APPENDIX B

DEPARTMENTAL MANAGEMENT CHALLENGES AND WEAKNESSES

Each year the Department identifies existing and potential management challenges, weaknesses, and areas in need of improvement. Two primary sources used to identify these issues are the Federal Manager's Financial Integrity Act (FMFIA) reporting process, and the DOJ *Office of the Inspector General (OIG) Top Ten Management Challenges*.

As required under the FMFIA, the Department reports to the President all weaknesses in internal controls that the Attorney General deems material, along with detailed corrective action plans. Additionally, in December of each year, the Inspector General issues a list of management challenges. Although the list is created from an auditor's perspective, there are often areas of overlap between the *OIG's Top Ten Management Challenges* and issues identified by the Attorney General.

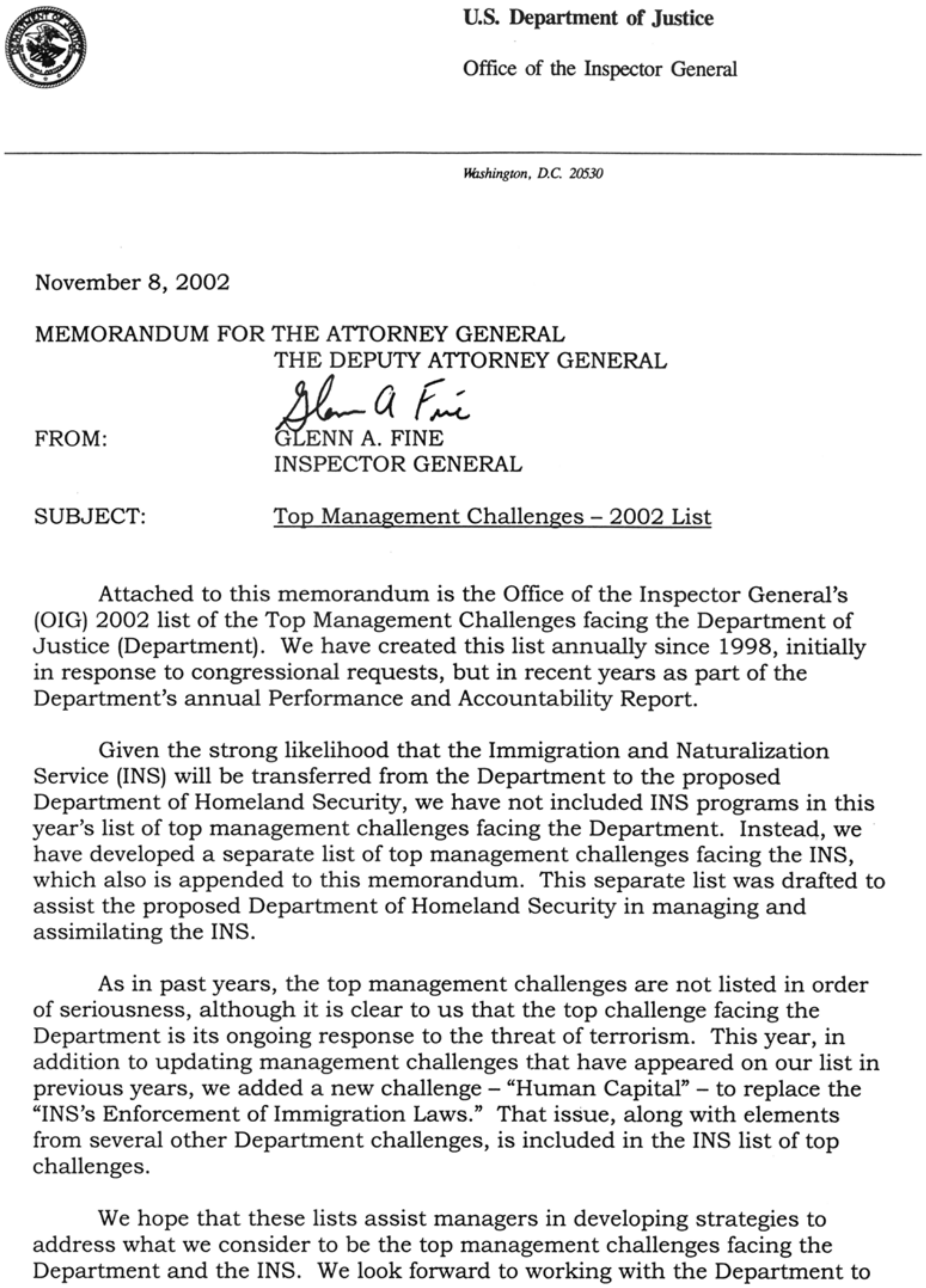
In December 2002, the OIG issued two Top Ten Management Challenge memorandums. The first identified existing or potential issues facing the Department. The second addressed issues specific to the Immigration and Naturalization Service (INS). However, due to the transfer of INS to the Department of Homeland Security in FY 2003, only issues within the OIG's first memorandum will be addressed within this Appendix.

Since many of the FMFIA weaknesses are duplicated under the *OIG's Top Ten Management Challenges*, only those not covered by the OIG are included in this Appendix; they are, Prison Crowding, Property and Equipment [FBI], and Management of IT [FBI]. The full FMFIA report is included within Appendix C of the Department's *FY 2002 Performance and Accountability Report,* available at: http://www.usdoj.gov/ag/annualreports/ar2002/index.html.

The following table summarizes the management challenges and identified weaknesses for the Department.

Identified Management Issues	FMFIA Material Weaknesses/ Non-conformances	OIG Top Ten Management Challenge Issue #	Location of Management Issue Discussion (within this Document)
Counterterrorism	No	1	Appendix B
Sharing of Intelligence and Law Enforcement Information	No	2	Appendix B
Information Systems Planning and Implementation	No	3	SG 8, Appendix B
Computer Security Implementation	Yes	4	Appendix B
Detention Space and Infrastructure	Yes	5	Appendix B
Financial Statement and Systems	Yes	6	SG 8, PMA Section, Appendix B
Grants Management [OJP, COPS]	No	7	SG 8, Appendix B
Performance-Based Management	No	8	Appendix B
Human Capital	No	9	SG 8, PMA Section, Appendix B
DOJ Reorganizations [FBI, OJP, INS]	No	10	SG 8, Appendix B
Prison Crowding	Yes	---	SG 6 Appendix B
Property and Equipment [FBI]	Yes	---	Appendix B
Management of IT [FBI]	Yes	---	Appendix B

OIG LETTER TO THE ATTORNEY GENRAL LISTING THE TOP TEN MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF JUSTICE



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

Glenn A Fine

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.

RESPONSES TO THE OFFICE OF INSPECTOR GENERAL’S TOP TEN MANAGEMENT CHALLENGES

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	Date of Submission:	Component:	Original Target for Completion:	Current Target for Completion:
COUNTERTERRORISM	11/12/2002	FBI	11/30/2002	On-going

Issue and Description:

- COMPREHENSIVE WRITTEN ASSESSMENT OF THE RISK OF A TERRORIST THREAT- ESTABLISHING PRIORITIES, ALLOCATING RESOURCES, ENHANCING ABILITY TO RESPOND

OIG recently audited the FBI’s management of aspects of its counterterrorism program from 1995 through April 2002. OIG found that 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. OIG found that the assessment would have been useful to define the nature, likelihood, and severity of the threat and identify intelligence gaps and determine appropriate levels of resources to effectively combat terrorism. Recently FBI developed a multi-layered strategic planning system, but had not established priorities adequately or allocated resources effectively to the counterterrorism program. The planning system acknowledged a general terrorist threat to the Nation, but did not perform and incorporate into the planning system a comprehensive assessment of the threat of terrorist attacks on U.S. soil. The planning system identified numerous vulnerabilities and weaknesses, but FBI did not make the fundamental changes necessary to correct deficiencies.

What we did in FY 2002 / What are the Current Approaches: The FBI concurs with the recommendation to prepare a comprehensive national-level assessment of the terrorist threat to the U.S. homeland. The terms of reference for the assessment were drafted on August 9, 2002. A draft for coordination was completed by September 30, 2002, and publication is expected by November 30, 2002.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
Publish comprehensive national-level threat assessment of the terrorist threat to the United States.	11/30/2002	11/30/2002	
Utilize threat assessment to establish CTD program priorities, allocate resources and enhance ability to respond to threats of terrorism.	On-going	On-going	

How We Will Know It Is Fixed: The Threat Assessment will be completed and published.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **COUNTERTERRORISM**	**Date of Submission:** 11/12/2002	**Component:** FBI	**Original Target for Completion:** N/A	**Current Target for Completion:** 9/23/03

Issue and Description:

- TIMEFRAME AND PROCESS FOR BUILDING A CORPS OF INTELLIGENCE ANALYSTS

OIG audit made 14 recommendations to help improve management of FBI's counterterrorism program, including that 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.

What we did in FY 2002 / What are the Current Approaches: The FBI concurs that its intelligence capabilities need to be continually updated and improved. Our goal is to have a robust analytical capability by the end of FY 2003. The FBI's training program has been modified to place more emphasis on basic analytical training. The basic analysts' course has been expanded from five weeks to six weeks, with more emphasis on analytical tradecraft. CIA instructors will teach the initial sessions, after which FBI instructors will take over. The first session of the new course will begin on February 22, 2003. In addition, CIA will hold a four-day course on managing analysis, which is mandatory for all FBI managers in the Counterterrorism Division (CTD) Analysis Branch. This course will begin during the first week in December, 2002.

The FBI's Terrorism Reports and Requirements Section was recently formed. The Section is responsible for managing the collection and dissemination of raw intelligence information (not analysis) relating to terrorism issues. A senior CIA Collection Management Officer is in place (since June 10, 2002) to design the section, implement procedures, hire and train Intelligence Operations Specialist (IOS) reports officers, disseminate the information, provide feedback to field offices and Legats, and serve as a focal point for the Intelligence, Policy, and Law Enforcement Communities regarding FBI raw intelligence reporting. There are currently Reports Officers working in the section, and additional Officers are currently in the background investigation phase of hiring. Also, CIA has agreed to send an additional Collection Management Officer to help build the section. A professional training program will be designed and implemented for all Reports Officers.

The Office of Intelligence, created in August 2002, is responsible for establishing an analytical career service for the FBI. A CIA officer from the Directorate of Intelligence will oversee this effort. This officer reported for duty on August 26, 2002 and will conduct the recommended review. In addition, a working group has been formed to examine how the FBI can make better use of its tactical and strategic analysts.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Hire and train professional cadre of analysts and reports officers	01/01/2003	9/30/2003	

How We Will Know It Is Fixed: Building a professional analytical cadre will take some time and this should be considered a work in progress. The FBI is committed to building a corps of professional, trained , and experienced Intelligence Analysts and Reports Officers.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **COUNTERTERRORISM**	**Date of Submission:**	**Component:** Department	**Original Target for Completion:**	**Current Target for Completion:** On-going

Issue and Description:

- PLAN FOR THE PROTECTION OF CRITICAL PHYSICAL ASSETS

OIG audit (#02-01) found 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.

What we did in FY 2002 / What are the Current Approaches:

The issue of the Department's performance of its responsibilities under Presidential Decision Directive (PDD) 63 to protect its critical infrastructure (which includes critical physical assets) is currently under OIG review. As set forth in a September 27, 2002 memorandum from then Acting Assistant Attorney General for Administration Janis Sposato to Inspector General Glenn Fine, and other related memoranda, it is the position of the Justice Management Division (JMD) that the current Departmental Continuity of Operations Plan and other measures, including submissions relating to protection of cyber infrastructure, satisfy both the requirements of PDD-63 and pertinent OIG recommendations.

As part of an August 8, 2001 audit of the Department's critical infrastructure protection plan, the OIG recommended that the Department, conduct a vulnerability study of such assets, and develop remedial and funding plans to address vulnerabilities in order to insure that its minimum essential functions can be performed in an emergency. The Director, Security and Emergency Planning Staff, using the appropriate criteria, had determined that the Department and Federal Bureau of Investigation Headquarters were the only two departmental buildings the unavailability of which would make it impossible to carry out the Department's minimum essential functions. Thus a relocation facility was constructed and a Continuity of Operations (COOP) plan devised to allow critical systems and personnel from these two buildings to operate were either unavailable. The development of the relocation facility and supporting COOP plan, together with earlier U.S. Marshals Service and General Services Administration assessments of departmental physical infrastructure vulnerabilities, have fulfilled the OIG critical physical infrastructure concerns. Thus, subject to continued discussions between OIG and JMD, it is JMD's position that the OIG determination that the Department has not planned adequately to protect its critical infrastructure is incorrect.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Negotiations between OIG and JMD on this issue are ongoing.		FY 2003	

How We Will Know It Is Fixed: When resolution between OIG and JMD on this matter is reached.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	Date of Submission:	Component:	Original Target for Completion:	Current Target for Completion:
COUNTERTERRORISM	11/13/2002	OJP	N/A	Completed 07/18/2002

Issue and Description:

- SLOW AWARDING OF GRANT FUNDS AND SPENDING OF AVAILABLE MONIES-ODP

Throughout FY 2002, IG conducted an audit of the domestic preparedness grants given to state/local entities for training and equipment to respond to acts of terrorism; and if those dollars were being used for their intended purpose (#02-15). OIG found that grant funds were not awarded quickly, and grantees were slow to spend available monies. Also, nearly $1 million in equipment purchased with grant funds were 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.

What we did in FY 2002 / What are the Current Approaches:

During FY 2002, ODP received, reviewed and processed the applications for FY 2000 and 2001 funds.

ODP also developed and delivered State Assistance Plans (SAP) that were tailored to the needs identified by each state in their Statewide Strategy. The SAP allocates and describes specific grant funds, training resources, exercise support, and technical assistance available to the state. ODP program managers conducted on-site visits with each State Administrative Agency (SAA) to deliver the SAP and discuss implementation.

ODP exercise managers are currently meeting with SAAs to assist them in developing an exercise plan for the implementation of the exercise funds they received as part of their FY 2002 award as well as exercise contract support.

ODP also set a deadline for receipt of the applications for the FY 2002 formula grant funds, which resulted in a more timely receipt of applications and award of the FY 2002 funds.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
Prepared correspondence to address the issue of the slow awarding of funds recommendation			07/18/2002

How We Will Know It Is Fixed:

In 2002, OIG closed finding based on correspondence submitted.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	**Date of Submission:**	**Component:**	**Original Target for Completion:**	**Current Target for Completion:**
SHARING OF INTELLIGENCE AND LAW ENFORCEMENT	11/12/2002	FBI	N/A	On-going

Issue and Description:

- PROTOCOL FOR NOTIFYING HIGHER LEVELS OF MANAGEMENT AND DISSEMINATING THREAT INFORMATION
- CRITERIA FOR EVALUATING AND PRIORITIZING THREAT INFORMATION

A recent OIG report (#02-38) found that in addition to developing and disseminating a written assessment of the threat of a terrorist attack, FBI also needs to more effectively process tactical threat information. The FBI receives a constant follow of information about possible terrorist threats and faces an enormous challenge in deciding what information requires what type of response. OIG audit noted a lack of criteria for initially evaluating and prioritizing incoming threat information and a lack of 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. Additional OIG is concerned 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.

What we did in FY 2002 / What are the Current Approaches: The FBI concurs with the recommendation to develop criteria for evaluating and prioritizing incoming threat information and is working to improve its threat management capabilities. A system now nearing deployment, was designed to ensure that new threat information is properly routed to all analysts, substantive units, executive management, FBI field offices and the law enforcement and Intelligence Community agencies concerned with tracking a particular threat. The FBI's Threat Monitoring Unit (TMU), working closely with the Intelligence Community, tracks all incoming threat information on a 24/7 basis. The criteria for assessing the reliability of threat information are largely predicated on the nature and reliability of the source and our knowledge of how terrorist groups operate. Analytical tools that can quickly enable us to see patterns and relationships between vast amounts of data can help, and will become increasingly important. Ultimately, the ability to predict and prevent future terrorist attacks depends on the expertise of the analysts and close cooperation between the operational and analytical units.

The FBI is taking a number of steps to improve the synergy between its analytical and operational units. It has begun co-locating operational and analytical units to facilitate information sharing and closer collaboration on terrorist targets. Improved communication between FBI field offices and headquarters will facilitate increased information sharing with the Intelligence Community and other law enforcement agencies.

The FBI is undertaking several initiatives to improve the distribution of information. It is establishing the Information and Requirements Group in the Office of Intelligence to serve as the central information clearing house for terrorist threat information and analysis. This group will be the single focal point through which other FBI entities and external agencies communicate with the FBI's CTD. It will handle all incoming FBI communications from field offices, Joint Terrorism Task Forces (JTTFs), and legal attaches on terrorism cases, as well as cables, reports, and other intelligence products from external agencies. Communications will be reviewed by a duty officer and staff, logged, parsed, and routed to appropriate units. An administrative tickler system will affix accountability and ensure that taskings are completed on schedule. The Office of Intelligence will be assisted in this effort by the Foreign Terrorist Tracking Task Force (FTTTF) and the 56 JTTFs throughout the country. The JTTFs in the field and the National JTTF in the FBI's CTD are effective, real time mechanisms for information sharing among the participating federal, state, and local agencies.

Another key element in the effort to improve the flow of terrorist information to other agencies is the creation of an FBI Reports Officer cadre that will function much like the Reports Officer cadre in CIA's Directorate of Operations.

FBI Reports Officers will take raw reporting from the field offices and Operations Branch in Headquarters and put it into a format that can be disseminated to FBI consumers, while at the same time protecting sensitive investigative information. The centerpiece of this effort is the Terrorism Reports and Requirements Section (TRRS) in the Investigative Operations Branch. TRRS, among other things, will be responsible for establishing reports policy and procedures. In addition, the FBI intends to establish a clearance request database, and a 24/7 Reports Watch Office to handle after hours dissemination of urgent reports and clearance requests.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Disseminate raw intelligence information reports to the Intelligence, Policy and Law Enforcement Communities.	On-going	On-going	
Provide feedback and requirements to FBI Field Offices and Legats to enhance their collection efforts.	On-going	On-going	
Develop an Indications and Warning System which will utilize threats and suspicious activity jointly with Intelligence Community information for analytical review.	On-going	02/28/2003	

How We Will Know It Is Fixed: Reports Officers will be assigned to every field office to manage the intelligence collection and dissemination process from the field. Procedures will be developed so that field offices can submit intelligence reports for direct dissemination. The FBI's TMU will become the primary repository for all threats and suspicious activity within the continental United States, and successful trends and analytical reports will be produced by appropriate entities based on the threats and information provided by the TMU.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **SHARING OF INTELLIGENCE AND LAW ENFORCEMENT**	**Date of Submission:** 11/12/02	**Component:** JMD, INS, FBI	**Original Target for Completion:**	**Current Target for Completion:** On-going

Issue and Description:

- INTEGRATION OF AUTOMATED FINGERPRINT SYSTEMS

Since 1998, the IG has been concerned about the inability of INS and FBI to link the information in their automated fingerprint identification systems. Linking IDENT and IAFIS could provide state and local law enforcement agencies with valuable immigration information as a part of a response from a single FBI criminal history search request. A recent follow up report (#I-2002-003) noted that the integration of FBI's Integrated Automated Fingerprint Identification System (IAFIS) and INS' automated fingerprint identification system-INDENT, has proceeded slowly and is still years away from full integration.

What we did in FY 2002 / What are the Current Approaches:

The current approach is to deploy to a representative sample of INS field sites (Border Patrol stations and ports of entry) the capability to take 10 rolled fingerprints and submit them electronically to the FBI's IAFIS and receive a rapid response (under 10 minutes). Data will be collected that will:

1) Indicate the percentage of aliens attempting to illegally enter the country that have prior records in the FBI's Criminal Master File,
2) Assess the operational impact on INS of taking 10 prints, and
3) Determine the operational impact of additional alien processing workloads on INS, EOIR, USMS, US Attorneys, BOP and the US Courts.

In addition, to facilitate eventual integration of the two systems, a research program is being initiated to determine if a method for rapidly capturing 10 rolled prints could be developed and to assess potential alternatives for searching IAFIS with fewer than 10 rolled prints ("n-print").

Based on analyses of the data collected, the next phase of system integration will be designed, developed and deployed. Because of potentially significant impacts on INS and other downstream agencies, it may be necessary for the next phase of system integration to include use of other than 10 rolled prints, requiring significant changes to IDENT and/or IAFIS. In addition, Congress may need to consider changes in immigration laws.

It is expected that complete integration of IDENT and IAFIS will take several years to accomplish. In FY 2002, JMD, INS and FBI took steps to avoid further situations like the one involving the Rafael Resendez-Ramirez case while progress toward integration is underway. Specifically, IDENT was enhanced by adding fingerprint records from IAFIS (two index fingers taken from a full set of ten) of individuals with a high probability of being apprehended by INS and who also had active wants and warrants listed in the National Crime Information Center (NCIC) system.

Also during FY 2002, progress was made in deploying the initial IDENT/IAFIS capability to INS field sites:

- Workstations (Version 1.1) allowing rapid IAFIS checks were deployed to the first 10 INS sites from which data will be collected (referred to as metrics sites).
- Workstations (Version1.1.1) with similar capability but upgradeable to later versions that include IDENT and ENFORCE functionality were developed. These stations are being deployed in early FY 2003 to another 10 INS metrics sites.
- Workstations (Version 1.1+) that allow simultaneous searches of IAFIS and IDENT were designed. They will be developed and deployed to another 10-21 INS metrics sites in mid FY 2003.

Progress in FY 2002 was delayed due to priority given to the development and deployment of the National Security Entry-Exit Registration System, which diverted attention and resources away from the design and development of an upgraded IDENT/IAFIS workstation that is necessary for the collection of the data mentioned above. This delay may, in turn, delay decisions related to the direction to be taken in phase two of this integration project, or cause those decisions to be made on incomplete data.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Issue Request for Information on Fast Capture of 10 Rolled Prints	11/30/02	11/30/02	
Deploy Version 1.1.1 workstation to 10 new INS metrics sites	12/15/02	12/15/02	
Deploy Version 1.1+ workstation to 10-21 new INS metrics sites	4/30/03	4/30/03	
Upgrade 20 existing INS metrics sites to Version 1.1+ workstations	5/31/03	5/31/03	
Complete testing of "n-print" alternatives (Target date to be determined in consultation with NIST)	TBD	TBD	
Issue report to Congress on potential system and operational costs resulting from IDENT/IAFIS integration	8/15/03	8/15/03	
Design/develop Version 1.2 workstation (includes JABS functionality)	9/30/03	9/30/03	
Develop Version 2 concept of operations and requirements analysis	6/30/04	6/30/04	
Begin Design/development of Version 2	9/30/04	9/30/04	

How We Will Know It Is Fixed:

When INS is able to retrieve FBI records, and other federal, state and local agencies can retrieve INS apprehension records, on a timely basis.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **INFORMATION SYSTEMS PLANNING AND IMPLEMENTATION**	**Date of Submission:** 11/12/02	**Component:** Department	**Original Target for Completion:** 12/04	**Current Target for Completion:** 12/04

Issue and Description:

The OIG continues to identify mission-critical computer systems within the Department that have been poorly planned, experienced long delays in implementation, or did not provide timely, useful, and reliable data. Given the critical role of information systems and the vast sums of money spent on developing and deploying these systems, information systems planning and implementation remains a top management challenge at the Department.

What we did in FY 2002 / What are the Current Approaches:

To meet these challenges identified by the OIG, the Chief Information Officer released the Department's Information Technology Strategic Plan in July 2002. The plan outlines how the Department is strengthening and refocusing its information technology program to meet the Department's new counterterrorism mission and support the achievement of its strategic goals. The Department has established a formal IT investment management (ITIM) policy and process to ensure that investment decisions are aligned with the strategic goals of the Department, are well-planned and justified, fit within the Department's overall IT strategy and enterprise architecture, and are managed effectively throughout the life cycle. The ITIM is designed to ensure disciplined management of IT investments and the involvement of Department and component leadership in the assessment of cost, risk and return for all proposed expenditures on IT. In FY 2002, all of the large components (BOP, EOUSA, FBI, DEA, INS, OJP, USMS, JMD) within DOJ established and began implementation of Information Technology Investment Management (ITIM) policies for managing all major information technology programs and projects. These ITIM policies were developed in line with the Chief Information Officer's Information Technology Strategic Plan released in July 2002. The Department's annual IT expenditures for FY 2003 total approximately $2.1 billion. This represents 8% of the total DOJ budget. The larger components listed above account for 95% of the Department's spending on information technology. In order to meet the goals outlined in the CIO's IT Strategic Plan, the following ITIM activities were accomplished in FY 2002:

- Components implemented an ITIM process
- Each component developed and prioritized its information technology portfolio
- An automated tool was acquired and deployed to facilitate monitoring and reporting of all information technology investments

The ITIM process represents a coordinated and integrated approach that builds on the existing structures and successful practices in order to provide a consistent management approach across the Department. On behalf of the smaller components in the Department, the CIO's organization has designed an ITIM-Lite process. This process is suitable for smaller components that may have more limited staff or those without the IT initiatives of the size and complexity that warrant a more formalized process.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
DOJ IT Investments Managed through an Approved ITIM process	FY 2003	100% for FY 2003	
Project Management Office (PMO) Establishes an organizational office as a center of excellence dedicated to "project management" as a needed management capability and as a resource center for practitioners to manage collaborative projects. Provide project oversight of Department initiatives.	Sept 2003	Sept 2003	
Implement Department ITIM process Develop and implement a periodic or event driven oversight process to perform Department oversight of IT projects in DOJ component portfolios	Develop – Jan 2003 Begin Implementation - Mar 2003 Reassess – Dec 2004	Jan 2003 Mar 2003 Dec 2004	
Unified Infrastructure Plan, design and deploy a Department-wide data network architecture for all DOJ components (*) this indicates an initial operating capability	Plan – Mar 2003 Design – Sept 2003 Deploy* – Dec 2004	Mar 2003 Sept 2003 Dec 2004	
Enterprise Architecture Establish formal link between enterprise architecture and ITIM.	May - 2003		
System Development Life Cycle Revise the existing SDLC Guide and publish a standardized systems development life cycle approach to help ensure effective planning, management, and commitment to information systems.	Revise - Dec 2002 Publish – June 2003		
Performance Planning & Management Update IT strategic plan annually. Develop and implement standardized methodologies for capturing financial, project, and performance information.	Develop – Jan 2003 Implement - April 2003		
How We Will Know It Is Fixed: By continuing to evolve the information technology investment management process and meeting the CIO's IT strategic initiatives, we will effectively align all information technology efforts and continue to build a collaborative strategic planning process involving all the Department's component organizations. These processes will monitor and report on the costs, schedules and technical performance of IT projects. The Department's process for oversight will provide the governance to ensure the success of mission-critical systems.			

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **INFORMATION SYSTEMS PLANNING AND IMPLEMENTATION**	**Date of Submission:**	**Component:** FBI	**Original Target for Completion:** N/A	**Current Target for Completion:** CY2003

Issue and Description:

- IMPROVED PROCEDURES FOR DOCUMENT HANDLING
- COMPUTER SYSTEM CAPABILITIES (INCLUDING DATABASE SYSTEMS)
- DISSEMINATION OF INFORMATION, INADEQUATE QUALITY CONTROL SYSTEMS

The FBI must be able to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. In March 2002, OIG reviewed the belated production of documents in the Oklahoma City bombing case (OKBOMB) and found widespread failures, which led to the belated disclosure of more than 1,000 documents. Failures were traced to the FBI's cumbersome and complex document-handling procedures and its antiquated and inefficient computer systems. OIG concluded that the computer systems could not handle or retrieve documents in a useful, comprehensive or efficient way.

Similarly, the OIG review of the Department's Campaign Finance Task Force found that information was not disseminated appropriately within the FBI and the Department and subsequently, to congressional oversight committees. OIG found a series of problems, including deficiencies in the use and maintenance of the FBI's computer database systems. OIG also noted antiquated and inefficient computer systems, inattention to information management, and inadequate quality control systems.

What we did in FY 2002 / What are the Current Approaches:

With the re-commissioning of the Records Management Division (RMD), the FBI has reestablished a division to ensure executive direction and full-time oversight on all records and all policies and functions affecting records. RMD, in coordination with the Information Resources Division (IRD), has begun the process to update computer database systems. The mission of RMD is to ensure the accuracy, completeness and proper disclosure of FBI records. RMD has re-engineered its component units to improve workflow and efficiency to better meet work process requirements within the division. RMD is developing systems so that proper quality control is in place throughout the FBI's records systems.

The FBI's RMD is establishing central records management applications (RMAs) for the maintenance and control of records within the central records database. The development of RMAs will aid in ensuring the dissemination of information in an accurate and complete manner with the proper security and quality control systems.

A revamped Executive Secretariat now supervises the FBI's Document Management Program for policy information at the executive level. The Executive Secretariat serves as the central Bureau records control point for all official documents for the Director and the Deputy Director of the FBI. An RMA is being tested in the Executive Secretariat for its practical applications to other records system. A fully operational document conversion laboratory, for the scanning of records to a digitized format, has been created and utilized on such matters as "Operation Enduring Freedom", the "ENRON Matter", and most recently the "Sniper Investigation." The scanned images are transferred currently to DVD or CD-ROM. The FBI employs an Optical Character Recognition process for converting imaging to text and verifying the information. The images, and their associated text, are then loaded into the appropriate database system. This system allows for easy access to and retrieval of information by FBI investigative personnel.

The FBI's RMD is conducting a first-ever Bureau-wide inventory to determine what records are in the FBI's possession and where these records are located. A study is being conducted on the creation of a central records repository wherein all records functions would be managed from one location, fully automated, with all FBI records stored and maintained at this location. Collection of storage requirements and maintenance costs is proceeding to ascertain the most effective and efficient location, facility and method for such an operation.

The FBI has begun to streamline its National Name Check Program (NNCP) to meet the increased demand for this vital function. Through an increase in its manpower complement and the updating of its procedures, the NNCP is disseminating information to other agencies in a more timely and effective manner, fulfilling its vital role in security matters.

The FBI's RMD instituted a Service Request Center where all requests for files and records are channeled. This center pulls together various operations involved in the receipt and preparation of requests. A tracking system will be included so each request can be catalogued and its progress traced. The progress of any request can then be ascertained and any potential problem handled in a timely manner.

The Records Management Center has been established to coordinate and develop Bureau-wide records creation and maintenance standards. The records creation and maintenance services will be provided directly to the customers in other FBI divisions.

A unit designed to study and develop records management policy and procedures has been created so the FBI will have up-to-date policies and procedures to ensure compliance with established government-wide regulations. The Records Policy and Training Unit constantly monitors the record systems of the FBI to ensure those systems are performing their functions within accepted records management procedures.

The FBI is striving to vastly improve its records management systems, capabilities and functionality to meet the future responsibilities of the organization, while ensuring that its present, diverse systems are coordinated to address its current vital records management responsibilities.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
-Establish a mobile scanning operation to handle field office and other off site document scanning projects	July 2003	July 2003	
-Re-engineering of RMD to identify appropriate personnel and distribution of new units to improve records management systems and efforts	November 2002	March 2003	
-Establish a document scanning operation at the FBI's records off site facility	February 2003	February 2003	
-Testing an RMA in Executive Secretariat operations for viability in other RMD units	March 2003	March 2003	

How We Will Know It Is Fixed: Upon the implementation of new systems and procedures, the FBI will be able to respond accurately, completely and in a timely manner to the multitude of records requests it receives. While these systems and applications are being developed, the FBI has improved its operations, as exhibited by its support of "Operation Enduring Freedom."

U. S. DEPARTMENT OF JUSTICE
Management Challenge Report
Issue and Milestone Schedule

Management Challenge: **COMPUTER SYSTEM SECURITY**	**Date of Submission:** 11/12/02	**Component:** Department	**Original Target for Completion:** Dec 2004	**Current Target for Completion:** Dec 2004

Issue and Description:

- VULERABILITIES, POTENTIAL COMPROMISE OF SENSITIVE SYSTEMS AND DATA—ACCOUNT INTEGRITY, SYSTMES AUDITING, AND COMPONENT LEVEL SECURITY POLICIES AND PROCEDURES

Regular computer security audits are being conducted as a requirement of the Government Information Security Reform Act (GISRA). Weaknesses has been identified in both classified systems and sensitive but non-classified systems. Specific concerns include issues with management, operational, and technical controls that protect each system and the data stored on it form unauthorized use, loss, or modification. Because technical controls prevent unauthorized system access, OIG concluded that the vulnerabilities noted in those areas were most significant. The most common vulnerability was with security policies and procedures, and password and logon management. OIG also noted concern about account integrity and systems auditing management. To varying degrees, the OIG GISRA audits also found insufficient or unenforced Department level and component level security policies and procedures. In several areas, OIG audits identified vulnerabilities such as broadly stated or minimally imposed standards allowed system security managers too much latitude in establishing system settings. Additionally vulnerabilities identified were more voluminous and material for the Department's classified compared to its SBU systems. To address the deficiencies OIG offered a series of recommendations, including increased oversight, development of documented procedures, and establishment of proper system settings to help improve computer security.

What we did in FY 2002 / What are the Current Approaches: To address repeatable weaknesses in the Department's implementation of computer security controls and to meet this challenge identified by the OIG, the Chief Information Officer released the Department's Information Technology Strategic Plan in July 2002. The plan outlines how the Department is strengthening and refocusing its information technology program to meet the Department's new counterterrorism mission and support the achievement of its strategic goals. Under the auspices of the Department CIO, an Information Security Staff will be created and managed by a senior executive with the responsibility for implementing the Department's IT security program through the development of standards, procedures, and guidance to ensure compliance with applicable Department, Federal, and National Security policies and directives and industry best-practices. In addition, this Staff will ensure that component classified and sensitive but unclassified systems have implemented the appropriate IT security controls and shall be responsible for ensuring that components identify corrective plans and milestones when the security controls are not met and for monitoring these corrective action plans. In the past year, the Department made significant progress in strengthening the Department's Information Technology Security Program and in implementing the requirements of the Security Act. These accomplishments include:

- Appointment a Chief Information Officer (CIO) with a broad mandate to provide Department-wide leadership in the information technology (IT) arena, including security;
- Development of an Information Technology Strategic Plan that sets forth a vision and specific initiatives for enhancing information security;
- Continued implementation and refinement of a Departmental system for tracking all IT security weaknesses and corrective actions;
- Full integration of security into other information technology management processes, such as capital planning;
- Development of the Department's Security Act Report, which included individual assessments of over 150 systems;
- Awarded a contract for independent verification and validation of component IT system security controls and initiated several tasks against the contract;
- Initiation of a project to define requirements for a Department-wide public key infrastructure program; and
- Initiation of a project to define requirements for a Department-wide security architecture.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
Information Security Staff Establish a centralized IT security office reporting directly to the Department CIO with responsibility for ensuring the appropriate security controls are implemented in the Department's classified and sensitive but unclassified systems.	December 2002	January 2003	
Develop IT Security Standards Develop minimum IT standards for implementation of security controls for the Department's classified and SBU systems. 12 standards have been identified.	January 2003	January 2003	
IT Security Architecture Develop and document the Department's IT Security Architecture at a high level that will be integrated into the Department's Enterprise Architecture. The high level IT Security Architecture will provide for increased information sharing and will include boundary protection requirements, network requirements, and PKI architecture.	Version 1.0 September 2003	September 2003	
Public Key Infrastructure Plan, design and deploy a Department-wide Public Key Infrastructure. Establish a PMO to manage the program and to coordinate with component initiatives.	PKI plan, design, and requirements – March 2003 Pilot – December 2003 Deployment – December 2004	March 2003 December 2003 December 2004	
Increased Oversight and Monitoring Enhance and deploy to components the Security Management and Reporting Tool (SMART) that tracks all known vulnerabilities, weaknesses, and corrective actions. Expand oversight activities to include classified systems.	February 2003 March 2003	February 2003 March 2003	
Security Awareness Training Develop and begin implementing a Department – wide (with the exception of the FBI) web-based security awareness training tool.	January 2003	January 2003	
Common Solutions and Automated Tools Identify common solutions and automated tools to monitor security compliance of network and system parameters and identify vulnerabilities.	September 2003 Implement-December 2004	September 2003 December 2004	

How We Will Know It Is Fixed: By continuing to evolve the information technology security program and meet the CIO's IT strategic initiatives, we will be able to effectively implement IT security controls, reduce the number of vulnerabilities and repeat OIG findings and provide for greater trust of the Department's systems and further enable information sharing and collaboration.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **COMPUTER SYSTEMS SECURITY**	**Date of Submission:** 11/19/2002	**Component:** FBI	**Original Target for Completion:** N/A	**Current Target for Completion:** 12/31/03

Issue and Description:

- SECURITY OVER SENSITIVE PROGRAMMATIC OR FINANCIAL DATA/ RELIABILITY OF FINANCIAL REPORTING

A recent OIG report (#01-13) 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.

What we did in FY 2002 / What are the Current Approaches: Specific information concerning weaknesses in FBI computer systems security is classified at the "Secret" level. However, the FBI provides the following information concerning its efforts to improve computer systems security: In December 2001, the FBI consolidated all security responsibilities – information assurance (IA), facility/industrial, and personnel - under a new Security Division. The FBI's IA Program, established in the Spring of 2002, is being designed to ensure confidentiality, integrity, accountability, and availability of FBI information. Actions are being taken in the areas of policy, personnel, and technology. The content, process, and format of FBI security policy are undergoing major, strategic change. Eighty-seven percent of legacy, classified systems are in the process of certification and accreditation or have already been accredited. A four-phased, Integrated Security Training, Awareness, and Education Program Plan was developed. A comprehensive security knowledge/skills requirement matrix was included in this Plan to ensure that the appropriate type and level of security knowledge are built into training courses and curriculum for each FBI functional role. The IA Program will be inserted into the FBI's Information Technology Investment Management (ITIM) and Enterprise Architecture (EA) Programs to identify security issues, document security requirements and define reporting mechanisms. This will allow full security integration of the IA Program into the FBI's selection, control, and evaluation processes for information resource management.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Specific milestones are classified at the "Secret" level.		12/31/2003	

How We Will Know It Is Fixed: All audit findings will be closed after agreed-upon actions are completed.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: DETENTION SPACE AND INFRASTRUCTURE	Date of Submission: 11/08/02	Component: Detention Trustee	Original Target for Completion: N/A	Current Target for Completion: On-going

Issue and Description:

- PROCUREMENT PROCEDURES TO OBTAIN JAIL SPACE FROM STATE/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, the OIG feels it is important that this matter be resolved promptly and that detention space be acquired in a coordinated, cost effective, and legal fashion.

- RAPID GROWTH LEADING TO OVERPAYMENTS (INS/USMS/BOP)

Over the past several years, OIG audits of detention space contractors have resulted in significant amounts of questions and unsupported costs paid to entities. For example, OIG audits of contractors for detention space have found that an Intergovernmental Agreement (IGA) for detention space resulted in the overcharge of $6 million (OIG report #GR70-01-005) due to an understatement of the average daily population. Currently INS, USMS and BOP continue to use different amounts to calculate jail day populations, OIG found that by using the same amounts, the Department could realize an annual savings of approximately $6.4 million. Additionally an audit of DeKalb County, Georgia's Sheriff's Office (OIG Report #GR-40-02-002) revealed that DeKalb County included $13.4 million of operating costs that were unallowable 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, the OIG questioned costs of $5.6 million and identified funds to better use of $7.8 million. Another IGA was audited revealing an overpayment of $3.6 million to the government of Guam (OIG report #GR-90-01-006).

- RESOURCES AND AUTHORITY TO CORRECT DEFIECIENCIES

OIG is concerned that the Detention Trustee may not have the authority or resources to resolve many of the long-standing issues described above.

What we did in FY 2002 / What are the Current Approaches: The Department houses a daily average of approximately 46,000 detainees in state and local facilities. In contrast, approximately 18,000 detainees are housed in federally owned and operated facilities. The relationships established by Intergovernmental Agreements (IGAs) with state and local governments are paramount to carrying out the function of detention. Such arrangements also save on costly capital development of federal facilities. In FY 2002, the Office of the Federal Detention Trustee (OFDT) under took a comprehensive review of the Department's IGAs and provided a recommendation to the Office of the Deputy Attorney General (ODAG), concerning "overpayments" and future policy for obtaining these services. OFDT recommended the overpayments should be recovered by the component involved, under the authority of the Debt Collection Act. ODAG concurred with the OFDT recommendation, and directed the relevant components involved to work with the Civil Division and appropriate United States Attorneys' Office to take action to recover the overpayments. The Office of Legal Counsel subsequently determined that the Department does possess statutory authority to enter into fixed-price contracts for detention services. To minimize the potential for abuse and help ensure cost efficiency, the Office of the Attorney General ordered that any such fixed-price contract must be approved by the component head and the OFDT.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
Issue Department-wide policy for entering into Intergovernmental Agreements	10/1/02	1/17/03	1/17/03
Arrangements to collect or forgive the overpayments under the authority of the Debt Collection Act	4/1/02	4/1/02	10/07/02

How We Will Know It Is Fixed: When the overpayments are collected or forgiven, and the new policy for future agreements is implemented.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	Date of Submission:	Component:	Original Target for Completion:	Current Target for Completion:
DETENTION SPACE AND INFRASTRUCTURE	11/08/02	INS	None	On-going

Issue and Description:

- INSTITUTIONAL REMOVAL PROGRAM

OIG audit (#02-41) found that INS's Institutional Removal Program (IRP) did not always have timely processing of IRP cases. In a sample of 151 cases of criminal aliens in INS custody reviewed, a total of $2.3 million in IRP-related detention costs were identified. Of which, $1.1 million was attributable to failures in the IRP process within INS's control.

What we did in FY 2002 / What are the Current Approaches:

As the final version of the report was released in September 2002, most of the corresponding initiatives will take place in FY 2003 and beyond. However, in FY 2002, INS created a program element that will provide for the funding and tracking of resources expended for the IRP. This program element officially went into effect October 1, 2002. In June 2002, INS established a position to serve as liaison between INS and the Department of State and to facilitate the timely issuance of travel documents.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
Completion of a study to determine the total foreign-born inmate population, the resources required to cover the population through IRP, and the risks involved in not providing full coverage.	2nd Quarter, FY 2004	2nd Quarter, FY 2004	
Revision of the Detention and Removal Field Manual to include clear, consistent, and standardized procedures for IRP documentation and A-file organization. The updated Manual will also include streamlined procedures for removal to minimize detention costs.	3rd Quarter, FY 2003	3rd Quarter, FY 2003	
Reclassification of the Detention Enforcement Officer (DEO) position to be the Immigration Enforcement Agent (IEA).	2nd Quarter, FY 2003	2nd Quarter, FY 2003	

How We Will Know It Is Fixed:

Criminal aliens issued final orders of deportation will be removed from the United States in a manner that minimizes Service detention costs.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **FINANCIAL STATEMENTS AND SYSTEMS**	**Date of Submission:** 11/12/02	**Component:** Department	**Original Target for Completion:** N/A	**Current Target for Completion:** On-going

Issue and Description:

- IMPROVEMENTS ARE NEEDED TO COMPLY WITH FEDERAL ACCOUNTING PRINCIPLES

IMPROVEMENTS ARE NEEDED IN GENERAL AND APPLICATION SYSTEM CONTROLS
ABILITY TO PREPARE TIMELY FINANCIAL STATEMENTS

In the FY 2001 Consolidated Report on Internal Controls, OIG found 13 material weaknesses and 12 reportable conditions pertaining to non-compliances with federal accounting and systems standards. Although the Department was able to overcome these issues and achieve an unqualified opinion, an intense, highly manual effort to prepare the financial statements and satisfy audit requirements was required. Outdated financial systems complicate the Department's efforts to meet standards and new due dates. The Department and its components have significant hurdles to overcome in order to meet OMB's accelerated FY 2003 audit due dates. Statements must be prepared in on a quarterly basis and auditors must be able to test and rely upon internal control processes throughout the year.

The Department also faces issues with staff resources. 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 limiting in-house knowledge and expertise.

What we did in FY 2002 / What are the Current Approaches:

a) The Chief Financial Officer required an audit Corrective Action Plan from each component with internal control weaknesses and/or non-compliances with laws and regulations. The plans were designed to eliminate or diminish the severity of the weaknesses cited in the FY 2001 audit reports. The Finance Staff closely monitors the plans and progress, and quarterly updates are provided to the Office of the Inspector General.

b) The Controller and Director, Finance Staff, met personally with component financial officers to review weaknesses cited in the FY 2001 audit and identify specific corrective action targets for each component.

c) The Finance Staff issued a Departmental timeline in March 2002, with a list of critical interim task and due dates designed to meet OMB's accelerated due dates; ongoing meetings of a Department-wide Financial Statements Working Group are held to resolve preparation issues, discuss guidance, and review new policies.

d) CFO's were directed to enforce compliant policies and procedures for obligation accrual processing, quarterly review of accrual balances, and reconciling accrual data with trading partners on a quarterly basis.

Current Approaches: for FY 2003, the CFO Corrective Action Plans will remain in force. New activities include:

- To assist in meeting new OMB due dates, DOJ will acquire a new financial statement consolidation package for DOJ-wide preparation use, which should reduce consolidation time by 10 to 15 days.
- DOJ will move internal FY 2003 statement due dates up by 30 days.
- DOJ will acquire a new Department-wide Unified Core Financial System to replace outdated component systems.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Components are hiring additional prep staff, (JMD, USMS, FBI)	6/30/2003	6/30/2003	
DOJ will acquire new financial statement preparation software	9/30/2003	9/30/2003	

<table>
<tr><td>DOJ will decrease the number of component level Material Weaknesses and Reportable Conditions in the audit reports</td><td>1/15/2003</td><td>1/15/2003</td><td></td></tr>
<tr><td>DOJ will acquire a commercial off-the-shelf (COTS) Core Financial System. Acquisition and Implementation planned for FY2003-FY2007. Date shown is for software license acquisition</td><td>5/30/2003</td><td>5/20/2003</td><td></td></tr>
<tr><td colspan="4">.<b>How We Will Know It Is Fixed:</b>
a) The Department will continue to earn a clean opinion on its Consolidated Financial Statement each year;
b) The Department will meet OMB’s accelerated due dates for the quarterly and annual financial statements;
c) Component level audit reports will show decreased material weaknesses and reportable conditions each year until they obtain clean reports on internal controls and are compliant with laws and regulations. The Department’s material weaknesses are a consolidated level will be eliminated or diminished in severity as underlying component weaknesses are corrected.</td></tr>
</table>

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	Date of Submission:	Component:	Original Target for Completion:	Current Target for Completion:
GRANTS MANAGEMENT		COPS		Completed

Issue and Description:

- TIMELY SUBMISSION OF GRANTEE MONITORING AND FINANCIAL REPORTS, ON-SITE MONITORING REVIEWS ADDRESSING ALL GRANT CONDITIONS

In 2002, OIG audits of grants disbursed by COPS identified more than $11 million in questioned costs and more than $3 million in funds to better use. Additionally, 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.

What we did in FY 2002 / What are the Current Approaches:

In FY 2000, COPS established a grant monitoring checklist to assess the grantees' compliance with the regulations, terms and conditions for each COPS grant. This checklist, used during all on-site visits and all office-based grant reviews, includes the following ten compliance areas: 1) Retention planning; 2) Failure to retain; 3) Community policing (Problem-Solving, Community Partnerships, Organizational Commitment); 4) Making Officer Redeployment Effective (MORE); 5) Criminal Intelligence Systems (28 CFR Part 23); 6) Programmatic Reporting (Departmental Initial Report, Annual Report, Progress Reports); 7) Questioned Costs; 8) Non-Supplanting Requirements (Early Hire, Reduction in Force); 9) Financial Status Report and; 10) Training Special Conditions (Hiring and MORE grants). COPS established the following policies (in FY 1999) and continues to follow them to ensure grantees submit grant monitoring and financial status reports on time:

- Grantees from Funding Accelerated for Small Towns (FAST), Accelerated Hiring, Education and Deployment (AHEAD) and Universal Hiring Programs (UHP) who fail to submit their required Department Annual Reports by the deadline are subject to the suspension and eventual termination of COPS grant funding. Grantees are sent several delinquency warning letters before being sent a notice of non-compliance, at which point their funds are suspended. If they do not submit the delinquent report(s) following the issuance of this notice, their funds are de-obligated and the grant in question is terminated. For 2001 reports, only two dozen grantees from among more than 6,000 had their grants suspended and only a dozen are subject to having their grants terminated and funds deobligated. To date for the 2001 reporting cycle, the submission rate is greater than 99%.
- At the beginning of each quarter, a preprinted Financial Status Report facsimile is sent to current grantees to encourage timely reporting. Grantees who fail to submit their quarterly Financial Status Reports by the deadline have their funding access automatically frozen within the Phone Activated Paperless Request System (PAPRS) automated drawdown system. Access to funding cannot be restored until any and all delinquent Financial Status Reports are submitted.

The $11 million in questioned costs and $3 million in funds to better use, are preliminary recommendations from OIG audits and do not represent actual grantee violations of grant conditions. Currently, COPS is in the process of determining whether the OIG's recommendations are valid and accurate. To do so, COPS obtains relevant information from the grantees concerning their grant expenditures and other compliance with grant terms and conditions. If COPS determines that a grantee has in fact violated the terms of its grant, then COPS fashions an appropriate remedy. That remedy can involve termination of funds, repayment, debarment from future COPS funding or other appropriate sanctions. During 2002, COPS undertook an initiative to identify all grantees, active and inactive, who did not have a current status report on file and then to request the grantee bring their reports up to date. In addition, ten Grants Management Training sessions were provided to grantees across the country emphasizing correct and timely reporting.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
N/A – The grant management issues raised by the OIG have already been addressed. The specific findings from FY 2002 audits of COPS grantees will be addressed over the course of a normal audit resolution process.			
How We Will Know It Is Fixed: The COPS Office considers these issues fixed. Ninety-nine percent of Department Annual Reports are returned on time, with grantees in noncompliance numbering approximately two dozen, down from several thousand per year previously. Grant monitoring reviews address all grant requirements: programmatic, financial, and administrative.			

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **GRANTS MANAGEMENT**	**Date of Submission:** 11/13/2002	**Component:** OJP	**Original Target for Completion:** 06/30/2003 and 03/2004	**Current Target for Completion:** 06/30/2003 and 03/2004

Issue and Description:

- TIMELY SUBMISSION OF GRANTEE MONITORING AND FINANCIAL REPORTS, ON-SITE MONITORING REVIEWS ADDRESSING ALL GRANT CONDITIONS

OIG reviews found that many grantees did not submit required program monitoring and financial reports in a timely fashion and that program officials' on-site monitoring reviews did not consistently address all grant conditions.

- INADEQUATE COUNTERTERRORISM PERFORMANCE MEASURES TO ASSESS ODP EFFORTS

OJP had not developed adequate performance measures for evaluating whether the program improved grantees' capability to respond to terrorist acts.

What we did in FY 2002 / What are the Current Approaches:

TIMELY SUBMISSION OF GRANTEE MONITORING AND FINANCIAL REPORTS, ON-SITE MONITORING REVIEWS ADDRESSING ALL GRANT CONDITIONS

OJP implemented procedures to change it business practices to allow for a withholding of funds if progress reports were not filed timely. Additionally, during FY 2002, OJP developed guides for conducting on site visits, conducted desk reviews of grantee files, and developed systems that better track grantee contacts including grantee follow up regarding on site visits. OJP Financial Guide was updated in May 2002 to include procedures stating that a withholding of funds will be instituted if grantees fail to follow grant requirements by untimely filing of progress reports.

INADEQUATE COUNTERTERRORISM PERFORMANCE MEASURES TO ASSESS ODP EFFORTS

ODP's mission is to develop and implement a national program to enhance the capacity of state and local agencies to respond to WMD terrorist incidents through coordinated training, equipment acquisition, technical assistance, and support for state and local exercise planning. In order to measure how well it has achieved its mission, ODP has established performance standards relating to training, equipment, technical assistance, and support for state and local exercise planning. All of these are essential to assessing ODP's ability to enhance the capacity of state and local agencies to respond to WMD terrorist incidents. Performance standards must reflect the nature of these contributions. For example, training enhances the capability of individuals, while equipment and exercises enhance the capability of communities. ODP has established appropriate performance measures for these contributions, and is in the process of implementing a comprehensive evaluation program to assess actual program performance.

In December 2002, ODP will complete the development of the evaluation process to update information within the strategies on a continuous basis

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
TIMELY SUBMISSION OF GRANTEE MONITORING AND FINANCIAL REPORTS, ON-SITE MONITORING REVIEWS ADDRESSING ALL GRANT CONDITIONS Implemented procedures to withhold funds if progress reports are not filed on a timely basis. Updated OJP Financial Guide to include procedures to be used if grantees do not follow grant requirements for timely filing of progress reports.			05/2002
Beginning in January 2003, the above procedures will be supplemented through electronic withholding of funds if OJP systems support untimely or unsubmitted reports.	01/2003	01/2003	
Phase in the Grants Management System to all Bureaus and Program Offices		06/30/2003	
INADEQUATE COUNTERTERRORISM PERFORMANCE MEASURES TO ASSESS ODP EFFORTS Issued the final draft of the Justice Exercise and Evaluations Manual. This Manual is a four-volume guide provided to ODP's state and local grant recipients. It consists of: an overview volume of the exercises process as part of domestic preparedness; the second volume provides the "how to" information needed to conduct an exercise; the third volume offers sample forms and documents related to, for example, interagency agreements and responsibilities; and the fourth volume provides the information needed to conduct an evaluation of the exercise's effectiveness. OJP has completed the first volume and has draft versions of the remaining volumes.	10/2002		09/2002
First cycle of impact evaluation results complete		03/2004	

How We Will Know It Is Fixed:

TIMELY SUBMISSION OF GRANTEE MONITORING AND FINANCIAL REPORTS, ON-SITE MONITORING REVIEWS ADDRESSING ALL GRANT CONDITIONS

In January 2003, the payment system will not allow grantees to access funds if they are not current with financial and programmatic reporting requirements, and performance measures will be evaluated to determine program outcomes.

INADEQUATE COUNTERTERRORISM PERFORMANCE MEASURES TO ASSESS ODP EFFORTS

To address the counterterrorism performance measures portion, OIG verbally agreed to close the recommendation on September 20,2002 pending the receipt of the DOJ Exercise and Evaluation Program Manual. Once this condition is met, OIG will close this recommendation.

We will know that the evaluation portion is completed when ODP is able to compare the March 2004 impact evaluation results against the performance measures developed through the initial December 2002 evaluation process.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	Date of Submission:	Component:	Original Target for Completion:	Current Target for Completion:
PERFORMANCE BASED MANAGEMENT	11/12/02	Department	N/A	Completed FY 2002

Issue and Description:

- LINKING OUTCOME MEASURES TO BUDGET DEVELOPMENT AND ALLOCATION OF RESOURCES

A significant management challenge for the Department is ensuring, through performance-based management, that its programs are achieving their intended purposes. Linking credible performance measures to budget development and allocation of resources has been uneven. In recent audits, the OIG has found that programmatic performance measures are not always well developed or adequately focused on outcomes.

What we did in FY 2002 / What are the Current Approaches:

- The internal budget process was structured by Strategic Goal and incorporated performance into the earliest stages of budget development.
- DOJ Budget programs (decision units) were realigned with primary mission areas and the Strategic Plan. This allows full program costs to be aligned with program accomplishments.
- A Performance and Resource Table was developed for inclusion in the budget that aligns resources with results. Another feature of this table is a display of budget enhancements and corresponding performance associated with the specific budget request.
- In FY 2001, broad outcome measures were established for drug trafficking and immigration. In FY 2002, a new measure was developed for locally targeted gun crime and USMS transitioned a key performance measure from warrants based data to fugitives.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
The pursuit of additional outcome oriented performance measures is a continuous effort for the Department.		On-going	

How We Will Know It Is Fixed: N/A

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge:	Date of Submission:	Component:	Original Target for Completion:	Current Target for Completion:
PERFORMANCE BASED MANAGEMENT	11/12/02	OIA	6/11/02	On-going

Issue and Description:

- INADEQUATE PERFORMANCE MEASURES, EXTRADITION CASES

A recent OIG report (#I-2002-008) found that the Office of International Affairs (OIA) had established performance measures for treaty negotiations, but had not established measures for processing extradition requests. Also, 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.

What we did in FY 2002 / What are the Current Approaches:

- The Section Chief, along with OIA line attorneys, supervisors and paralegals, reviewed every extradition and mutual legal assistance file in the office, with the objective of advancing the cases or, if they are no longer viable, closing them. The process resulted in closing over 5,000 files. Each geographic team in OIA has been directed to undertake its own comprehensive file review on a semi-annual basis.
- OIA developed written protocols to establish office-wide guidelines for reviewing case files, including a description of the type of case to be reviewed, specific actions to be taken, and criteria for closing files.
- OIA is updating case status information in OIA's Oracle system and adapting existing fields to enhance our ability to capture and retrieve case-related data. All attorneys and paralegals have completed Oracle training.
- OIA set up two NCIC computer terminals in OIA to enable the Office to take direct action to quickly determine a fugitive's status, and thereby handle extradition cases more efficiently.
- After advertising to fill vacant attorney and support position vacancies, the best-qualified candidates have been interviewed and are completing the final stages of the hiring process.
- The file review gave OIA an accurate tally of the number of active files in the office. In order to distribute the cases more equitably, a modified office reorganization was developed, involving OIA's two largest geographic teams, which will result in a reallocation of country assignments between the teams and a reassignment of cases among attorneys.
- The Criminal Division does not agree with the OIG's criticism and follow-up recommendation regarding performance measures. The OIG criticized OIA for not establishing performance measures for such things as processing extraditions requests and evidence requests. However, the OIG based this on their review of the Department's Performance Plan – not the Division's Performance Plan that is more comprehensive and does include measures for extradition and mutual legal assistance (evidence) requests.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
After discussion with the Evaluation and Inspections Division of the OIG, OIA is very close to closing out any open recommendations with this review.		FY 2003	

How We Will Know It Is Fixed: See milestone section above.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **PERFORMANCE BASED MANAGEMENT**	**Date of Submission:** 11/13/2002	**Component:** OJP	**Original Target for Completion:** 03/2002	**Current Target for Completion:** Completed 04/2002

Issue and Description:

- INADEQUATE PERFORMANCE MEASURES, DNA BACKLOG REDUCTION

In a recent audit of OJP's Convicted Offender DNA Sample Backlog Reduction Grant Program (#02-20), OIG 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 an adequate performance measure, OJP cannot measure progress in achieving its mission to reduce and eventually eliminate the convicted offender DNA sample backlog.

What we did in FY 2002 / What are the Current Approaches:

Effective April 2002, OJP revised its mission statement and performance measure for the Convicted Offender DNA Sample Backlog Reduction Grant program to better reflect the mission of the program. For comparative purposes the original and revised mission statement and performance measure are listed below:

Original Mission: To reduce and ultimately eliminate the convicted offender DNA sample backlog awaiting analysis and entry into the National DNA Index System (NDIS).

Revised Mission: To reduce and ultimately eliminate the convicted offender DNA sample backlog awaiting analysis and increase the number of samples available for entry into the National DNA Index System (NDIS).

Original Performance Measure: Number of samples analyzed with 13 STR DNA markers entered into the national database.

Revised Performance Measure: Number of samples analyzed with 13 STR DNA markers available to the national database.

In light of the revisions to the program's mission and the corresponding performance measures, we believe that the data that we are collecting and monitoring (i.e., number of samples analyzed and number of states experience and increase in the number of samples contributed) appropriately reflect our efforts toward meeting the revised mission. Therefore, we consider this recommendation closed.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
N/A (In April 2002, OJP revised the mission statement to better reflect the efforts of the Convicted Offender DNA Sample Backlog Reduction Grant program.)			

How We Will Know It Is Fixed:

The mission statement has been revised to more accurately represent the objective of the program and the data being collected.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **PERFORMANCE BASED MANAGEMENT**	**Date of Submission:** 11/12/2002	**Component:** FBI	**Original Target for Completion:** N/A	**Current Target for Completion:** On-going

Issue and Description:

- ESTABLISHING AN EFFECTIVE SYSTEM OF PERFORMANCE MEASURES, COUNTERTERRORISM (CT) PROGRAM

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

What we did in FY 2002: The FBI developed a program management strategy designed to achieve maximum feasible capacity in the CT program and continues to pursue full implementation of this strategy. Every year, the program measures CT capacity via the Annual Field Office Report (AFOR). The AFOR provides a template to FBI field offices for evaluating their CT capabilities, based on specified criteria in all areas of CT effort. Each field office rates its CT program and the information is analyzed at Headquarters to provide an annual update to FBI executive management regarding the state of the FBI's CT program. The analysis of the AFOR information enables the CT program to identify gaps in capacity and develop targeted strategies to address those gaps.

The FBI will finalize and publish its CT program plans during mid-FY 2003. These plans lay out the operational goals, objectives, and strategies against priority threats for the coming fiscal year. These plans serve to focus FBI management on priority initiatives, ensuring a coordinated national effort against the terrorism threat.

Current Approaches: The FBI is finalizing its CT program plans and will distribute them throughout its Counterterrorism Division (CTD) and field offices. The program will then develop operational performance measures consistent with program plan strategies to track performance against specific operational strategies. The FBI will continue to assess capacity through the AFOR processes and will continue discussion with oversight entities to fully link performance results to the budget. Finally, the FBI will continue to implement ongoing strategies to close capacity gaps identified through the AFOR process. Tracking operational success (operational performance measures) as well as capacity information will provide a comprehensive view of the CT programs' progress towards achieving maximum feasible capacity in counterterrorism efforts.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Finalize and publish CTD Program Plans.	10/01/2002	12/01/2002	
Develop operational performance measures consistent with program plans and develop a tracking system to evaluate success on a regular basis.	On-going	On-going	
Publish the Supplemental Director's Report on Counterterrorism and calculate a new PCI.	04/01/2003	04/01/2003	
Conduct 2003 AFOR Process to evaluate capacity, publish Director's Report on Counterterrorism.	09/01/2003	09/01/2003	

How We Will Know It Is Fixed:

FBI program managers will have access to continuous feedback on the success of operational strategy through a system of real-time tracking of indicators linked to program plans. These measures will indicate if strategies are successful and should be continued or if strategies need to be revised.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: HUMAN CAPTIAL	Date of Submission: 11/20/02	Component: Department	Original Target for Completion:	Current Target for Completion: On-going

Issue and Description:

- ATTRACTING, TRAINING AND RETAINING SUFFICIENT QUALIFIED EMPLOYEES

The Department continues to experience a management challenge in attracting, training, and retaining sufficient qualified employees in many areas of operation. Many employees are leaving for positions with the new Transportation Security Agency or the private sector. Additionally, retaining high quality information technology specialists who are knowledgeable about the latest hardware and software is a challenge and the government runs the risk of falling further behind the private sector. In other areas, the Department components face problems in expeditiously hiring qualified specialists. The Department must have the capabilities, resources, and facilities to adequately train the influx of entry-level personnel. Lastly, attention must be paid to training new managers who will be needed to replace the significant number of senior employees nearing retirement age.

What we did in FY 2002 / What are the Current Approaches:

We have developed the DOJ Human Capital Strategic Plan to address human capital issues requiring the Department's serious attention; the Plan has four main goals:

Goal 1: Design an effective organization and workforce that aligns with the overall DOJ mission and Strategic Plan; Goal 2: Reduce skill gaps through recruitment, training, and succession planning; Goal 3: Develop an organizational culture that clearly identifies and communicates performance expectations to employees, reports and assesses results, and provides incentives/penalties/remedial training; Goal 4: Strengthen human capital leadership within DOJ.

The Plan was designed to make sure that the Department's human capital goals and objectives concentrate on the Human Capital portion of the President's Management Agenda, as explicated on the Scorecard maintained by the Office of Management and Budget. The Plan strongly relates to the Attorney General's ten management goals for the Department, and reflects both findings and recommendations recently generated during the course of several in-depth reviews of human capital management within the Department and its major components. We have already begun to work on action items resulting from the Plan; DOJ will take the lead, and the components will participate, in creating appropriate policies, programs, processes, and frameworks as called for in the Plan. Specific accomplishments cited in the Plan include:

- DOJ is seen by applicants to have highly desirable job opportunities;
- DOJ has well-established, excellent training programs for new law enforcement and legal job entrants;
- Workforce average age (40) significantly lower than Federal Government average (47);
- Projected annual retirement rates are low, and actual retirement rate for 2001 was 1/3 less than projected;
- DOJ's "recruit and train" model results in a substantially large majority (95-97 percent) of supervisors coming from in-house ranks;
- DOJ has tested and is implementing an electronic training strategy;
- Several components have tested and implemented electronic hiring systems; and
- DOJ has an extensive data bank on job competencies needed for all its occupations.

Milestones FY 2003/FY2004:	Original Target Date	Current Target Date	Actual Date of Completion
A detailed action plan (9 pages) may be obtained by calling Debra Tomchek on 305-4976			

How We Will Know It Is Fixed: Ultimately, the success of human capital initiatives is measured by achievement of Annual Performance Plan goals. Without the proper numbers, skills, and motivation of employees, it will not be possible to achieve the objectives outlined on the Department's Strategic Plan.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: **HUMAN CAPITAL**	**Date of Submission:** 11/12/02	**Component:** FBI	**Original Target for Completion:** N/A	**Current Target for Completion:** 3/2003

Issue and Description:

- HIRING AND TRAINING STAFF TO MEET THE BUREAU'S COUNTERTERRORISM MISSION

FBI must hire and train additional intelligence analysts and investigators to assist in meeting the Bureau's new counterterrorism responsibilities.

What we did in FY 2002 / What are the Current Approaches:

The FBI is making substantial progress in building a corps of intelligence analysts. Our reorganization includes a total of 367 tactical and strategic analytical personnel. Currently, there are 181 analytical personnel in place and another 118 that are in the background investigation phase for hiring. These numbers do not include the 25 CIA analysts currently detailed to the FBI's Counterterrorism Division (CTD).

Additionally, 100 FBI Special Agents were transferred into its CTD in FY 2002, and 13 have been transferred in thus far in FY 2003. There were approximately 30 Special Agents transferred out of the FBI's CTD in FY 2002, and 30 have been transferred out thus far in FY 2003.

The FBI has completely revamped its analyst training program. The basic analysis course was expanded from five to six weeks, with more emphasis on analytical tradecraft. The CIA has assisted in designing the tradecraft portion of the course, and CIA instructors will teach the first four sessions, after which FBI instructors will take over. The first session of the new basic course will begin on February 22, 2003. In addition, CIA will hold a four-day course on managing analysis, which is mandatory for all FBI managers in the Terrorism and Prevention Analysis Branch. The course will begin during the first week of December 2002. We are also in the process of staffing the Office of Intelligence, which will be responsible for overseeing the career development of all FBI analysts.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
Approximately 75 percent of the Intelligence Research Specialists will be on-board by March 2003 (the one-year point).	December 2002	March 2003	

How We Will Know It Is Fixed: The FBI's analytical complement will be fully staffed and funded and analytical products will be disseminated to the Intelligence and Law Enforcement Communities on a routine basis.

U. S. DEPARTMENT OF JUSTICE

Management Challenge Report

Issue and Milestone Schedule

Management Challenge: DEPARTMENT OF JUSTICE REORGANIZATIONS	Date of Submission:	Component: Department FBI, OJP	Original Target for Completion:	Current Target for Completion: On-going

Issue and Description:

- MANAGING DEPARTMENT EMPLOYEES THROUGH ON-GOING REORGANIZATIONS AND/OR TRANSFERS

With the impending absorption of INS into the Department of Homeland Security the Department will be challenged to ensure that the vital missions of the INS, such as communication systems, information technology systems, human capital systems, and physical location of people and other assets, are not impeded during the transition period. Similar challenges will result if the Bureau of Alcohol, Tobacco and Firearms (BATF) is transferred to DOJ from the Department of the Treasury.

Additionally, FBI continues to reorganize to more effectively respond to its new priority to detect and deter acts of terrorism against U.S. interests and OJP is reorganizing in an attempt to improve its grant operations. The OIG is particularly concerned with OJP's efforts to create efficiencies and streamline operations.

What we did in FY 2002 / What are the Current Approaches:

INS: DOJ anticipates that Congress will pass legislation to create the Department of Homeland Security and is involved in ensuring that the transition of INS to DHS is smooth and accomplishes the President's goal of securing our nation and preventing further terrorist attacks. The expected impacts on Justice operations and human capital are enormous, and are requiring much sorting and negotiation. As plans crystallize, the human capital aspects of the transition must be monitored, reported, and addressed to ensure continuation of optimum service in key DOJ mission areas.

BATF: The proposed legislation to create the DHS includes a proposed amendment to transfer the enforcement (not revenue) functions of BATF to DOJ. This legislation is supported by the President, the Secretary of the Treasury, and the Attorney General. DOJ staff are working with Treasury and Congress to develop the specific elements and implications of the legislation, such as administrative management impacts and funding.

FBI: The FBI has completed several major steps in its ongoing reorganization. First, it established the positions of four Executive Assistant Directors (EADs) and organized Headquarters divisions and offices into branches headed by each of these EADs. These branches are Criminal Investigations, Counterterrorism/ Counterintelligence, Law Enforcement Services, and Administration. Second, the FBI created and fully staffed several new divisions: the Investigative Technologies Division and the Records Management Division. Other new divisions, as listed below, are still in the process of being fully staffed. Third, the FBI has dissolved the Investigative Services Division and reassigned its work to other entities. Finally, the FBI reallocated 518 field agents from criminal programs to counterterrorism training and security.

OJP: OJP is in the process of implementing the Department, OMB, and Congressionally-approved two-phase reorganization plan. The intent of this plan is to begin the process of transforming OJP into a centralized, more transparent organization accountable for managing a federal justice assistance program that rapidly responds to the field, focuses resources more effectively, and reduces confusion, overlap, and duplication. Furthermore, BJA began implementation of its reorganization, which included the realignment of DCPO and CPO staff/functions, along with other changes to streamline BJA operations and improve services to its customers. DCPO and CPO staff have been reassigned to BJA and all BJA staff completed a robust training program to assist them in the transition to new positions. Additionally, the Office of the Chief Information Officer (OCIO) was created as a separate administrative support office within OJP. The new Chief Information Officer is on board and staff/functions have been reassigned to OCIO.

Milestones FY 2003/FY2004:	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
INS: No milestones at this time.	N/A	N/A	N/A
BATF: No milestones at this time.	N/A	N/A	N/A
FBI:	--	--	--
-Establish and fully staff the Security Division	Continuing through 2003/2004		
-Establish and fully staff the Cyber Division	Continuing through 2003/2004		
-Reallocate field criminal agents to Counterintelligence (exact number is classified)	Pending review/approval by Congress FY 2003		
-Establish and fully staff the Office of Intelligence	Continuing through 2003/2004		
-Restructure the Counterterrorism Division	Continuing through 2003/2004		
OJP:	--	--	--
-Office of Communication created by restructuring and renaming the Office of Congressional and Public Affairs. (Director of the Office of Communication selected) -Tentative selection for Director of the Office of Communications submitted to the Department of Justice for review			8/16/02 9/2002
-Community Capacity Development Office (CCDO) reorganization will be established by realigning functions of the American Indian and Alaskan Native Desk and the Executive Office for Weed and Seed.		3/2003 (tentative)	
-Consolidate the Office of the Comptroller, Office of Budget and Management Services, Equal Employment Office, and Office of Administration		3/2003 (tentative)	

How We Will Know It Is Fixed:

Departmental reorganization will be complete.

RESPONSES TO FMFIA MATERIAL WEAKNESSES (NOT COVERED BY OIG TOP TEN MANAGEMENT CHALLENGES)

<table>
<tr><td colspan="4" rowspan="5"><b>U. S. DEPARTMENT OF JUSTICE</b>
<b>Corrective Action Report</b>
Issue and Milestone Schedule</td><td colspan="2"><b>Date of Submission</b></td></tr>
<tr><td colspan="2"><b>First Quarter Update:</b></td></tr>
<tr><td colspan="2"><b>Second Quarter Update:</b></td></tr>
<tr><td colspan="2"><b>Third Quarter Update:</b></td></tr>
<tr><td><b>End of Year Report:</b></td><td>10/21/02</td></tr>
<tr><td colspan="4"><b>Issue Title</b>
Prison Crowding</td><td><b>Issue ID</b>
1985-6201</td><td><b>Organization</b>
Bureau of Prisons</td></tr>
<tr><td><b>Date First Initiated</b>
1985</td><td><b>Original Target for Completion</b>
09/95</td><td><b>Current Target for Completion</b>
09/07</td><td><b>Actual Date of Completion</b></td><td colspan="2"><b>Issue Type (Organization Rating)</b>
Material Weakness</td></tr>
<tr><td colspan="3"><b>Source Title</b>
BOP</td><td><b>Date of Source Report</b>
1985</td><td colspan="2"><b>Issue Type (DOJ Rating)</b>
Material Weakness</td></tr>
</table>

Issue Description

In 1985 the Bureau's Executive Staff recognized crowding as a material weakness. The crowding rate grew through 1990 to a high of 69% over the Bureau's rated capacity. As of September 30, 2002, the crowding rate was 33% over rated capacity. The Bureau continues to rely on funding for contract beds and the construction of additional federal facilities to keep pace with a growing inmate population and to gradually reduce our crowding rate, thereby ensuring the manageable operation of the system.

The total Federal Prison Population was 163,436 as of September 30, 2002, reflecting an increase of 6,864 for FY 2002.

We project the total Bureau population will continue to grow and should reach 192,941 by September 30, 2007. Through the construction of new facilities and expansion projects at existing institutions, our Long Range Capacity Plan projects a rated capacity of 127,920 beds by September 30, 2007. Should new construction and expansion plans continue through FY 2007 as planned, crowding is projected to be 33% over the projected rated capacity.

What We Will Do About It

Increase the number of beds in the Bureau to keep pace with the projected increases in the federal inmate population. Efforts to reach this goal include expanding existing institutions, acquiring surplus properties for conversion to correctional facilities, constructing new institutions, utilizing contract facilities and expanding the use of contract beds, and exploring alternative options of confinement for appropriate cases.

Milestone C: The projections have changed since publication of the FY 2001 Federal Managers' Financial Integrity Act Corrective Action Reports (included as Appendix G in the FY 2001 Accountability Report). This is due to updated data from the Administrative Office of the U.S. Courts, which has indicated that, while the federal inmate population will continue to increase, the rate of growth will be somewhat slower. The decline in projected inmate population is a result of a reduction in both immigration and drug cases, as well as final absorption into the BOP of the District of Columbia sentenced felon population as mandated by the National Capital Revitalization Act of 1997.

Milestones	Original Target Date	Current Target Date	Actual Date of Completion
A. Completed Actions/Events As of September 30, 2002, the Bureau's population reached 137,527 and was being housed in capacity of 103,262, resulting in a crowding rate of 33%.	09/02		09/02
B. Short Term (10/02 - 10/03) Planning estimates call for a rated capacity of 107,463 to be reached by close of FY 2003. The crowding rate is projected to be 34% at that time, an increase of 1% for the year.	09/03		
C. Longer Term (10/03 and beyond)			
Focus the use of limited Community Corrections Center resources to provide relief, as appropriate, to facilities housing low and medium security inmates. The information below represents inmates housed in Bureau operated facilities.	09/93	09/03	
September 30, 2004 Inmate Population: 151,775 Rated Capacity: 115,941 Crowding Rate: 31%	09/04		
September 30, 2005 Inmate Population: 160,038 Rated Capacity: 121,294 Crowding Rate: 32%	09/05		
September 30, 2006 Inmate Population: 165,279 Rated Capacity: 124,624 Crowding Rate: 33%	09/06		
September 30, 2007 Inmate Population: 170,478 Rated Capacity: 127,920 Crowding Rate: 33%	09/07		

How We Will Know It Is Fixed

Results are measured as a new institution or expansion project is activated or contract beds are obtained and resulting increases in rated capacity are established. A corresponding decrease in the crowding percentage rate will also be a tangible measurement of the results. Progress on construction projects at new and existing facilities can be validated via on-site inspections of each facility or by review of monthly construction progress reports.

U. S. DEPARTMENT OF JUSTICE

Corrective Action Report

Issue and Milestone Schedule

Date of Submission	
First Quarter Update:	
Second Quarter Update:	
Third Quarter Update:	
End of Year Report:	12/23/02

Issue Title	Issue ID	Organization
FBI Property and Equipment		Federal Bureau of Investigation

Date First Initiated	Original Target for Completion	Current Target for Completion	Actual Date of Completion	Issue Type (Organization Rating)
08/02	03/03	03/03		Material Weakness

Source Title	Date of Source Report	Issue Type (DOJ Rating)
OIG Audit Report # 02-27	08/02	Material Weakness

Issue Description

Office of the Inspector General (OIG) Report # 02-27, "The Federal Bureau of Investigation's (FBI) Control Over Weapons and Laptop Computers," released in August 2002, revealed significant problems with the FBI's management of weapons and laptop computers. Although the number of functional weapons reported missing during the review period amounted to less than one-half of one percent of the FBI's inventory, the significance of these losses is measured in the sensitive nature of the missing property, not in numbers. Similarly, the number of laptops reported missing during this same period equated to only approximately two percent of the FBI's inventory. However, because the security level of 70 percent of the lost or stolen laptops was "unknown," the loss is potentially significant as the information contained on these laptops could compromise national security or jeopardize ongoing investigations.

What We Will Do About It

The FBI has been aware of this problem for some time and has, prior to the issuance of this report, taken the following actions to address the concern:

- The FBI created and implemented a new policy mandating the timely reporting of loss or theft of property to all appropriate entities; the policy was officially issued in August 2002.
- Form FD-500, Report of Lost or Stolen Property, has been revised to include the date of loss or theft, the date of entry to NCIC, and the name of the Property Custodian responsible for property oversight.
- The FBI implemented a new policy that all weapons and laptops will be inventoried annually using barcode technology.

- A new regulation has been implemented requiring all divisions to generate a monthly On-Order report to review new property that should be placed on the Property Management Application (PMA); all divisions have been reminded of the requirement to place all property on the PMA in a timely manner.
- A new Schedule of Delegated Disciplinary Offenses and a policy statement addressing property losses have been promulgated.
- A policy has been established regarding safeguarding property outside of FBI office space and has been included in the appropriate manuals.

In addition and in response to recommendations received from the OIG, the FBI will take further actions to address this problem, as indicated below.

Milestones	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
1. Implementation of Boards of Survey to review cases of employee negligence leading to loss or theft of property.	11/02	11/03	
2. Issuance of policy regarding employees' personal financial responsibility for lost or stolen property.	11/02	11/02	11/01/02
3. Completion of biennial inventory of accountable property.	03/03	03/03	
4. Revision of the Manual of Administrative Operations and Procedures (MAOP) to clarify processes for separating employees, including establishment of procedures for reimbursement for lost property.	10/02	12/02	10/25/02
5. Institution of policies and procedures on the acquisition, inventory, audit, turn-in, maintenance, decommission, sanitization, and destruction of information technology resources.	02/03	02/03	

How We Will Know It Is Fixed

The problem will be corrected when all of the above milestones have been completed and when the FBI is able to fully account for its recorded property, particularly sensitive property such as weapons and laptop computers.

U. S. DEPARTMENT OF JUSTICE

Corrective Action Report

Issue and Milestone Schedule

Date of Submission	
First Quarter Update:	
Second Quarter Update:	
Third Quarter Update:	
End of Year Report:	01/14/03

Issue Title	**Issue ID**	**Organization**
FBI Management of Information Technology		Federal Bureau of Investigation

Date First Initiated	**Original Target for Completion**	**Current Target for Completion**	**Actual Date of Completion**	**Issue Type (Organization Rating)**
2002	TBD			Material Weakness

Source Title	**Date of Source Report**	**Issue Type (DOJ Rating)**
OIG Audit Report 03-09: FBI’s Management of Information Technology Investments	12/02	Material Weakness

Issue Description

A December 2002 Office of Inspector General (OIG) audit report entitled, “Federal Bureau of Investigation’s (FBI) Management of Information Technology (IT) Investments,” stated that in the past the FBI has not given sufficient management attention to IT investments. As a result, the FBI has not fully implemented critical processes necessary for such management and has invested large sums of money on IT projects without assurance that these projects would meet intended goals.

What We Will Do About It

FBI management has recognized that its past methods to manage IT projects have been deficient, and recently has committed to changing those practices. In January 2002, the FBI developed a conceptual model for selecting, controlling, and evaluating IT investments. The model seeks to define a process that will promote a Bureau-wide perspective on IT investment management, so that only IT projects with the best probability of improving mission performance are selected. Further, the process is intended to provide the methods, structures, disciplines, and management framework that governs the way IT projects are controlled and evaluated.

Milestones	**Original Target Date**	**Current Target Date**	**Actual Date of Completion**
1. Develop full plan and implementation schedule to address and meet the weaknesses described in the OIG report.	TBD		

How We Will Know It Is Fixed

FBI IT projects will stay within budget and on schedule and result in successful program operations.