APPENDIX D

Inspector General's List of the Most Serious Management Challenges

U.S. Department of Justice

Office of the Inspector General

Washington, D.C. 20530

November 8, 2002

MEMORANDUM FOR THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management Challenges – 2002 List

Attached to this memorandum is the Office of the Inspector General's (OIG) 2002 list of the Top Management Challenges facing the Department of Justice (Department). We have created this list annually since 1998, initially in response to congressional requests, but in recent years as part of the Department's annual Performance and Accountability Report.

Given the strong likelihood that the Immigration and Naturalization Service (INS) will be transferred from the Department to the proposed Department of Homeland Security, we have not included INS programs in this year's list of top management challenges facing the Department. Instead, we have developed a separate list of top management challenges facing the INS, which also is appended to this memorandum. This separate list was drafted to assist the proposed Department of Homeland Security in managing and assimilating the INS.

As in past years, the top management challenges are not listed in order of seriousness, although it is clear to us that the top challenge facing the Department is its ongoing response to the threat of terrorism. This year, in addition to updating management challenges that have appeared on our list in previous years, we added a new challenge – "Human Capital" – to replace the "INS's Enforcement of Immigration Laws." That issue, along with elements from several other Department challenges, is included in the INS list of top challenges.

We hope that these lists assist managers in developing strategies to address what we consider to be the top management challenges facing the Department and the INS. We look forward to working with the Department to

address these challenges, both by drawing upon findings and recommendations from past OIG reviews and by conducting new reviews in these and other important areas.

Please contact me if you have any questions or if we can assist in any way.

Attachments

cc: Robert Diegelman
Acting Assistant Attorney General for Administration
Justice Management Division

David T. Ayres
Chief of Staff to the Attorney General

Susan Richmond
Assistant to the Attorney General

David H. Laufmann
Chief of Staff to the Deputy Attorney General

David A. Margolis
Associate Deputy Attorney General

Daniel J. Bryant
Assistant Attorney General for Legislative Affairs

Top Management Challenges in the Department of Justice: 2002

The Office of the Inspector General (OIG) has developed an annual list of top management challenges facing the Department of Justice (Department) since 1998. This list of top challenges, originally prepared in response to congressional requests, is now required by the Reports Consolidation Act of 2000 to be included in the Department's annual Performance and Accountability Report.

In light of pending legislation to transfer the Immigration and Naturalization Service (INS) from the Department to the proposed Department of Homeland Security, we have not included INS programs in this year's list of top management challenges facing the Department. Instead, we have developed a separate list of top management challenges in the INS. We believe that this approach will assist the Department of Homeland Security in successfully assimilating the INS, or the Department in managing the INS should it not be transferred.

1. Counterterrorism: In the year since the September 11, 2001, terrorist attacks, the Department has identified preventing, detecting, and deterring future terrorist acts as the agency's highest priority. To this end, the Department and other federal, state, and local government agencies are attempting to increase communication, share intelligence, and increase domestic preparedness. In light of the seriousness of the threat and the significance of the task, counterterrorism is the top management challenge for the Department.

   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: 1) prevention and disruption of terrorist operations before an incident occurs; 2) investigation of terrorist incidents to bring perpetrators to justice; and 3) prosecution of individuals who have committed or intend to commit terrorist acts against the United States. The Strategic Plan notes the challenges facing the Department as it seeks to effectively manage its counterterrorism program and avoid gaps in coverage or duplicate services provided by other law enforcement or intelligence organizations. In addition, the infusion of billions of dollars to help fund these expanded counterterrorism efforts presents Department managers with challenges to ensure that the funds are spent in an efficient and effective manner.

   During the past year, the OIG has continued to review Department programs that relate to the Department's ability to successfully address these challenges. For example, the OIG recently audited the Federal Bureau of Investigation's (FBI) management of aspects of its counterterrorism program from 1995 through April 2002. We found that the FBI had not developed a comprehensive written assessment of the risk of a terrorist threat facing the United States, despite its statement to Congress in 1999 that it would. We concluded that such an assessment would have been useful not only to define the nature, likelihood, and

severity of the threat but also to identify intelligence gaps and determine appropriate levels of resources to effectively combat terrorism. Further, although the FBI has developed an elaborate, multilayered strategic planning system, the system had not established priorities adequately or allocated resources effectively to the counterterrorism program. Specifically, the planning system acknowledged a general terrorist threat to the nation, but the FBI did not perform and incorporate into its planning system a comprehensive assessment of the threat of terrorist attacks on U.S. soil. Similarly, the planning system identified numerous vulnerabilities and weaknesses in the FBI's capabilities to deal with the general terrorist threat, but the FBI did not make the fundamental changes necessary to correct the deficiencies.

The OIG audit also detailed the level of resources that the FBI has dedicated to counterterrorism and related counterintelligence between 1995 and 2002. The report made 14 recommendations to help improve management of the FBI's counterterrorism program, including that the FBI establish a time goal and a process for building a corps of professional, trained, and experienced intelligence analysts for assessing and reporting on threats at both the strategic and tactical levels.

As part of a review of critical infrastructure protection sponsored by the President's Council on Integrity and Efficiency (PCIE), the OIG issued a report entitled, "Departmental Critical Infrastructure Protection Planning for the Protection of Physical Infrastructure" (OIG Report #02-01). The audit found that the Department's ability to perform vital missions is at risk from terrorist attacks or similar threats because the Department had not planned adequately for the protection of its critical physical assets. This is the second phase of a four-part review planned by the PCIE to examine critical infrastructure issues in federal agencies.

The Department cannot respond to the counterterrorism challenge alone, and to this end it provides grants to state and local agencies to enhance their ability to respond to terrorist acts. In fiscal year (FY) 2002, the OIG audited the State and Local Domestic Preparedness Grant Program (OIG Report #02-15) and found that grant funds were not awarded quickly, and grantees were slow to spend available monies. We also found that nearly $1 million in equipment purchased with grant funds was unavailable for use because grantees did not properly distribute the equipment, could not locate it, or had been trained inadequately on how to operate it.

A somewhat different but critical challenge for Department employees in responding to the terrorism threat is to use its law enforcement and intelligence gathering authorities consistent with the law. The USA PATRIOT Act directed the Inspector General to "receive and review" allegations of civil rights and civil liberties abuses by Department employees. In furtherance of this mandate, the OIG is investigating several specific allegations of abuse against Department employees. In addition, the OIG is completing a review of the treatment of non-citizens detained in the aftermath of the September 11 terrorist attacks. Specifically, the OIG is examining the access to counsel, timeliness of charging decisions, and conditions of confinement for non-citizen detainees at the Metropolitan Detention Center in

Brooklyn, New York, and the INS contract detention facility in Paterson, New Jersey.

In FY 2003, the OIG intends to devote significant resources to reviewing Department programs and operations that affect its ability to respond to the threat of terrorism. Among the planned OIG reviews are examinations of: (1) the Department's counterterrorism fund; (2) the FBI's dissemination of intelligence information to federal, state, and local law enforcement agencies; (3) the effectiveness of multi-component anti-terrorism task forces; and (4) the FBI's language program and efforts to hire linguists. We also will continue to review intelligence-sharing processes within the Department, a key component in the Department's counterterrorism effort and a topic discussed more extensively in the next challenge.

2. Sharing of Intelligence and Law Enforcement Information: One of the key issues arising from the September 11 terrorist attacks is the importance of sharing intelligence and other law enforcement information among federal, state, and local agencies. During the past year, the Attorney General, the FBI Director, and Members of Congress repeatedly have discussed the importance of information sharing, both to the investigation of the terrorist attacks and in the government's efforts to prevent future attacks.

Ten days after the September 11 attacks, 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 October 2001, the President signed the USA PATRIOT Act, 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.

The Department continues to face significant challenges in ensuring that other federal, state, and local law enforcement agencies have access to information important to their work. The OIG examined several of these issues in its September 2002 review of aspects of the FBI's counterterrorism program (OIG Report #02-38). In addition to the need to develop and disseminate a written assessment of the threat of a terrorist attack, our audit noted a number of impediments to the FBI's effective processing of tactical threat information. The FBI receives a constant flow of information about possible terrorist threats and, consequently, faces an enormous challenge in deciding what information requires what type of response. Among the weaknesses we noted during our audit were the lack of criteria for initially evaluating and prioritizing incoming threat information and a lack of a protocol for when to notify higher levels of FBI management, other units and field offices, and other agencies in the law enforcement and intelligence communities. We also found that the FBI's ability to process intelligence information is hampered by its lack of an experienced, trained corps of professional intelligence analysts for both tactical and strategic threat analysis.

An ongoing OIG review is reviewing the FBI's ability to process and share intelligence information. At the FBI Director's request, the OIG is examining issues related to the FBI's handling of information and intelligence that the FBI had in its

possession prior to the September 11 attacks. Among the issues we are reviewing is how the FBI handled an electronic communication written by its Phoenix Division in July 2001 regarding Islamic extremists attending civil aviation schools in Arizona and issues raised in the May 21, 2002, letter to the FBI Director from the Minneapolis Chief Division Counsel.

In FY 2003, the OIG plans to review the FBI's dissemination of intelligence information to assess whether: (1) the flow of intelligence between the FBI and the broader federal intelligence community is satisfactory to all parties involved; (2) information and services of the FBI's Office of Law Enforcement Coordination and the Office of Intelligence are routinely accessible to federal, state, and local law enforcement agencies; (3) terrorism warnings and advisories are informative, useful, and timely; (4) impediments exist to the sharing of intelligence, warning, and advisories.

The OIG continues to examine efforts by the FBI and the INS to link information in their agency's respective automated fingerprint identification systems. A March 2000 OIG special report ("The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System") highlighted the failure of the FBI and INS to share important criminal justice information. We noted the importance of expeditiously integrating the FBI's Integrated Automated Fingerprint Identification System (IAFIS) with the INS's IDENT system to enable the two fingerprint systems to share information.

A fully integrated IDENT/IAFIS system will 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. In December 2001, the OIG issued a follow-up report (OIG Report #I-2002-003) on the status of IDENT/IAFIS integration efforts and concluded that integration has proceeded slowly and remains years away. In FY 2003, the OIG intends to conduct another follow-up review to assess the Department's progress in linking IDENT and IAFIS.

3. Information Systems Planning and Implementation: OIG audits, 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 supporting the Department's operational and administrative programs, and the vast sums of money spent on developing and deploying these systems, information systems planning and implementation continues to be a top management challenge in the Department.

   In most criminal investigations – and certainly in the aftermath of the September 11 attacks – the FBI must be able to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. Failure to capitalize on leads in its possession can delay or seriously impede an investigation. In a March 2002 review of the belated production of documents in the Oklahoma City bombing case (OKBOMB), we found that widespread failures by the FBI led to the belated disclosure of more than 1,000 documents. We traced the failures to a variety of

causes, including the FBI's cumbersome and complex document-handling procedures and its antiquated and inefficient computer systems. Although we did not find that the FBI's failures in the OKBOMB case were caused by its computer systems, we concluded that these systems cannot handle or retrieve documents in a useful, comprehensive, or efficient way.

This was not the first time the OIG had identified problems in the FBI's ability to access information from its computer systems. In a 1999 OIG review, we examined why classified intelligence information pertaining to the Department's Campaign Finance Task Force investigation was not disseminated appropriately within the FBI and the Department and, subsequently, to congressional oversight committees. The OIG found that a series of problems, including deficiencies in the use and maintenance of the FBI's computer database systems, ultimately contributed to this failure.

The problems encountered in our OKBOMB and Campaign Finance reviews shine light on historical problems in the FBI's information technology systems, including: antiquated and inefficient computer systems; inattention to information management; and inadequate quality control systems. The FBI Director has committed to moving the agency forward in these areas, and the OIG will continue to monitor the FBI's efforts to improve its information systems planning and implementation.

The OIG is finishing an audit of the FBI's management of its information technology projects. The review also examines the FBI's efforts to develop enterprise architecture and effective project management. In FY 2003, we plan to audit the FBI's Trilogy system to determine whether: (1) the FBI complied with federal regulations in selecting primary contractors for Trilogy; (2) the FBI complied with Federal Acquisition Regulations and Justice Acquisition Regulations in procuring Trilogy products; and (3) Trilogy's implementation is on schedule to meet cost, schedule, program management, and performance baselines.

Similarly, we plan to audit the Drug Enforcement Administration's (DEA) IT investment management process to ensure that the DEA is effectively managing its IT investments so that they provide the benefits for which they were designed. In addition, we plan to examine the DEA's strategic planning and performance measurement activities related to IT management.

4. Computer Systems Security: The threat to Department computers, databases, and networks from unauthorized access remains strong as hackers and others employ new technologies in their efforts to compromise Department computer networks and information. Since 1991, the Department has classified computer security as a material weakness.

The OIG regularly performs security assessments and penetration testing using advanced security system software. We have repeatedly found serious problems in the Department's computer security that could lead to the compromise of sensitive systems and data.

The OIG also conducts 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 2002, we issued reports on the effectiveness of information security control techniques for nine Department computer systems, including four classified and five sensitive but unclassified (SBU) mission-critical systems.

Our GISRA audits of both classified and SBU systems revealed vulnerabilities with management, operational, and technical controls that protect each system and the data stored on it from unauthorized use, loss, or modification. Because technical controls prevent unauthorized access to system resources by restricting, controlling, and monitoring system access, we concluded that the vulnerabilities noted in those areas were the most significant. Overall, the GISRA audits found common vulnerabilities with security policies and procedures, and password and logon management. We also reported our concerns about account integrity and systems auditing management. To varying degrees, our audits found insufficient or unenforced Department-level and component security policies and procedures.

In several areas of identified vulnerabilities, broadly stated or minimally imposed standards allowed system security managers too much latitude in establishing system settings and, consequently, systems were not fully secured. The vulnerabilities identified were more voluminous and material for the Department's classified compared to its SBU systems. We attributed this to the fact that the Department has performed penetration testing on its SBU systems, but not its classified systems.

To address the deficiencies noted, we offered a series of recommendations, including increased oversight, development of documented procedures, and establishment of proper system settings to help improve computer security. The components generally concurred with our findings and agreed to implement corrective action. If GISRA is reauthorized in FY 2003, the OIG intends to examine pursuant to GISRA additional classified and SBU systems in the Department.

GISRA, however, was not the only computer security-related work performed by the OIG in FY 2002. For example, we audited the BOPNet computer system (OIG Report #02-03) to examine security controls that protect the Federal Bureau of Prison's (BOP) computer systems and the sensitive information stored on them. The review disclosed vulnerabilities in password, login, and system auditing management. These vulnerabilities occurred because of insufficient or unenforced Department-level and BOP security policies and procedures.

We also performed computer security assessments of the FBI's headquarters information systems control environment (OIG Report #01-13) and the Justice Data Centers (OIG Report #01-10) as part of the Department's financial statement audits. The FBI audit identified weaknesses in general and application controls that could compromise the FBI's ability to ensure security over sensitive programmatic or financial data and the reliability of its financial reporting. The Justice Data Centers review found that the Data Centers have improved their internal controls and have remedied all prior year reportable conditions. The OIG will continue to perform computer security assessments as part of its annual review of the Department's financial statements.

5. Detention Space: At the time this list of top management challenges was developed, Congress had not decided whether the INS's detention responsibilities would remain in the Department or be transferred along with the INS to the Department of Homeland Security. For this reason, and because the Detention Trustee is likely to remain in the Department irrespective of the decision about the INS, we cite this issue as a top Department management challenge.

   Obtaining detention space at reasonable cost and efficiently managing that space remains a top management challenge for the Department. Both the U.S. Marshals Service (USMS) and the INS have experienced rapid growth in their use of detention space, from an average of approximately 32,000 beds in 1996 to approximately 50,000 beds in 2002. The USMS faces a shortage of detention space near federal courts, resulting in the need to transport detainees to distant facilities. The INS apprehends 1.6 million illegal aliens annually and must detain many of these aliens until their removal.

   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. Over the past several years, OIG audits of contractors for detention space have resulted in significant amounts of questioned and unsupported costs paid to the entities.

   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 in excess of $6 million due to York's understatement of its average daily population, a key figure used to determine reimbursement from the INS. If York used the daily rate determined by our audit, and if the INS, USMS, and BOP continue to use the same amount of jail days, the Department could realize annual savings of approximately $6.4 million.

   We also audited the IGA for detention space with the DeKalb County, Georgia, Sheriff's Office (OIG Report #GR-40-02-002). The audit revealed that DeKalb County included $13.4 million of operating costs that were unallowable, unallocable, or unsupported; understated its average total inmate population by more than 29 percent; and over-billed the INS $5.7 million in FY 2000. As a result, we questioned costs of $5.6 million and identified funds to better use of $7.8 million.

   A third IGA audit, regarding the Government of Guam's detention of INS and USMS detainees (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.

   There are considerable differences regarding the nature of the agreements used to obtain jail space from state and local governments. In the OIG's 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. Given the number of individuals currently detained by the Department, and the hundreds of millions of dollars involved, it is important that this matter be resolved promptly and that detention space be acquired in a coordinated, cost effective, and legal fashion.

In 2001, the Department appointed a Detention Trustee with broad responsibilities related to many of the issues discussed above. We remain concerned that the Detention Trustee may not have the authority or resources to resolve many of these long-standing issues. In FY 2003, the OIG will continue to monitor the work of the Office of the Detention Trustee to review whether detention space needs are coordinated among the components, bed space is acquired at equitable rates, and the acquired bed space is appropriate for its use.

A recent OIG audit illustrated another facet of the Department's detention challenge. The OIG examined the INS's Institutional Removal Program (IRP) (OIG Report #02-41), which is designed to identify removable aliens in federal, state, and local correctional facilities, ensure that they are not released into the community, and deport them from the United States as soon as they have completed serving their sentences. The OIG found that the INS did not always timely process IRP cases. As a result, the INS has been forced to detain criminal aliens released from state and local correctional facilities after they have served their sentence until deportation proceedings can be completed. In a sample of 151 cases of criminal aliens in INS custody reviewed by the OIG, we identified a total of $2.3 million in IRP-related detention costs, of which $1.1 million was attributable to failures in the IRP process within the INS's control. We recommended that the Department devise methods to encourage the full cooperation of state and local governments, which is essential to an effective and efficient IRP.

6. Financial Statements and Systems: In FY 2001, the Department received an unqualified opinion on its consolidated financial statement, the Department's first such "clean" opinion. Each of the Department's components also received unqualified opinions in FY 2001. We believe that the Department and the components deserve credit for removing many of the obstacles that, in the past, have prevented auditors from stating an opinion on the Department's financial statements.

   While obtaining an unqualified opinion in FY 2001 is a significant accomplishment, however, important issues continue to exist that could threaten the Department's ability to maintain these improvements.

   We reported three material weaknesses in the FY 2001 Consolidated report on Internal Controls. Within the components, we found 13 material weaknesses and 12 reportable conditions. The Department was able to overcome these issues to achieve an unqualified opinion through intense, manual efforts to prepare the financial statements and satisfy the audit requirements. However, given the accelerated reporting deadlines to OMB that begin with the FY 2002 audit, the Department has significant hurdles to overcome in order to meet the due dates because of its continued dependence on these manual efforts.

   In addition, we continue to find that component financial and other automated systems are not integrated and do not readily support the production of financial

statements. To succeed within the expedited time frames, the Department must be able to prepare financial statements more timely, and auditors must be able to test and rely upon internal control processes throughout the year. Yet, most Department components still view the preparation of financial statements as primarily a year-end exercise, even though quarterly statements are now required.

In addition to the accelerated deadlines and system implementation issues, the Department also faces issues with staff resources. We have found that several components lack adequate staff to perform many of the tasks needed to produce the financial statements. Consequently, the Department continues to rely heavily on the use of contractors to prepare the statements which, in addition to the expense, contributes to a lack of in-house knowledge and expertise.

7. Grant Management: Over the past 10 years, the Department has become a significant grant-making agency that has disbursed billions of dollars for, among other initiatives, community policing, drug treatment programs, reimbursement to states for incarcerating illegal aliens, and counterterrorism initiatives. For a Department that previously had limited experience in awarding, monitoring, and reporting on grant progress, the infusion of such significant amounts of grant money has resulted in ongoing management challenges.

The OIG continues to audit grants disbursed by the Office of Community Oriented Policing Services (COPS) to examine grantee compliance. In FY 2002, our audits of COPS grant recipients identified more than $11 million in questioned costs and more than $3 million in funds to better use.

OIG reviews of this and other Department grant programs 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, in 2002 the OIG issued an audit of the Office of Justice Programs' (OJP) administration of domestic preparedness grants to state and local agencies to enhance their ability to respond to terrorist acts (OIG Report #02-15). Through January 15, 2002, the OJP awarded grants totaling about $149 million – $101.7 million to 257 grantees for equipment and $47.1 million to 29 grantees for training. The audit found that grant funds were not awarded quickly and grantees were slow to spend available monies. As of January 15, 2002, more than half of the total funds appropriated for the grant program from FY 1998 through FY 2001 – $141 million out of $243 million – still had not been awarded. About $65 million in grant funds awarded was still unspent. In addition, we found that nearly $1 million in equipment purchased with grant funds was unavailable for use because grantees did not properly distribute the equipment, could not locate it, or had been inadequately trained on how to operate it. Although the grantees we contacted were satisfied with the overall quality of training funded by the grant program, we found that the OJP had not developed performance measures for evaluating whether the program improved grantees' capability to respond to terrorist acts.

The OIG is currently examining administrative grant activities in OJP, and between OJP and COPS, to identify functions that can be streamlined. In FY 2003, the OIG plans to audit grant management in other Department grant programs. In addition,

we also will continue to audit individual grantees to determine whether grants funds are used for their intended purpose.

8. Performance-Based Management: The Department attempts to hold itself accountable by developing performance measures that assess outcomes and results rather than inputs. Similarly, the President's management agenda for FY 2002 requires integration of budget and performance. The President's management agenda stresses performance-based management, stating that over 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 significant management challenge for the Department is ensuring, through performance-based management, that its programs are achieving their intended purposes. In a Department that has grown rapidly over the past decade, linking credible performance measures to budget development and allocation of resources has been uneven. As a regular part of OIG program audits, the OIG examines performance measures for the component or program under review and offers recommendations as to whether the reported results are supported by reliable measurement methods or systems. Additionally, as part of the annual financial statement audits, the OIG obtains information about the existence and completeness of performance measurement data.

   In recent audits of Department programs, we generally find that the performance measures in these programs are not always well developed or adequately focused on outcomes. For example, in March 2002 the OIG issued a report on the Office of International Affairs' (OIA) Role in the International Extradition of Fugitives (OIG Report #I-2002-008). The report noted that the OIA had established performance measures for treaty negotiations, but had not established measures for processing extradition requests. We also found that the OIA did not have internal policies, procedures, or standards pertaining to extradition cases that identified staff responsibilities, time frames, or priorities to guide employees or communicate management expectations.

   Further, in our May 2002 audit of the OJP's Convicted Offender DNA Sample Backlog Reduction Grant Program (OIG Report #02-20), we found that OJP had not developed performance measures that could assess whether the national backlog of DNA samples awaiting analysis was being reduced through its grant program. Without a performance measurement that specifically assesses the Program's impact on the national offender backlog, the OJP cannot measure progress in achieving its mission to reduce and eventually eliminate the convicted offender DNA sample backlog.

   In the OIG's audit of the FBI's Counterterrorism Program (OIG Report #02-38), we recommended that the FBI close the gap between planning and operations in its counterterrorism program by establishing an effective system of performance measures. Those measures should, in addition to focusing on program outcomes, identify standards for holding managers at all levels accountable for achieving the goals and objectives delineated in the FBI's strategic plans.

The General Accounting Office (GAO) reviewed the Department's FY 2000 performance report and the FY 2002 performance plan (GAO Report #01-729) to assess Department progress in achieving selected key outcomes identified as important Department mission areas. It 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 OIG also has undertaken a review focusing of the overall use of performance measures by a Department component. We are currently auditing the DEA's implementation of the Government Performance and Results Act to assess whether it has developed quantifiable goals that support its mission and whether the performance data gathered to date are valid and accurate. We also are reviewing whether the DEA has an effective system to collect, analyze, and report data related to its performance measures.

9. Human Capital: The Department continues to experience a management challenge in attracting, training, and retaining sufficient qualified employees in many of its areas of operation. Exacerbating this challenge is the fact that Department employees are leaving to take higher-paying positions in other government agencies (such as the new Transportation Security Agency) and in the private sector. We also are concerned that the Department of Homeland Security, possibly offering higher salaries than Department employees currently earn, will siphon off trained employees in areas such as law enforcement, intelligence analysis, information technology, and linguistics.

   Throughout the Department, agencies have difficulty attracting and retaining high quality information technology specialists who are knowledgeable about the latest hardware and software. Employees with specialized skills in this area are in high demand in the marketplace, and the Department has had some difficulty competing with private sector companies and other government agencies who can offer greater monetary rewards. Without greater recruitment and retention of highly qualified information technology employees, the government runs the risk of falling further behind in several of the challenges noted above, such as Information Systems Planning and Implementation, Computer Systems Security, and Financial Statements and Systems.

   In other areas, Department components face problems in expeditiously hiring qualified specialists. For example, the FBI must hire and train additional intelligence analysts and investigators to assist in meeting the Bureau's new counterterrorism responsibilities. In addition, because of the lack of investigators experienced in working counterterrorism cases, the FBI is rehiring recently retired FBI agents for temporary assignment. Furthermore, the FBI is seeking to build a corps of experienced translators to address a lack of expertise in certain languages and focus on reducing the backlog of translation requests.

   The Department must have the capabilities, resources, and facilities to adequately train the influx of entry-level personnel. For example, training staff at the Federal Law Enforcement Training Center in Glynco, Georgia, is working six days a week in an effort to train the high volume of new employees.

We also believe the Department must focus attention and training resources on new managers who will be needed to replace the significant number of senior Department employees nearing retirement age.

10. Department of Justice Reorganizations: Managing employees through ongoing and impending reorganizations presents a critical management challenge for the Department. While much of the ongoing reorganizations are designed to increase the Department's ability to combat terrorism, some changes are designed to correct long-standing organizational problems. The challenge for Department managers is not only to ensure that the reorganization activities accomplish their intended purposes, but also to see that the Department's interconnected programs and functions are not affected adversely by the changes during what may be prolonged transition periods.

The largest impending reorganization is the creation of the Department of Homeland Security and its absorption of all or part of the INS. Congress and the Administration currently are grappling with the mechanics of how to merge 22 departments and agencies with 170,000 employees into a single agency with a wide-ranging mission. While no definitive decisions have been made as of the date of this document, it is clear that creation of the Department of Homeland Security will have a significant impact on the Justice Department. The Department will be challenged to ensure that the vital missions of the INS are not impeded during the transition period. GAO echoed similar concerns in a recent report (GAO Report #02-957T), stressing the challenges during the transition period relating to communication systems, information technology systems, human capital systems, and the physical location of people and other assets. Similar challenges will result if the Bureau of Alcohol, Tobacco and Firearms is transferred from the Department of the Treasury into the Department of Justice.

The FBI continues its internal reorganization to more effectively respond to its new priority to detect and deter acts of terrorism against United States interests. In December 2001, the FBI Director announced a restructuring plan for FBI Headquarters that he described as the first step in a "phased process of reorganizing assets, modernizing and integrating new technology, and consolidating functions." Additional restructuring measures have been implemented, and the FBI is seeking to reengineer structures and processes throughout its organization.

To aid in these restructuring efforts, the OIG is examining various aspects of the FBI's operations and programs. For example, the OIG's comprehensive review of the Department's performance in preventing, detecting, and investigating the espionage activities of former FBI agent Robert Hanssen will offer recommendations for programmatic and structural reorganization in the FBI's counterintelligence programs.

Additionally, OJP is reorganizing in an attempt to improve its grant operations. As mentioned previously, the OIG is reviewing OJP to assess potential duplication in its grant management and oversight process, both within OJP and between COPS and OJP, in an effort to identify opportunities to create efficiencies and streamline operations.

These restructuring efforts throughout the Department present significant challenges to managers and employees. Importantly, the Department must ensure that its critical missions are effectively met while the reorganizations are taking place – reorganizations that, hopefully, will leave the Department better prepared to address these and other top management challenges in the future. The OIG intends to assist in this effort by reviewing the proposed changes and offering recommendations for improvement.

Top Management Challenges in the Immigration and Naturalization Service: 2002

The Office of the Inspector General (OIG) annually issues a list of top management challenges facing the Department of Justice (Department). This year, in light of pending legislation to transfer the Immigration and Naturalization Service (INS) from the Department to the proposed Department of Homeland Security, we have created separate lists of top management challenges in the Department and in the INS. The following list of top INS challenges is intended to assist the Department of Homeland Security in successfully assimilating the INS, or the Department in managing the INS should it not be transferred.

1. Border Security: The INS's ability to screen individuals seeking to enter the United States remains a key element of homeland security and the INS faces many challenges in this area. For example, we have found that the INS lacks adequate staff and equipment to guard northern land and water borders. The INS's strategy to control the southwest border, while much further deployed than its northern border strategy, needs additional infrastructure support, such as physical facilities and technology, and may take many years to fully implement. When the INS apprehends aliens, it does not have the capability to effectively identify those who are wanted by law enforcement or who may pose a threat to the United States. Also, the INS's capacity to detain aliens prior to their removal is not sufficient.

   The OIG has examined many facets of the INS's efforts to control U.S. borders. For example, in two reviews of the INS's Border Patrol deployment and operation along the northern border (OIG Report #I-2000-004, and follow-up report OIG Report #I-2002-004), we found that INS staffing and resource shortages along the northern border continue to be a critical impediment to effective control of illegal immigration. With respect to the southwest border, the General Accounting Office (GAO) reached similar conclusions. The GAO's report, "INS' Southwest Border Strategy: Resource and Impact Issues Remain After Seven Years" (GAO-01-842, August 2, 2001), estimated that it may take the INS up to another decade to fully implement its strategy.

   The OIG also has examined other methods of entry into the United States that are important to the border security challenge. "The Potential for Fraud and INS's Efforts to Reduce the Risks of the Visa Waiver Pilot Program" (OIG Report #I-99-10) and our follow-up report (OIG Report #I-2002-002) examined vulnerabilities in the Visa Waiver Program and found that INS inspectors lacked access to full information regarding missing and stolen passports. We also found serious security concerns in the Transit Without Visa Program. In two other reports, "Transit Without Visa (TWOV) Program Inspection" (OIG Report #I-92-27 and our follow-up report, "Improving the Security of the Transit Without Visa Program" (OIG Report #I-2002-005), we determined that airlines failed to supervise passengers at United States airports in the Transit Without Visa program, and that the INS could not verify that such passengers actually left the country. In another examination of

port-of-entry (POE) operations, "Immigration and Naturalization Service Deferred Inspections at Airports" (OIG Report #01-29), we found that 11 percent of entering aliens who were allowed to enter the country upon condition that they agree to appear at an INS office to complete their deferred inspection failed to do so and that the INS's subsequent pursuit of such persons was incomplete and ineffective.

The challenge of securing the nation's borders extends to how the INS processes aliens after they are apprehended. A critical part of this challenge is the integration of the INS's automated biometric fingerprint identification system (IDENT) and the Federal Bureau of Investigation's (FBI's) integrated automated fingerprint identification system (IAFIS). Our most recent examination of the integration efforts, "Status of IDENT/IAFIS Integration" (OIG Report #I-2002-003), followed up on two prior reviews, "Review of the Immigration and Naturalization Service's Automated Biometric Identification System (IDENT)" (OIG Report #I-1998-010), and "The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System" (March 2000). In these reports, we recommended that the Department continue to seek linkage of the FBI and INS biometric identification systems and use IDENT while integration of IDENT and IAFIS is proceeding. We also recommended, as an interim measure, adding fingerprint records to the IDENT lookout database for aliens wanted in connection with crimes.

The INS took this step, which according to the INS has resulted in the apprehension of thousands of aliens who had criminal warrants outstanding. We believe that full integration of IDENT and IAFIS will improve the ability of the INS to identify and detain aliens who are wanted for crimes or who may pose a threat to the nation's security. In recognition of the critical importance of integration of these systems, we are initiating another follow-up review in fiscal year (FY) 2003 to assess the progress of the integration efforts.

2. Enforcement and Removal: The INS's ability to find and remove the estimated 7-12 million illegal aliens in the United States is an enormous challenge. Currently, there are many gaps in the INS's ability to identify aliens who are ineligible to remain in this country. The INS's systems for tracking when aliens enter and leave the United States clearly are inadequate. Improving these systems will require persistent efforts and substantial investments of resources. This will be a daunting challenge to an agency that does not have a history of success with large technology initiatives. Moreover, even if the INS succeeds in creating effective tracking systems, it must implement an effective program for removing aliens after they have been identified.

In 1997, the OIG examined the INS's efforts to identify aliens who overstayed the limits prescribed by their visas, a condition that the INS has estimated involves approximately 40-50 percent of the illegal alien population in the United States. Recently, we conducted a follow-up review, "INS Efforts to Improve the Control of Nonimmigrant Overstays" (OIG Report #I-2002-006), which found that the INS has made little progress in effectively dealing with nonimmigrant overstays or in addressing the recommendations we made in 1997. The INS does not have reliable data on overstays or a reliable system to track overstays, and it acknowledges that any effective enforcement strategy depends on the future establishment of a comprehensive entry/exit system.

The GAO reached similar conclusions in its report, "Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy" (GAO-02-861T, June 19, 2002), which also examined the INS's efforts to develop an interior enforcement strategy. In 1999, the INS issued its Interior Enforcement Strategy to focus resources on areas that would have the greatest impact on reducing the size and annual growth of the illegal resident population. The GAO concluded that for the INS's interior enforcement strategy to be effective, the INS needs better data to determine staff needs, reliable information technology systems, clear and consistent guidelines and procedures for INS field staff, effective coordination within the INS and with other agencies, and performance measures that help the INS assess program results.

The OIG recently assessed the INS's Institutional Removal Program (IRP), an INS program designed to identify deportable criminal aliens incarcerated in federal, state, and local correctional facilities and remove them from the United States upon completion of their sentence. Our review, "Immigration and Naturalization Service's Institutional Removal Program" (OIG Report #02-41), determined that the INS has not managed the IRP process effectively. We found that the INS has yet to determine the nationwide population of foreign-born inmates, particularly at the county level. Without this information, the INS cannot properly quantify the resources it needs to fully identify and process all deportable inmates. In addition, at the county level we found that IRP interviews of foreign-born inmates to determine deportability were minimal to non-existent. As a result, many potentially deportable foreign-born inmates passed through county jails virtually undetected. We found instances where inmates not identified by the INS as potentially deportable went on to commit additional crimes, including cocaine trafficking, child molestation, and aggravated assault, after being released into the community.

Further, our review found that the INS did not always timely process IRP cases. As a result, it has been forced to detain in INS custody criminal aliens released from state and local correctional facilities – after they have served their sentence – until deportation proceedings can be completed. In the OIG's sample of 151 cases of criminal aliens in INS custody, we identified a total of $2.3 million in IRP-related detention costs, of which $1.1 million was attributable to failures in the IRP process within the INS's control. We estimated that the total cost of holding IRP inmates in INS detention could run as high as $200 million annually.

In another OIG report, "The INS Escort of Criminal Aliens" (OIG Report #I-2001-005), we reviewed the INS's implementation of its policies for escorting criminal aliens who are being removed from the United States. We found that the INS placed the traveling public at potential risk because it did not consistently follow its own escort policy. Some INS supervisory field officials disregarded provisions of the INS escort policy, resulting in the transportation of violent aliens on commercial airlines without escorts. In addition, the INS failed to identify some dangerous aliens during the routine pre-removal alien file review process. We also found that INS field officials often failed to provide the required ratio of escorts to dangerous aliens, and the INS did not always provide escorts during the final segment of multi-flight removal trips.

3. Entry/Exit and Student Tracking Systems: According to INS estimates, in FY 2001 the INS inspected over 35 million nonimmigrants at air POEs, approximately 1 million at sea POEs, and approximately 195 million at land POEs. However, because of inadequate tracking systems, the INS does not know whether these nonimmigrants have overstayed or otherwise violated the conditions of their admittance to the United States.

As we discussed above, a reliable and efficient system of tracking nonimmigrant entries and exits is essential to the INS's enforcement and removal responsibilities. We evaluated the INS's efforts at developing an effective entry/exit system, which was mandated by Congress in both the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 and the Immigration and Naturalization Service Data Management Improvement Act of 2000. In our audit report entitled "The Immigration and Naturalization Service's Automated I-94 System" (OIG Report #01-18), we determined that the INS's I-94 entry/exit system was a failure. At the time of our audit in 2000, the system operated at only four air POEs with the participation of only two airlines. The system had not been deployed at any land or sea POEs. We found that the INS's efforts to track the implementation of the system were inadequate. Despite having spent $31.2 million on the system from FY 1996 to FY 2000, the INS did not have clear evidence that the system would meet its intended goals, and estimated that an additional $57 million would be needed for FY 2001 through FY 2005 to complete the system.

After the terrorist attacks of September 11, 2001, the effectiveness of monitoring nonimmigrant visitors came under additional scrutiny. The USA Patriot Act, enacted on October 26, 2001, requires that an integrated entry/exit control system be implemented with all deliberate speed and that an Integrated Entry and Exit System Task Force be established to accomplish this task. The exit/entry control system would collect and match arrival and departure records for every alien and provide reports on overstays. On February 18, 2002, the INS officially terminated the Automated I-94 System project. The INS created an Entry-Exit Program Office to explore alternative technical solutions and processes for the entry/exit control system. The INS faces enormous challenges to implement this system in a timely, complete, and cost-effective manner.

In addition to its difficulties in tracking nonimmigrants generally, the INS has been unable to monitor effectively certain categories of nonimmigrants, such as students. In a report issued in May 2002, the OIG examined the INS's efforts to monitor the approximately 500,000 aliens who annually enter the United States under student visas. In our report, we first examined the INS's processing of two September 11 terrorists' applications for a change of status from visitor to student, and the reasons that the notification forms approving the change of status were mailed to a Florida flight school six months after the terrorists had died while perpetrating the September 11 attacks. We found the INS's adjudication and notification process to be untimely and significantly flawed. Even after adjudication, the requisite forms were delayed for months before being mailed to the flight school, which we attributed to the INS's failure to monitor a contractor's performance adequately.

We then examined the INS's paper-based system for monitoring and tracking foreign students in the United States, and found that it was antiquated and inadequate. We concluded that the INS's new Internet-based student tracking

system, the Student and Exchange Visitor Information System (SEVIS), will be a significant advance and will help address many of the failings of the current system. But SEVIS alone will not solve the problems of the INS's tracking of foreign students. For example, the INS must review and properly recertify thousands of schools that currently are certified to enroll foreign students, must ensure that its employees and the schools timely and accurately enter information into SEVIS, and must ensure that the information from SEVIS is analyzed and used adequately. We concluded that the INS was unlikely to meet the January 2003 deadline for full implementation of SEVIS. At the end of the report, we provided 24 recommendations to help address deficiencies in INS practices and procedures that we found in our review and in the INS's proposed implementation of SEVIS.

4. Applications Backlog: The INS handles approximately 50 types of applications for immigration services, including applications for employment authorization, change of status to permanent residence, asylum, and citizenship. Processing the millions of applications in a timely and consistent fashion has been a longstanding challenge for the INS.

   This challenge was examined in an OIG special report, "An Investigation of the Immigration and Naturalization Service's Citizenship USA Initiative" (July 31, 2000). At the time the INS initiated Citizenship USA, it projected that an applicant for citizenship would have to wait three years for agency action. The report found that during the time in which the INS focused attention on this poorly planned effort at reducing the citizenship backlog, the backlog of applications for other immigration benefits grew substantially.

   The GAO reported similar problems in its report, "Immigration Benefits: Several Factors Impede Timeliness of Application Processing" (GAO-01-488, May 4, 2001). The GAO also found that while the backlog for citizenship had decreased, the backlog for other applications had increased. The GAO concluded that the INS experienced significant problems managing its application workload, despite years of increasing budgets and staff. It found that the INS did not maximize the deployment of staff to process applications in a timely fashion because it lacks a systematically developed staff resource allocation model. The GAO also found that the INS did not know how long it took to process applications because its automated systems contained unreliable data and its districts did not have automated systems for tracking many types of applications.

   As noted above, in the OIG report on the INS's contacts with two September 11 terrorists, the OIG found significant backlogs in the processing of I-539 applications for change of status. Mohamed Atta and Marwan Alshehhi had applied to the INS Texas Service Center to change their immigration status from tourist to student in the year before the attacks on the World Trade Center. Both Atta's and Alshehhi's I-539 applications took 10 months for adjudication. This type of delay in adjudicating I-539 applications was typical because I-539s had been a low priority for the INS, resulting in substantial processing backlogs. The average processing times for I-539s have remained consistently high since at least 1998, ranging from 129 to 200 days. For FY 2002, the INS made processing I-539s a priority and set the target processing time at five months. However, we question whether the INS can meet its new processing deadlines unless sufficient resources are consistently devoted to the effort.

Our annual audits of the INS's financial statement continued to find evidence of significant deficiencies in the INS's ability to handle immigration applications and monitor its productivity and progress in addressing backlogs. During FY 2000, INS management had to expend tremendous efforts in conducting a wall-to-wall physical inventory of applications to determine how many it had pending and how many it had processed to completion at the end of the fiscal year. The INS manually counted approximately 2 million applications – first, in several preliminary counts and then a final end-of-year count that shut down production at several sites for more than a week and delayed application processing. We concluded that the INS needs an automated system for recording the status of pending applications and for better managing its backlogs.

5. Financial Statements and Systems: The INS continues to expend tremendous manual efforts and costs in preparing its financial statements and supporting financial statement audits. This is due primarily to the lack of automated systems that readily support ongoing accounting operations, financial statement preparation, and the audit process. For instance, although the INS obtained an unqualified opinion in its FY 2001 financial statement audit, the achievement was tenuous and does not reflect a healthy financial accounting system. The INS has been in the process of replacing its core financial system for over five years. Among other problems, it continues to use a significant feeder system that does not comply with federal financial systems criteria. The INS still processes the majority of its transactions through the Financial Accounting and Control System (FACS), its legacy accounting system, which now serves as a feeder system to its new Federal Financial Management System. However, FACS has many inherent control weaknesses due to its age and design.

   While the INS has made progress in its financial statements, it still needs to make further improvement in areas such as identification of deferred revenue, financial management systems controls, general electronic data processing controls, verification of intra-governmental transactions, documentation of accrual estimation, and controls over key performance measures. In our FY 2001 financial statement audit, we identified the first three items as material weaknesses.

   In addition, as discussed above, the INS has a critical problem determining how many immigration benefits applications it has processed and, thus, its calculation of earned revenue and management of its examinations fee account. So far, it has been able to meet the end-of-year requirement only by a manual count and shutdown of some processing facilities.

   None of these deficiencies is subject to easy solution. We believe the INS's challenge will increase as the government accelerates the completion dates for the financial statements and shifts to quarterly reporting.

6. Information Technology Planning and Implementation: The INS's implementation of technology projects has been a long-term management challenge. The Department recognized the challenge when it identified INS information technology as a material weakness in 1998. In an OIG report issued that year, "Immigration and Naturalization Service Management of Automation Programs" (OIG Report #98-09), we concluded that the INS had not adequately managed its automation

programs. The report warned that the INS was at risk that completed projects would not meet their intended goals, completion of the automation programs would be significantly delayed, and unnecessary costs could occur.

A year later, the OIG issued a follow-up report (OIG Report #99-19) that found continuing problems with INS information technology planning and management. Specifically, we reported that project costs continued to increase without established baselines against which actual costs incurred could be compared and without justifications for the increases. We found that INS managers did not adequately monitor planned project tasks to ensure timely completion and that monthly progress reviews were incomplete, unclear, and untimely. Further, the INS had not developed comprehensive performance measures to ensure that completed projects, once deployed, would meet intended goals. Finally, the report noted serious deficiencies in the INS's compliance with its system development life-cycle process. As a result, the INS had no assurance that systems would meet performance and functional requirements.

We continue to have concerns about the INS's management of its information technology programs. For example, we performed an audit entitled, "The Immigration and Naturalization Service's System Data Pertaining to Secondary Inspections at Selected Preclearance Airports" (OIG Report #01-11), to assess the technology available to INS inspectors at secondary inspection sites. INS inspectors at airports rely on inspection data maintained in the Treasury Enforcement Communications System (TECS). Other federal entities and INS programs rely on TECS data in their law enforcement operations. Our audit found variations in the reliability of INS data entry practices. For example, at one site INS inspectors entered the required referral designation and secondary inspection results in TECS for only 3 percent of the approximately 51,000 secondary inspections performed during the audit period. The lack of reliable data jeopardizes other INS law enforcement efforts, including the INS's ability to provide assistance to other federal entities.

We have discussed above other OIG reports that described vulnerabilities in INS information technology programs, including the status of IDENT/IAFIS integration (OIG Report #I-2002-003), the INS's contacts with two September 11 terrorists, and the Automated I-94 System (OIG Report #01-18). Significant issues that we continue to find in INS information technology projects demonstrate the need for a major dedication of resources and oversight to this critical management challenge.

7. Computer Systems Security: The INS depends on computers to process millions of immigration transactions, to record its dealings with millions of aliens, and to conduct its office automation activities. Protecting these systems from unauthorized access, manipulation, or destruction is vital to the INS's operations. The OIG has examined the security of INS computer systems pursuant to the Government Information Security Reform Act and performed additional testing while conducting the annual financial statement audit. Computer systems security remains a critical challenge that the INS, like other government agencies, must address on a continuing basis.

For example, we reviewed the "backbone" INS system that provides office automation tools to more than 30,000 INS employees and 10,000 contractor

employees worldwide. We also reviewed the automated system that supports INS records management functions. Our review of the management, operational, and technical controls that protect the INS's core network found medium to high vulnerabilities for unauthorized use, loss, or modification in 9 of the 17 control areas that were tested, with 2 reported as high vulnerabilities. We noted a need for improvements or corrective actions with respect to the security evaluation and risk assessment; interconnections with other networks; intrusion detection systems; tape management; and access, password, and encryption practices.

Our review of the INS records management system found deficiencies in 12 of the 17 control areas tested. We found inadequate security evaluation and risk assessment practices, and recommended that these deficiencies may warrant rescinding the system's certification and accreditation in favor of an interim approval to operate until corrective action is completed. We also recommended corrective action regarding system contingency planning and clarification of the responses required in the event of a service disruption. In all, the OIG made 18 recommendations to the INS for corrective actions regarding the 2 systems.

8. Detention Space Management: Obtaining and efficiently managing detention space for INS detainees is a critical management challenge. In 2000, the INS apprehended 1.8 million aliens, many of whom are held temporarily before being voluntarily returned to Mexico. Statutory changes enacted by Congress in 1996, which require the INS to detain certain classifications of aliens until their removal, have increased the number of aliens who must be detained for more than short periods. For example, the number of aliens detained for formal removal or other immigration proceedings has grown, from 72,154 in 1994 to 188,547 during 2001.

To obtain additional detention space, the INS has relied on outside contractors (including state and local governments and for-profit entities) to house INS detainees. For example, the Department's Detention Trustee has estimated that almost 70 percent of the Department's detainees (which also includes those held by the U.S. Marshals Service) are held in state, local, or contractor-operated facilities. OIG audits of contractors for detention space have resulted in significant dollar findings, generally for unsupported costs. 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 in excess of $6 million due to York's understatement of its average daily population, a key figure used to determine reimbursement from the INS. Further, our audit estimated that the Department could save an additional $6.4 million if the rate was lowered to comport with the audited figures and the Department used the same number of jail days during the following year.

Other OIG audits identified significant overpayments that the INS and the Department made under other IGAs. For example, our audit of an IGA with the DeKalb County, Georgia, Sheriff's Office (OIG Report GR-40-02-002) found that the INS was over-billed by $5.7 million in FY 2001. DeKalb County's understatement of the average total inmate population by more than 29 percent resulted in this over-billing. An audit of 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.

The INS has not yet acted to recover these overpayments. At York, the INS has not reduced its payments to conform to the audited rates. Moreover, in our view, the INS and the Department have not yet settled on a procurement process to obtain detention space in a manner that meets existing procurement regulations.

Juvenile illegal aliens present special detention challenges for the INS. In our report entitled "Unaccompanied Juveniles in INS Custody" (OIG Report #I-2001-009), we found that the INS did not always segregate non-delinquent juveniles from delinquent juveniles and that the INS was not always able to promptly place juveniles in a detention facility or shelter due to a shortage of appropriate facilities. In another report, entitled "Juvenile Repatriation Practices at Border Patrol Sectors on the Southwest Border" (OIG Report #I-2001-010), we found that unaccompanied Mexican juveniles sometimes were detained over a weekend at Border Patrol stations in holding cells built for temporary confinement.

9. Organizational Structure: For several years, the INS has considered various reorganization plans. Congress also has proposed restructuring the INS in an effort to address many of its management and programmatic challenges. Recently, the Administration and Congress have proposed to transfer all or part of the INS's functions to the Department of Homeland Security.

   A major redesign of the INS's structure and location could affect, at least in the short term, productivity, quality assurance, employee morale, and the quality of the services provided to the public. The challenge for the INS, in whichever organization it is located, will be to ensure that the reorganization accomplishes its intended purposes and that the agency's essential services and functions continue without interruption during the transition. Whichever way the INS is reorganized, fundamental corrections in its business practices, policies, and systems are necessary. We believe it is imperative that any reorganization or transfer of the INS not substitute or delay such corrective actions.

10. Human Capital: To fulfill its mission, the INS must have sufficient trained staff and supervisors. This has been a critical challenge for the INS. For example, the INS has had difficulty filling Border Patrol agent positions because of high attrition rates among agents, delays in recruitment, and limitations in training facilities. These problems have been exacerbated by the recruiting successes of the Transportation Security Administration's (TSA) Sky Marshal program and TSA's ability to offer higher pay than the INS for many of its positions.

    Like other parts of the Department, the INS also suffers from difficulties in attracting and retaining employees in information technology and computer security positions. Moreover, the INS's average workforce is less experienced as a result of significant attrition among experienced employees. The INS also is heavily reliant upon contractor support for many functions associated with its information systems, records management, immigration service processing, detention services, guard services, and other functions.

In our examinations of the INS's programs and operations, we frequently have encountered inconsistent and nonconforming business practices and transactions. Field offices use different forms, criteria, and often appear ignorant of agency policy and guidance. In particular, we have found both inconsistent practices among field offices and fundamental deficiencies in common business transactions. These findings suggest that, among other measures, the INS needs to improve its training so that employees perform their duties correctly and in accordance with standard INS policy.

While the INS is not unique in experiencing a human capital challenge, correction of the many difficult systemic problems that we have described in this list of top management challenges requires an adequately trained and qualified INS workforce. To the extent INS does not address human capital challenges, its ability to solve its other management challenges will be undermined.

This page is intentionally blank.