum dated September 21, 2001, the Attorney General directed that information exposing a credible threat to the national security interests of the United States should be shared with appropriate federal, state, and local officials so that any threatened act may be disrupted or prevented. In late October, the President signed the *USA Patriot Act of 2001*, which permits greater sharing of intelligence and law enforcement information, such as information derived from Title III intercepts, information provided to grand juries, and information contained in criminal history databases.

However, the Department faces significant challenges in both ensuring that these new authorities are used appropriately and in ensuring that other federal, state, and local law enforcement agencies have access to information important to their work. An example of these issues is the failure of the INS and the FBI to link the information in their automated fingerprint identification systems and the consequences of that failure. A 1998 OIG inspection in the INS entitled "Review of the INS's Automated Biometric Identification System" (OIG report #I-1998-10) and a March 2000 OIG Special Report examined how the INS handled its encounters with a Mexican national accused of a series of murders in the United States ("The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System").

Nothing in the INS's automated fingerprint identification system (IDENT) alerted INS employees that the FBI and state and local law enforcement were looking for Resendez in connection with a brutal murder. The INS's IDENT system was not linked to FBI data, and when Border Patrol agents apprehended Resendez as he attempted to illegally cross the border into New Mexico, the Border Patrol followed its standard policy and voluntarily returned Resendez to Mexico. He returned to the United States within days of his release and murdered several more people before surrendering. This case highlighted the failure of the INS and the FBI to develop a way to share important criminal information about individuals. We noted the importance of expeditiously integrating IDENT with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) to enable the two systems to share fingerprint information.

A fully integrated IDENT/IAFIS system would provide INS employees with immediate information on whether a person they apprehend or detain is wanted by the FBI or has a record in the FBI's Criminal Master File. Similarly, linking IDENT and IAFIS could provide state and local law enforcement agencies with valuable immigration information as part of a response from a single FBI criminal history search request. The OIG recently issued a follow-up report (OIG Report #I-2002-003) on the status of INS and FBI efforts to integrate the two systems, concluding that integration has proceeded slowly and is still years away.

The OIG also has begun an audit that will address another aspect of information sharing. This audit assesses the procedures used by immigration inspectors at air ports of entry to prevent inadmissible persons from entering the United States. The OIG will analyze whether primary and secondary inspectors have access to needed intelligence information to prevent the entry of inadmissible persons into the United States.

3. Information Systems Planning and Implementation: OIG audits, inspections, evaluations, and special reports continue to identify mission-critical computer systems in the Department that were poorly planned, experienced long delays in implementation, or did not provide timely, useful, and reliable data. Given the critical role these systems play in the Department's operational and administration programs - not to mention the vast sums of money spent on developing and deploying these systems - information systems planning and implementation remains a top management challenge in the Department.

   For example, OIG audits have found that the INS has made huge investments in automation technology and information systems that have yielded questionable results. Our March 1998 audit titled "INS Management of Automation Programs" (OIG report #98-09) disclosed significant weaknesses in the management of the INS's automation initiatives. Among other things, we found that several major INS systems were behind schedule and that the INS lacked definitive performance measures for tracking critical project milestones. In July 1999, we issued a follow-up review of the INS's management of its automation programs (OIG report #99-19), which found that the INS continued to spend hundreds of millions of dollars on automation initiatives without being able to explain how the money was spent or what was accomplished.

   The General Accounting Office (GAO) has raised similar concerns in its reviews of INS IT practices. One GAO report concluded that the INS did not have an institutional system blueprint that lays out the organization's current and target IT operating environment (GAO report #AIMD-00-212). In another review, GAO determined that the INS had not implemented practices associated with effective IT investment and enterprise architecture management. Further, the INS's investments were not aligned with an agency-wide blueprint that defines the agency's future plans, and the INS did not know whether its ongoing investments were meeting their cost, schedule, and performance commitments (GAO report #02-147T). In another report, the GAO found that the INS was managing its IT investments as individual projects rather than as a complete portfolio and, consequently, will not be able to determine which investments contribute most to the agency's mission. The GAO also found that the Department was not guiding and overseeing the INS's investment management approach (GAO report #01-146).

   The OIG has also reviewed individual INS technology systems and found problems. In March 2000, the OIG issued a follow-up review of the INS's Passenger Accelerated Service System (INSPASS) (OIG report #00-07), an automated system designed to facilitate the inspection of low-risk travelers at airports. The report noted that as of 1998 the INS had spent more than $18 million to develop INSPASS and had, since the OIG's previous INSPASS audit in March 1995 (OIG report #95-08), increased INSPASS reliability, usage, and performance. However, we found that the benefits provided by INSPASS in FY 1998 were insignificant because only 1 percent of the travelers in the six participating airports used the automated system. While INSPASS

is a small program, we concluded that the problems found there illustrated some of the INS's overall problems with managing its automation initiatives.

Both the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 and the INS Data Management and Improvement Act of 2000 required the INS to develop an automated entry/exit system for use at land, sea, and air ports of entry. The INS's automated I-94 system was developed to meet the requirements of both laws. The efficient use of a fully automated I-94 system could aid the INS in identifying and tracking individuals when they enter and exit the country. Yet, a 2001 OIG audit (OIG report #01-18) assessed the design and implementation of the automated I-94 System and determined that the INS has not properly managed the project. As a result, despite having spent $31.2 million on the system from FY 1996 to FY 2000, the INS: (1) does not have clear evidence that the system meets its intended goals, (2) has gained the cooperation of only two airlines and is operating the system at only four airports, and (3) is in the process of modifying the system. Recent INS projections estimate that an additional $57 million for this system will be needed through FY 2005.

The OIG is currently examining the process by which the INS tracks and monitors foreign students and exchange visitors once they enter this country. As part of the review, OIG inspectors are examining the INS's implementation of the Student and Exchange Visitor Information System, an automated information system designed to track the immigration status of such students.

The OIG's concerns about Department information systems are not limited to the INS. An OIG Special Report issued in July 1999 examined how the Department handled FBI intelligence information related to its campaign finance investigation ("The Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation"). This report raised questions about how the FBI uses its automated databases. The Department's Campaign Finance Task Force used the FBI's Automated Case Support (ACS) system and other FBI databases to obtain information on individuals and organizations they had under investigation. However, we found that FBI practices and policies have handicapped the usefulness of the FBI's databases. For example, problems in the way information was entered or searched in the databases, together with the way that search results were handled within the FBI, resulted in incomplete data being provided to the Task Force. Further, we found that many of the FBI personnel we interviewed were not well versed in the use of the FBI's database systems.

In addition, the OIG's ongoing review of the belated production of documents in the Timothy McVeigh case will assess similar issues related to the FBI's automated information systems.

Due to the importance of information technology in the FBI and the large amounts of money involved, the OIG has begun an audit of the FBI's management of its information technology projects. This audit will assess: (1) how the FBI selects its IT projects, (2) how the FBI ensures that projects under development deliver benefits, and (3) how the FBI ensures that completed projects deliver the expected results.

We have raised issues with other Department information technology systems. For example, the OIG's FY 2000 audit of the U.S. Marshal Service's (USMS) financial statement (OIG report #01-30), found that implementation of the USMS

Standardized Tracking, Accounting, and Reporting System (STARS) continues to be problematic. During FY 2000, USMS field offices were continuing to use the agency's Financial Management System, which was originally scheduled to be replaced by STARS, because of delays in implementing the new system.

In FY 2001, the OIG issued an audit of the implementation of the Collection Litigation Automated Support System (CLASS) by the Department's Office of Debt Collection Management (DCM). This audit (OIG report #01-15) determined that the DCM was at least 18 months behind schedule in implementing CLASS and had incurred more than $4.6 million in additional costs. Moreover, DCM management could not project a completion date and estimated additional completion costs of $400,000 per month. Delays resulted from management indecision, changes in telecommunication requirements, and disagreements between the DCM and the Executive Office for United States Attorneys about CLASS's capabilities.

4. Computer Systems Security: In response to the threat to Department computers, databases, and networks, and in recognition of the importance of information technology, the Department has classified computer security as a material weakness since 1991. Recently, the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations gave the Department an "F" for its computer security efforts in FY 2001, the same grade the Department received in FY 2000.

   OIG audits have disclosed serious problems in computer security that could lead to the compromise of sensitive systems and data. The OIG conducts security assessments and penetration testing using state-of-the-art security system software. These reviews have found that select computer controls were inadequate to protect the systems and their sensitive data from unauthorized use, loss, or modification.

   The OIG is also conducting regular computer security audits mandated by the Government Information Security Reform Act (GISRA), which requires that Inspectors General audit the security of critical information systems in their agencies. Our audits assess the Department's compliance with GISRA and related information security policies, procedures, standards, and guidelines. In FY 2001, we tested the effectiveness of information security control techniques for nine systems (five sensitive but unclassified (SBU) and four classified systems) at the Executive Office for U.S. Attorneys, Federal Bureau of Prisons (BOP), Drug Enforcement Administration (DEA), Justice Management Division (JMD), and FBI.

   With respect to the five SBU systems audited, we found weaknesses in management, operational, and technical controls, including password management, logon management, user and account rights assignment, file system and system configuration, and system auditing management. With respect to the four classified systems, we found that select computer security controls were not implemented to protect the systems from unauthorized use, loss, or modification. We also noted weaknesses in password and logon management, account integrity, system auditing management, physical and personnel controls, contingency planning, and policies and procedures. Penetration testing on three classified systems also resulted in auditors obtaining access to the systems. For example, on one system the auditors obtained root access allowing them to identify user account identifications and passwords and giving them the capability to erase, modify, or upload files.

The weaknesses found on the SBU systems are considered low to moderate risk. Weaknesses found on the classified systems, when considered collectively, are a moderate to high risk. Weaknesses were more voluminous and material for the Department's classified systems because they had not been subject to the frequency of external reviews as had the SBU systems. For FY 2002, the OIG intends to perform 14 GISRA audits and will conduct application reviews of the DEA's MERLIN and BOP's SENTRY automated information systems.

In FY 2001, the OIG also issued a report assessing the Department's critical infrastructure protection planning for its computer-based infrastructure (OIG report #01-01). This report, part of a President's Council on Integrity and Efficiency government-wide review of the nation's critical infrastructure assurance program, found that while the Department submitted the required critical infrastructure protection plan, it had not yet: (1) adequately identified all its mission-critical assets, (2) assessed the vulnerabilities of each of its ADP systems, (3) developed remedial action plans for identifying vulnerabilities, or (4) developed a multi-year funding plan for reducing vulnerabilities. As a result, the Department's ability to perform certain vital missions could be at risk from terrorist attacks or similar threats.

5. The INS's Enforcement of Immigration Laws: The INS's enforcement of immigration laws, particularly its ability to deter illegal immigration and remove aliens who are here illegally, is a critical and longstanding management challenge.

   Within the INS, the Border Patrol faces significant enforcement challenges along the southwest and northern borders to stem the tide of illegal aliens, drugs, and potential terrorists. For example, in last year's list of top management challenges (December 1, 2000), we reported on the OIG's review of "The Border Patrol's Efforts Along the Northern Border" (OIG report #I-2000-004). The report identified significant gaps in the INS's northern border operations, the increasing illegal activity along the northern border, and the limited resources available to address this growing concern. In response to a recommendation contained in the OIG report, the INS reassessed its approach in managing risks at the northern border. Its new approach focuses on enhancing national security and on controlling cross-border crime activity and illegal migration while facilitating legitimate travel and commerce. While Attorney General Reno approved the northern border strategy in the final days of her term, one year later the INS has not developed any implementation plan. Given the Department's emphasis on securing the nation's borders post September 11, the need for implementation of a coordinated northern border strategy is greater than ever.

   Alien smuggling remains a serious problem confronting the INS, and the INS needs to have an effective anti-smuggling program. However, the OIG report "Survey of INS's Anti-Smuggling Units" (OIG report #I-2001-03) concluded that the INS's anti-smuggling program operates with limited effectiveness. The review found: (1) the program lacked coordination and direction, (2) the structure of the anti-smuggling program is problematic, and (3) the program has insufficient financial and personnel resources.

   A May 2000 GAO report titled "Alien Smuggling Management and Operational Improvements Needed to Address Growing Problems," (GAO report #GGD-00-103) reached a similar conclusion. This GAO report found that the INS's alien smuggling efforts have been fragmented and uncoordinated, that the INS does not know if it is

using its anti-smuggling resources most effectively, and that it lacks an agency-wide automated tracking system that would help prevent duplicative investigations and promote intelligence sharing.

An OIG audit found serious problems in how the INS handles its deferred inspection process. When additional immigration examinations are required of individuals seeking entry into the United States, they are sent to secondary inspection. If an immediate decision regarding admissibility cannot be made there, INS inspectors have the discretion to defer the inspection until a later date so that documentary evidence - such as an existing INS file - can be reviewed. In these cases, the individual is admitted (or "paroled") into the country and must report to an INS district office at a later date to complete the inspection. A 2001 OIG audit of the INS Deferred Inspection Program (OIG report #01-29) revealed that in our sample nearly 11 percent (79 of 725) of the individuals paroled into the country under the deferred inspections process failed to appear at an INS office to complete their inspection.

This audit also found that the INS did not have adequate procedures in place to ensure that individuals who fail to appear are either brought in to complete their inspections or are appropriately penalized for failing to appear. In many cases, we found that the INS did not initiate follow-up activity of any kind. Our analysis revealed that among those who failed to appear, INS inspectors identified over 50 percent as either having criminal records or immigration violations at the time of entry. Subsequent OIG inquiries of criminal history databases revealed that nine individuals in our sample were charged or convicted of crimes considered to be aggravated felonies after their deferral.

Additionally, we found that the INS's controls were inadequate to determine the effectiveness of the deferred inspection process or the number of individuals deferred and the outcome of those inspections. Records maintained at airports and district offices were incomplete. Inspectors at all nine airports we visited destroyed deferral documentation after limited and varied retention periods. The INS's paper-based tracking of deferred inspections failed to provide an adequate agency-wide system of tracking deferrals. As a result, inspectors were unable to detect parole violators and other repeat offenders upon their reentry into the United States.

The INS lacks an effective enforcement policy that specifically targets the overstay population. While the INS estimates that overstays comprise 41 percent of the illegal alien population in the United States, INS data shows that only a small percentage of the deportable aliens apprehended by INS investigators are overstays.

A 1996 OIG inspection found that the INS's program to deport illegal aliens has been largely ineffective, finding that the INS was successful in deporting only about 11 percent of non-detained aliens after final orders had been issued. Anecdotal information continues to support this low percentage. In a more recent inspection (OIG report #I-99-09), we noted that ineligible aliens, including convicted felons, were inappropriately granted voluntary departure because the INS and the Executive Office for Immigration Review had not ensured that all eligibility requirements are met. We found that the INS lacks an effective departure verification system and therefore has no way of knowing whether illegal aliens granted voluntary departure have left the country.

The monitoring of alien overstays and removal of criminal aliens has been a Department material weakness since 1997. Among other issues, the INS failed to identify many deportable criminal aliens, including aggravated felons, or initiate Institutional Removal Program (IRP) proceedings before they were released from prison. The Department's Management Controls Report for FY 2000 stated that the INS issued new policy guidance to clarify the roles of agents working in the IRP, developed better inmate tracking systems to identify and deport criminal aliens, and developed new staffing models to allow the INS to concentrate resources where they are most needed. The OIG is currently performing an audit of the IRP to determine if past OIG recommendations were implemented and assess whether program enhancements can streamline the IRP process.

The OIG issued an inspection report in 2001 titled "INS's Escort of Criminal Aliens" (OIG report #I-2001-005). This report found that the INS's practice of escorting criminal aliens on commercial airlines when the aliens are removed from the United States to non-border countries placed the traveling public at potential risk because the INS does not consistently follow its established escort policy. In three of the four districts visited by the OIG, INS managers disregarded established INS policies, resulting in the placement of violent aliens, without escorts, on commercial airlines.

As discussed above, the OIG is conducting several follow-up reviews that identified issues to assess the progress made to correct deficiencies identified by previous OIG inspections of the INS's enforcement efforts. The follow-up reviews concern OIG inspections on "Border Patrol Efforts Along the Northern Border" (OIG report # I-2000-04), "The Potential for Fraud and INS Efforts to Reduce the Risks of the Visa Waiver Pilot Program" (OIG report #I-1999-10), "Transit Without Visa Program Inspection" (OIG report #I-1992-07), and "INS's Monitoring of Nonimmigrant Overstays" (OIG report #I-1997-08).

6. Financial Statements and Systems: While the Department has made some progress in improving its financial statements and systems, this issue remains a top management challenge. In FY 2000, the Department received an unqualified opinion on its consolidated balance sheet and statement of custodial activity (OIG report #01-07). However, the Department received a qualified opinion on the remaining financial statements due to the INS's inability to substantiate the earned revenues offset portion of Immigration Program Costs because of inadequate records to support the pending applications at the beginning of the fiscal year.

   Audits of the Department's financial statements reported three material weaknesses and one reportable condition at the consolidated level and 15 material weaknesses and 23 reportable conditions at the component level for FY 2000. Thus, much work still needs to be done to eliminate the internal control weaknesses found during the financial statement audits. Congress recognized this when the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations gave the Department a "D-" for its FY 2000 financial management, the same grade it received for its FY 1999 efforts.

   Most Department components still tend to view the preparation of financial statements as an end-of-the-year exercise they often meet by hiring a significant number of contractors and performing labor-intensive procedures. Because the Department lacks automated systems to readily support financial statement preparation and ongoing accounting operations, many tasks have to be performed

manually. One such task, the year-end count of INS applications needed to determine deferred revenue, caused delays in processing applications. Other problems resulted from the lack of integration between the Department's automated accounting systems and subsystems. Because systems are not designed to readily produce or support information needed to produce the financial statements, the Department's finance staffs had to perform additional manual reconciliation of data. The Department's ability to maintain or improve its audit results will require continuation of the substantial efforts expended this past year. Any decrease in this effort could adversely affect the Department's audit results.

In addition, Department components including the INS and Federal Prison Industries, Inc., continue to encounter significant difficulties in implementing their financial management systems. With new financial systems needed at several components, it is imperative that the Department overcomes these implementation difficulties in order to continue on a path toward improving its financial management and eventually removing this issue as a management challenge.

7. Detention Space and Infrastructure - the USMS and the INS: Obtaining and efficiently managing detention space for the USMS and the INS - a material weakness in the Department since 1989 - remains a top management challenge. Both agencies continue to experience rapid growth in their use of detention space, from an average of 43,408 beds in 1998 to a projected 64,962 beds in 2002. The INS, in particular, may need additional detention space in light of the Department's response to the September 11 attacks. Expanding the use of detention space also places increasing demands on INS and USMS transportation, communications, and staff.

   To obtain additional detention space, the Department has relied on outside contractors (including state and local governments and for-profit entities) to house federal detainees. OIG audits of contractors for detention space have resulted in significant dollar findings. For example, in FY 2001 we issued an audit of an intergovernmental agreement (IGA) for detention space with York County, Pennsylvania (OIG report #GR-70-01-005). The audit revealed that in FY 2000, York overcharged the Department a total of $6.1 million due to York's understatement of its average daily population, a key figure used to determine reimbursement from the INS. If York uses the jail day rate determined by our audit and the INS, the USMS, and the BOP continue to use the same amount of jail days, the Department could realize savings of approximately $6.4 million annually.

   An OIG audit of the IGA with the Government of Guam (OIG Report #GR-90-01-006) found that for the period of October 1, 1998, through September 30, 2000, the Department overpaid Guam more than $3.6 million based on the actual allowable costs and the average daily population. In addition, the OIG found that the Department could realize annual savings of $3.3 million by using the audited rate for future payments.

   Our discussions with the Department, the INS, and the USMS disclosed considerable disagreement regarding the nature of the agreements used to obtain jail space from state and local governments. In our view, the Department has not yet settled on a procurement process to obtain detention space in a manner that meets prudent business practices and existing procurement regulations.

Another OIG audit (OIG report #01-16) determined that as many as 18,000 federal detainees are held in private facilities on any given day, and the use of these private facilities is expected to increase. We concluded that the Department's reliance on only a few private providers raises concerns about the impact should one of those providers cease operations. The OIG report noted that the BOP, the USMS, and the INS had not developed a coordinated contingency plan to address the loss of bed space if a private provider is unable to continue operations on a large scale. Without coordinated contingency planning, the disruption of contract detention services could lead to a host of legal, health, financial, logistical, safety, and security issues.

OIG reviews have highlighted the need for additional bed space for juveniles detained by the INS. During an inspection of the Border Patrol's efforts to control illegal entries along the United States-Canada border (OIG report #I-2000-004), the OIG was told by the Border Patrol that most aliens apprehended by Border Patrol Agents (BPAs) are released pending a court date because of shortages in detention space. Aliens interviewed by BPAs along the northern border reported that smugglers had assured them that even if they were apprehended while being smuggled into the United States they would later be released.

In an OIG review titled "Unaccompanied Juveniles in INS Custody" (OIG report #I-2001-009), the OIG examined the treatment of unaccompanied and undocumented juveniles who are held in INS custody for more than 72 hours and placed into formal immigration proceedings. We found deficiencies at INS districts, Border Patrol sectors, and INS headquarters that could have potentially serious consequences for the well being of the juveniles. These deficiencies included lack of segregation for non-delinquent and delinquent juveniles and lack of required weekly visits by INS juvenile coordinators with all juveniles in INS custody.

In FY 2002, the OIG plans to audit the Department's detention activities. Among the issues of concern is the extent to which Department components share information about detention needs in specific geographic areas and coordinate with each other in acquiring detention space at consistent and economical rates. In addition, we will also continue to audit USMS and INS agreements for detention space with government and for-profit providers, as OIG resources permit.

Finally, the Department recently established a Detention Trustee with broad responsibilities related to many of the problems discussed above. We are concerned that the Detention Trustee may not have the authority or resources to resolve the many long-standing detention issues that he is expected to address.

8. Grant Management: In recent years, the Department has become a grant-making agency that has disbursed billions of dollars to grantees. Among other initiatives, the grants support community policing, encourage drug treatment programs, reimburse states for incarcerating illegal aliens, and fund counterterrorism initiatives. For a Department that historically had limited experience in awarding, monitoring, and reporting on grant progress, the infusion of such significant amounts of grant money over the past several years has resulted in a continuing management challenge for the Department.

   Overall, OIG reviews have found that many grantees did not submit required program monitoring and financial reports and that program officials' on-site monitoring reviews did not consistently address all grant conditions. For example, an

OIG inspection found that some grantees who received formula grant funds from the OJP for prison substance abuse services needed to improve their reporting of program implementation and their accounting for matching funds and federal grant funds sub-awarded to state and local agencies (OIG report #I-2000-022). We found that OJP's administration of this grant program could be strengthened through better monitoring and by obtaining more timely and definitive information from grantees.

OJP provides State Criminal Alien Assistance Program (SCAAP) grants to state and local governments to help defray the cost of incarcerating undocumented criminal aliens convicted of felonies. Our audit of this program (OIG report #00-13) found that the five states reviewed by the audit received overpayments for unallowable inmate costs and ineligible inmates. The aggregate cost of these overpayments totaled approximately $19.3 million. We also found that OJP's methodology for compensating applicants was over-inclusive and should be improved, and we estimated that OJP overpaid applicants in our sample for at least 1,760 inmates whose immigration status was "unknown."

Several years ago, the OIG audited the management and administration of the Office of Community Oriented Policing Services (COPS) Grants Program (OIG Report #99-14) to evaluate COPS' ability to meet its goal of adding 100,000 police officers, COPS' and OJP's monitoring of grantees, and the quality of guidance provided to grantees to assist them in implementing essential grant requirements. At the time of the audit, we reported numerous deficiencies in the grant monitoring of COPS grants, some of which have continued through FY 2001. Based on our concerns, the OIG will continue to audit individual COPS grantees to ensure the monies provided are used for the purposes specified in the grant award (42 individual COPS grant audits were issued in FY 2001).

In FY 2002, the OIG is planning to perform an audit of administrative grant activities in OJP, and between OJP and COPS, to identify functions that can be streamlined.

9. Performance Based Management: On November 8, 2001, the Attorney General challenged the Department to hold itself accountable through performance measures, stating that "Performance should be measured by outcomes and results, not inputs." Similarly, the President's "Management Agenda for Fiscal Year 2002" prepared by the Office of Management and Budget (OMB) demands integration of budget and performance, stating "[o]ver the past few years the Department has seen a significant expansion in its mission and a rapid growth in resources. Meaningful measures supported by performance data, particularly measures of program outcome, are essential to evaluate this investment and determine future resource requirements."

   A pressing management challenge for the Department is ensuring, through performance based management, that its programs are achieving their intended purposes. The Department received a congressional grade of "F" for its 1999 performance report that assesses agency progress towards meeting the mandates of the Government Performance and Results Act (GPRA).

   The GAO reviewed the Department's FY 2000 performance report and the FY 2002 performance plan to assess Department progress in achieving selected key outcomes that were identified as important Department mission areas. The GAO reported that the Department's overall progress towards achieving each of the four key outcome

measures was difficult to ascertain because the performance report generally lacked measurable targets and lacked clear linkage between performance measures and outcomes.

The OMB has recognized that the Department's establishment of a Strategic Management Council (SMC) should aid in focusing the Department's resources on programs that result in positive outcomes, not simply output. The SMC is designed to provide direction and leadership on Department strategic planning, resource management, and performance accountability.

In a Department that has grown so rapidly over the past decade, linking credible performance measures to budget development and allocation of resources is a significant challenge. As a regular part of OIG program audits, we examine performance measures for the component or program under review. We highlight the existence or absence of such measures and offer recommendations as to whether the reported results are supported by reliable measurement methods or systems. We will continue to do so with our audits.

In addition, in FY 2002 we plan to audit the DEA's implementation of the GPRA. The audit will assess whether the DEA has developed quantifiable goals that support its mission and whether the performance data gathered to date are valid and accurate.

10. Department of Justice Organizational Structure: The Department is developing or implementing reorganization plans in several of its components. While some of this reorganization is related to the events of September 11, some is designed to correct long-standing organizational problems. The challenge for Department managers is not only to ensure that the reorganizations accomplish their intended purposes, but also to see that the Department's interconnected programs and functions are not adversely impacted by the changes.

    The INS has proposed reorganizing itself into two separate but connected bureaus, one to handle enforcement of immigration laws and one to provide services and benefits to immigrants. Members of Congress are advocating competing reorganization proposals, including one that would break the INS into separate agencies to focus on enforcement and benefits and another that would create separate bureaus but retain a single agency structure. Among the INS's many challenges in any such reorganization will be to ensure that quality service is provided to eligible applicants while reconciling competing priorities, addressing insufficient accountability between field offices and headquarters staff, repairing outdated IT systems, and harmonizing inconsistent operations and policies.

    OJP is reorganizing to reduce duplication in grant programs and improve efficiency. As mentioned previously, the OIG plans to audit OJP to assess the level of duplication in its grant management and oversight process in an effort to identify efficiencies.

    Finally, the FBI is reorganizing its operations and reevaluating its mission in light of the September 11 attacks and its new priority to prevent acts of terrorism. In December 2001, the FBI Director announced a restructuring plan for FBI Headquarters that the FBI described as the first step in a "phased process of reorganizing assets, modernizing and integrating new technology, and consolidating functions."

To assist in this restructuring effort, the OIG will review the FBI's allocation of resources to conduct the varied investigations under its jurisdiction. The audit will: (1) evaluate the types and number of cases the FBI investigates, (2) assess performance measures for FBI casework, and (3) determine if opportunities exist for certain investigations to be handled by other federal, state, and/or local law enforcement agencies.