

This page intentionally left blank.

DEPARTMENTAL MANAGEMENT CHALLENGES

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 November, 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. Both of the full reports follow.

Department Of Justice

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT

Corrective Action Reports for FY 2003

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:	09/30/03
Issue Title Computer Security Implementation				Issue ID	Organization Department
Date First Initiated 10/01/02	Original Target for Completion 12/30/04	Current Target for Completion 06/30/04	Actual Date of Completion	Issue Type (Organization Rating) Program Material Weakness	
Source Title			Date of Source Report	Issue Type (DOJ Rating) Program Material Weakness	
<p>Issue Description</p> <p>Financial and Security Act audits and reviews conducted by the Department's Inspector General and independent verification and validation (IV&V) reviews, penetration testing, self assessments, and certifications and accreditations continue to identify weaknesses in both classified systems and sensitive but unclassified (SBU) systems. Specific concerns include issues 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 system access, the Department's OIG concluded that the vulnerabilities noted in those areas were most significant. The most common vulnerability was with security standards and procedures, and password and logon management. Due to insufficient common standards and inadequate Department oversight, components have been given broad abilities to implement controls and too much latitude in establishing system settings. Additionally, vulnerabilities identified are more voluminous in the Department's legacy networks and infrastructures.</p>					
<p>What We Will Do About It</p> <p>To address repeatable weaknesses in the Department's implementation of computer security controls, the Chief Information Officer (CIO) released the Department's Information Technology Strategic Plan in July 2002. The plan outlines how the Department is strengthening and refocusing its information technology (IT) program to meet the Department's new counterterrorism mission and support the achievement of its strategic goals. In May 2003, the CIO established a Deputy CIO position at the Senior Executive Service (SES) level for IT security with responsibility for ensuring the full implementation of the Department's IT security program to include all functions for policy and oversight. In addition, the CIO realigned resources within the CIO organization to increase the number of FTEs working on the Department's IT security program by over 100 percent. This Staff will ensure that component classified and SBU systems have implemented the appropriate IT security controls and shall be responsible for ensuring that components identify corrective plans of action and milestones when the security controls are not met and for monitoring of these corrective action plans.</p> <p>In the past year, the Department has made significant progress in strengthening the Department's IT security program and in implementing the requirements of the Federal Information Security Management Act (FISMA). These accomplishments include:</p> <ul style="list-style-type: none"> ▪ Establishment of a centralized IT security office, headed by a Deputy CIO at the SES level; ▪ Establishment of an IT Security Council and seven project teams with responsibility for developing IT security standards, policies, and test controls; ▪ Continued development of a public key infrastructure (PKI) capability to support enhanced authentication controls and strategic initiatives for information sharing; ▪ Implementation of a web-based security awareness training program for a large part of the Department; ▪ Continued refinement of a departmental system for tracking all IT security weaknesses and corrective actions; ▪ Developed the Department's Security Act Report, which includes individual assessments of over 200 systems; ▪ Awarded a contract for IV&V of component IT system security controls and initiating several tasks against the contract; ▪ Continued development of a security architecture as an integrated element of the Department's enterprise architecture; and ▪ Expanded development of policies and standards for IT security, based on FISMA and new standards identified by the National Institute of Standards and Technology. <p>FY 2003 End of Year Update</p> <p>Milestone 1: In May 2003, an IT Security Staff, managed by a Deputy CIO was established under the CIO with responsibility for IT security policy, implementation, and oversight for both classified and SBU systems. (Closed)</p> <p>Milestone 2: (Closed) 17 minimum IT security implementation standards were developed. The 17 align with the NSIT areas of technical, operational, and management controls.</p> <p>Milestone 3: In September 2003, the Department completed an IT security architecture that is integrated into the Department's enterprise architecture. The IT security architecture provides a security framework and structure to guide investments and systems in implementing IT security controls and provides for increased information sharing, security controls in boundary devices, network devices, and supports the Department's PKI architecture. (Closed)</p> <p>Milestone 4: On-going. (Revised date of completion.) The DOJ-wide PKI requirements have been developed. DOJ drafted a certificate policy that is closely aligned with the federal policy and the Federal Bridge Certificate Authority (FBCA). In May 2003, a contract was awarded for the design and implementation of a Department root certificate authority (CA) and an FBI subordinate CA. The Department's root CA and the first subordinate CA are expected to be operational in November 2003 and certificates will begin being issued to approximately 600 users during phase 1 in December 2003.</p> <p>Milestone 5: Ongoing. (Revised date.) Increase oversight and monitoring by enhancing and deploying to components a security control tool that tracks all known vulnerabilities, weaknesses, and corrective actions for both classified and SBU systems.</p>					

Milestone 6: Delayed implementation due to Union coordination and piloting. On March 28, 2003, the CIO sent a memo to all DOJ employees announcing implementation of the Web-based Computer Security Awareness Training (CSAT) program. (Closed.)

Milestone 7: Work is progressing. Implementation date has been accelerated.

Milestones	Original Target Date	Current Target Date	Actual Date of Completion
1. Establish a centralized Information Security Staff, reporting directly to the Department CIO, with responsibility for ensuring the appropriate security controls are implemented in the Department's classified and SBU systems.	12/02	01/03	01/03
2. Develop minimum IT security standards for implementation of security controls for the Department's classified and SBU systems. 12 standards have been identified.	01/03	01/03	01/03
3. 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.	09/03 (version 1.0)	09/03 (version 1.0)	09/03
4. Plan, design and deploy a Departmentwide PKI. Establish a Project Management Office to manage the program and to coordinate with component initiatives.	03/03 (PKI plan, design, and requirements) 12/03 (pilot) 12/04 (deployment)	03/03 (PKI plan, design, and requirements) 12/03 Phase 1 (deployment)	03/03
5. Increase oversight and monitoring by enhancing and deploying 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.	02/03 03/03	02/03 03/04 (revised)	01/03
6. Develop and begin implementing a Departmentwide (with the exception of the FBI) web-based security awareness training tool (CSAT).	01/03	04/15/03	03/28/03
7. Identify common solutions and automated tools to monitor security compliance of network and system parameters and identify vulnerabilities.	09/03 12/04 (implement)	02/04 (revised) 06/04 (implement)	
How We Will Know It Is Fixed			
By continuing to evolve the IT 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, provide for greater trust of the Department's systems, and further enable information sharing and collaboration.			

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:	10/31/03
Issue Title Management of Information Technology Investments			Issue ID	Organization Federal Bureau of Investigation	
Date First Initiated 2002	Original Target for Completion	Current Target for Completion 09/04	Actual Date of Completion	Issue Type (Organization Rating) Program Material Weakness	
Source Title OIG Audit Report 03-09			Date of Source Report 12/02	Issue Type (DOJ Rating) Program 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 In January 2002, the FBI began implementation of an IT investment management process as a part of the FBI's overall IT strategic management framework. To date, significant progress has been made toward creating a stronger foundation for IT management practices. Thirteen of 30 recommendations have been closed. The Department is working closely with the FBI to ensure the integration of the DOJ and FBI investment management processes and project oversight processes. Biweekly meetings are held between DOJ and the FBI on a broad range of major FBI IT issues, including the integration of the FBI IT investment management and oversight processes with the Department's processes. DOJ representatives attend the FBI project status briefings (i.e., project management reviews) which have been initiated to review the project status on major FBI IT projects. In addition, the Department is working with the FBI to ensure the alignment of its investment management and project oversight processes with the FBI's processes in the FBI's "Project Management Handbook" which outlines the FBI's IT investment management and project oversight processes.					
FY 2003 End of Year Update <p>Milestones 1, 10, 11: The documents were delivered in January 2003.</p> <p>Milestone 2: Document delivered during August 2003. OIG noted simplified investment management process (IMP) removes the need for specialized training.</p> <p>Milestone 3: Project Management Functional Overview completed during last quarter of FY2003. Project Management Handbook will be completed by December 2003. OIG noted this milestone will be closed when the Project Management Handbook is delivered to them for review.</p> <p>Milestone 4: The project management function is residing in the Information Resources Division rather than as a separate formal Congressionally -approved entity.</p> <p>Milestone 5: Policy for all projects with life cycle costs of \$10 million or greater is in place, but has not been implemented. Response showing project portfolio and projects with PMPs will be provided to the OIG in a November 2003 response.</p> <p>Milestone 6: IT asset inventory for the Information Resources Division has been completed and the OIG has closed the recommendation pertaining to completion and monitoring of the IT asset inventory. Additionally, the IT inventory assessment will begin no later than December 2004. After assessment, investment review boards will use the information as a decision-making tool. Other divisional IT assets will be inventoried and assessed over the remainder of FY 2004.</p> <p>Milestone 7: Document delivered during last quarter of FY2003. OIG noted it will close this recommendation when decision directives from project management and control gate reviews demonstrate key practices are regularly executed. The FBI expects to provide the OIG with feedback during November 2003.</p> <p>Milestone 8: Policies and procedures for identifying business needs and supporting documentation were delivered to the OIG. The OIG has closed this part of the milestone. Staff limitations have delayed the training element for this milestone. The FBI expects to have course outlines and presentation materials ready and begin holding classes for each division by December 2003.</p> <p>Milestone 9: IMP policy document delivered during August 2003 notes applicability of process and threshold to all funds.</p> <p>Milestone 12: IMP policy and procedures notes are required for architectural review. The OIG has closed this portion of the milestone. OIG expects further evidence of senior management sponsorship of all new projects and end-user involvement throughout the project life cycle. The Project Management Handbook will address these areas and is expected to be complete by November 2003.</p> <p>Milestone 13: The FBI's project management functional overview, along with IMP policy and procedures, describes the FBI's plan for IMP and system development life cycle (SDLC) methodology.</p> <p>Milestone 15: Baseline for Virtual Case File Delivery 1 established during September 2003. Releases 2 and 3 baselines are pending. Transportation Network Component/Information Presentation Component (TNC/IPC) revised baseline under discussion with FBI and contractor.</p> <p>Milestone 16: Technical requirements complete through Joint Application Development sessions. Documentation to OIG is expected during November 2003.</p>					

Milestone 17: Response to Criminal Justice Information Services (CJIS) Division review completed during July 2003. Response to other two reports delayed due to lack of staff. Staff assigned to complete response were detailed to the Terrorism Screening Center as of October 2003. Plan to complete responses is on hold until adequate resources are provided. In the interim, the FBI has completed and is following DOJ-sanctioned Trilogy risk management plan.

Milestone 18: New IMP requires feedback from all impacted entities before a project is approved.

Milestone 20: Contract to assist technical field staff awarded. Training for Microsoft Windows 2000 certification is ongoing. Since March 2001, 300 electronics technicians have received Trilogy-specific training. Classroom and web-based training for end-users has been offered. As of October 2003, 3,521 staff had been trained. VCF web-based training is under development. FBI Academy Learning Management System is operational and providing office software training to Trilogy users.

Milestone 22: Initial set of tools deployed into Enterprise Operations Center during the second quarter of FY2003. Additional tools will be delivered under Trilogy full site capability deployment.

Milestone 23: FBI has selected PureEdge eForms product to support both the existing macros and web-based forms, providing a standard format for all documents. The product will provide word processor features as well as digital signatures, email interfaces, and document management interfaces. FBI purchased licenses to create 75 eforms and has created 25 eforms to replace Word-Perfect macros.

Milestone 24: Assignment for this plan has not been delegated. Process will be tested for one entire budget cycle to determine if it is effective.

Milestones	Original Target Date	Current Target Date	Actual Date of Completion
1. Establishment of regularly scheduled meetings with standing agendas for the investment boards and of specific roles and responsibilities for each board member.	06/02	06/02	06/02
2. Establishment of education and training plans to ensure that board members acquire required core competencies.	03/03	12/03	08/03
3. Implementation of official project management guidance.	06/03	12/03	
4. Establishment and operation of a project management office.	06/03	09/03	n/a
5. Approval of a project management plan for each IT project by the Project Oversight Committee.	09/03	12/03	
6. Completion and consistent upkeep of the IT inventory and use of it by the boards as a decision-making tool.	06/03	09/04	09/03
7. Execution of key process activities necessary for the investment review boards to maintain effective oversight.	09/03	09/03	09/03
8. Establishment of and training on policies and procedures for identifying the business needs and users of IT projects.	09/03	12/03	
9. Application of IMP to all IT project proposals, including those funded through base funding.	09/03	09/03	07/03
10. Implementation of recommendations on expanding the policies and procedures set forth in the post-implementation review.	06/02	06/02	06/02
11. Incorporation of input from various ITIM users into the development and refinement of the control and evaluate phases.	08/02	08/02	08/02
12. Performance of a business architecture compliance review of IT proposals to ensure support of the Bureau's mission.	06/03	06/03	06/03
13. Implementation of a plan for integration of the IMP with a system development life-cycle methodology.	06/03	06/03	07/03
14. Development of the first phase of a comprehensive enterprise architecture and implementation of a maturation plan.	04/03	06/03	06/03
15. Establishment and monitoring of baselines for Trilogy.	03/03	01/04	
16. Definition and dissemination of the technical requirements for Trilogy's User Application Component.	03/03	09/03	
17. Preparation and monitoring of an action plan to address the risks identified by the three internal reports on Trilogy.	03/03	12/03	
18. Establishment of a process for future IT deployments wherein field offices can submit input and receive feedback from HQ.	06/03	06/03	06/03
19. Correction of Trilogy service support contractor deficiencies.	03/03	03/03	01/03

20. Resolution of outstanding issues related to the Trilogy on-line training system and a training plan specifically designed for IT specialists and electronic technicians.	09/03	09/03	
21. Delivery of remaining Extended Fast Track computers.	02/03	03/03	03/03
22. Procurement of trouble-shooting equipment for Trilogy.	03/03	03/03	03/03
23. Creation of a web-based replacement approach for WordPerfect macros.	06/04	06/04	
24. Integration of the IT strategic planning process, the IMP, and the performance goals in the Department IT plan.	09/04	09/04	

How We Will Know It Is Fixed

Addressing the recommendations assists the FBI in further maturing the IT Strategic Management Framework. The FBI's progress toward implementation will be measured against GAO's "ITIM Framework for Assessing and Improving Process Maturity." The FBI is working to integrate strategic planning, budgeting, enterprise architecture, investment management, and project management into an overall framework that meets GAO's guidelines, OMB direction, and DOJ policy in a manner that supports the FBI's mission.

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

U.S. DEPARTMENT OF JUSTICE Corrective Action Report Issue and Milestone Schedule					Date of Submission			
					First Quarter Update:			
					Second Quarter Update:		04/22/03	
					Third Quarter Update:			
					End of Year Report:			
Issue Title Prison Crowding				Issue ID 1985-6201	Organization Bureau of Prisons			
Date First Initiated 1985	Original Target for Completion 09/95	Current Target for Completion	Actual Date of Completion CLOSED	Issue Type (Organization Rating) Material Weakness				
Source Title BOP			Date of Source Report 1985	Issue Type (DOJ Rating) Material Weakness				
Issue Description <p>Note: The Department of Justice (DOJ) has reassessed Prison Crowding and has removed it from its list of material weaknesses. DOJ first reported Prison Crowding in 1985, and the crowding rate peaked at 69% over rated capacity in 1990. However, the crowding rate is now down to 33% over rated capacity, and the construction and budget plans continue to maintain that rate. The low incidents of escapes (0) from, and homicides (4) and assaults (4,000) in, prisons from FY 2002 through the present also support removing this from DOJ's list of material weaknesses. BOP recognizes that Prison Crowding is a serious management challenge and is constantly reviewing its processes and evaluating ways to better manage the prison population.</p> <p>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.</p> <p>The total Federal Prison Population was 163,436 as of September 30, 2002, reflecting an increase of 6,864 for FY 2002.</p> <p>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.</p>								
What We Will Do About It <p>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 exploring alternative options of confinement for appropriate cases.</p> <p>There will often be discrepancies between projected and actual numbers with this type of data due to the unpredictable environment in prisons. Plans are developed based on historical data, past experience, population projections, and best faith efforts to project for the future.</p>								
How We Will Know It Is Fixed <p>Results are measured as a new institution or expansion project is activated 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. Incidents of escapes, homicides, and assaults will be minimal.</p>								

U.S. DEPARTMENT OF JUSTICE Corrective Action Report Issue and Milestone Schedule				Date of Submission	
				First Quarter Update:	
				Second Quarter Update:	04/04/03
				Third Quarter Update:	
				End of Year Report:	
Issue Title			Issue ID	Organization	
Detention Space and Infrastructure			1989-6401	Office of Detention Trustee; U.S. Marshals Service; Immigration and Naturalization Service	
Date First Initiated	Original Target for Completion	Current Target for Completion	Actual Date of Completion	Issue Type (Organization Rating)	
09/30/89	09/30/92	01/30/03	CLOSED	Material Weakness	
Source Title			Date of Source Report	Issue Type (DOJ Rating)	
				Material Weakness	
Issue Description <p>Note: The Department of Justice (DOJ) has removed Detention Space and Infrastructure from its list of material weaknesses. DOJ has resolved all current material issues and has met all milestones. In addition, the Immigration and Naturalization Service (INS), a major factor in this issue, has been transferred from DOJ to the Department of Homeland Security. The Office of the Detention Trustee will continue to monitor use of detention space and will determine if any other material weaknesses arise in the future.</p> <p>Detention space for the United States Marshals Service (USMS) and the INS has been a management challenge since 1989. Both agencies are experiencing rapid growth in their use of detention space, from an average of 31,966 beds in 1996 to a projected 64,800 beds in 2003. (The actual number of detainees in the custody of the USMS and the INS on September 30, 2002, was 63,779.) The USMS is experiencing a shortage of detention space near federal court cities, resulting in the need to transport prisoners to other distant facilities, often in other states. The INS apprehends 1.6 million illegal aliens annually. The INS has some discretion on who it detains; however, because of statutory changes enacted by Congress in 1996, INS is required to detain certain aliens until their removal. This results in the detention of more aliens who previously could have been released on bond pending the outcome of their removal proceedings. Furthermore, it is the INS' experience that the vast majority of non-detained aliens do not appear for their removal hearings and/or do not surrender for removal after a final order of removal has been issued. Therefore, detention is an effective tool to ensure participation in removal proceedings and compliance with removal orders. This expanding need for detention space places increasingly heavy demands on the INS and USMS infrastructure, including transportation, buildings, communications equipment, and staff. This also increases concerns related to health and safety of detainees and USMS and INS employees.</p>					
What We Will Do About It <p>To deal with this multi-agency issue, the Department of Justice (Department) created a Detention Planning Committee which, in turn, developed a multi-year Federal Detention Plan. The Department worked with the USMS, INS, and the Bureau of Prisons to update this plan in February 2000. In addition, the Department appointed a Detention Trustee in FY 2001 and established the Office of the Detention Trustee (ODT). The Detention Trustee is now responsible for oversight and management of many multi-agency issues related to detention.</p> <p>The USMS will maintain and expand the use of state and local jail space through the use of Interagency Agreements (IGAs), the Cooperative Agreement Program, and the recently expanded contract authority for service contracts for contract beds.</p> <p>Previously, the USMS planned to establish detention management and oversight positions at contractjails housing 200 or more USMS prisoners (this plan was identified as milestone #4 in previous reports). ODT supported this plan, in keeping with the stated office mission. At this time, ODT does not have the authority to request employees on behalf of USMS to further this goal. ODT is in the process of changing the current policy so that ODT employees can perform this function in detention facilities identified by USMS. Until the current policy has been changed, this plan has been tabled until manpower and resources become available. ODT has completed conditions of confinement reviews of 40 facilities. Additional funding for conditions of confinement reviews was requested for FY 2003.</p> <p>The INS will pursue alternatives to detention and less restrictive detention options in the coming years. INS is committed to ensuring that, to the greatest extent possible, detained aliens are placed in facilities appropriate to their background and circumstance. INS will continue to review the management of the Detention and Removal Program via the INS Program for Excellence and Comprehensive Tracking (INSpect) and through the newly created Operations Analysis, Training, and Compliance Division. The scope of the review includes facility issues, security and control, detainee conduct and detainee services, transportation and escort, and docket control.</p> <p>Regarding milestone #3, INS has created a robust detention bed space projection model, in conjunction with an experienced Department contractor. This model will help INS manage resources and forecast bed space requirements. The model is district based and will assist the INS in the justification of needed staff, budget, and construction requests. These efforts will contribute to the Departmentwide model.</p> <p>Regarding milestone #4, the prior target completion date of January 30, 2003, was based on the projected passage of the FY 2003 budget, which did not occur until February 20, 2003. Since passage, ODT has formed a team of experts to develop a plan to evaluate the health and safety of federal prisoners in non-federal institutions. Additionally, ODT has established cross-organizational working groups for detention services acquisition, budget and resources, and detention programs.</p> <p>Regarding milestone #5, the baseline report and needs assessment was completed in May and was submitted to OMB on 06/30/02; however, submission to Congress was delayed due to publishing issues after departmental review.</p>					

Milestones	Original Target Date	Current Target Date	Actual Date of Completion
1. Establish a Detention Trustee.	09/30/01	09/30/01	09/30/01
2. Expand the current 5-year contract authority for Service Contracts. (Public Law 106-553)	09/30/99	11/30/00	12/21/00
3. Create a more encompassing model for projecting detainee population. (INS)	05/30/01	05/30/01	07/30/01
4. (Previously milestone 5). Establish an oversight team to handle privatization issues and private jail contracts. (ODT)	11/30/99	01/30/03	03/19/03
5. (Previously milestone 6). Complete a needs assessment and develop a baseline report. (ODT)	05/05/02	05/05/02	07/30/02

How We Will Know It Is Fixed

- (1) There will be sufficient bed space capacity to house criminal defendants and illegal aliens in each federal court city (including EOIR locations) without unwarranted transportation by the USMS and INS.
- (2) There will be consolidated detention planning that ensures that detention bed space is acquired in a cost-efficient manner that leverages the combined needs of the USMS and INS.
- (3) A data system will be established that identifies available bed space for use by federal law enforcement, particularly the USMS and INS.
- (4) Implementation of national standards that are applicable to all space providers and achievement of a high level of compliance with those standards.

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:	10/31/03
Issue Title Property and Equipment			Issue ID	Organization Federal Bureau of Investigation	
Date First Initiated 08/02	Original Target for Completion Spring 03	Current Target for Completion	Actual Date of Completion 09/03 CLOSED	Issue Type (Organization Rating) Program Material Weakness	
Source Title OIG Audit Report # 02-27		Date of Source Report 08/02	Issue Type (DOJ Rating) Program Material Weakness		
Issue Description <p>This issue is CLOSED, pending concurrence of the San Francisco Regional Audit Office (SFRAO)/OIG.</p> <p>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.</p>					
What We Will Do About It <p>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:</p> <ul style="list-style-type: none"> ▪ 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. <p>In addition and in response to recommendations received from the OIG, the FBI will take further actions to address this problem, as indicated below.</p>					
FY 2003 End of Year Update <p>Milestone 1: The FBI will NOT implement Boards of Survey. The Office of Professional Responsibility (OPR) has established procedures and disciplinary schedules for these matters. The FBI's Property Management Unit (PMU) will review all lost/stolen reports for capitalized assets and refer gross negligence to OPR. These procedures have been approved by the Assistant Director of Property Management at DOJ.</p> <p>Milestone 3: Due to earlier delays in the arrival of, and training on, barcode tracking system software, this date has slipped slightly. However, the FBI completed the inventory in September 2003.</p> <p>Milestone 4: The revision to clarify processes for separating employees was submitted to Records Management on 10/25/02. The Director's memo regarding the financial liability for lost property was distributed on 11/01/02.</p> <p>Milestone 5: The FBI has in place policies and procedures for the acquisition, inventory, audit, turn-in, maintenance, decommission, sanitization, and destruction of information technology resources (Manual of Investigative Operations and Guidelines (MIOG) Part II, Section 35-13). The FBI's Security Division purchased an enterprise license for sanitizing hard drives. However, due to the events of 9/11/01, the national Security Agency has suspended agencies from destroying and wiping hard drives clean.</p>					
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	n/a	n/a
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.			Spring 03	09/03	09/03/03

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	09/03
<p>How We Will Know It Is Fixed</p> <p>This problem will be corrected when all of the above milestones have been completed and the FBI is able to account fully for its recorded property, particularly sensitive property such as weapons and laptop computers. DOJ will consider this problem officially corrected when the SFRAO/OIG removes it as a material weakness from audit report 02-27, "The FBI's Control Over Weapons and Laptop Computers." SFRAO anticipates completing the follow-up to the audit report by May 2004.</p>			

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:		11/19/03	
Issue Title DOJ Financial Systems Compliance			Issue ID	Organization Department of Justice			
Date First Initiated 02/28/01	Original Target for Completion On-going	Current Target for Completion On-going	Actual Date of Completion	Issue Type (Organization Rating) Financial System Material Weakness			
Source Title Management Review and Annual Financial Statement Audits			Date of Source Report 11/30/01	Issue Type (DOJ Rating) Financial System Material Weakness			
Issue Description <p>The Department of Justice (Department) audit report on the FY 2000 consolidated financial statements identified the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), United States Marshals Service (USMS), and Federal Prisons Industries (FPI) as not meeting federal accounting standards or systems requirements, and having material weaknesses in system controls/security. For DOJ as a whole, the need to address weaknesses cited in the financial statement audits, nonconformances with Office of Management and Budget (OMB) Circular No. A-127, technological changes, and the need to better support critical financial operations and agency programs contribute to the necessity to modernize the Department's financial systems and improve internal controls.</p> <p>The FBI operates a legacy system which significantly limits the capabilities necessary to support the effective and efficient processing of financial management information throughout the Bureau. The USMS implemented a new financial management system in 1998 at its headquarters office. However, due to implementation difficulties, the USMS did not migrate its district offices to the system.</p>							
What We Will Do About It <p>The Department identified a unified core financial system as one of the ten goals for revamping the Department's management. The unified core system will be a commercial off-the-shelf (COTS) Financial Management System product(s) certified by the Joint Financial Management Improvement Program as meeting core federal financial management system requirements.</p>							
FY 2003 End of Year Update <p>Milestone 2: Develop consolidated functional and technical requirements for the unified core system, along with a procurement module, for issuance of a solicitation to procure a COTS solution. The COTS solicitation was issued on February 14, 2003.</p> <p>Milestone 3: Develop consolidated requirements for Integration and Implementation (I&I) for issuance of the draft solicitation. This milestone has been modified to reflect a change in acquisition strategy. A draft solicitation was issued to obtain comments from industry regarding our I&I requirements and approach. The release date for the I&I solicitation will coincide with the issuance of the COTS software contract.</p> <p>Milestone 4: Receive the COTS proposals. A Departmentwide Technical Evaluation Panel is in the process of evaluating the vendors' COTS proposals for the software. The target date of award has changed due to an extended period of COTS software evaluation which directly impacts timing of product acceptance test, the issuance of the I&I RFQ and the award of the I&I contract.</p> <p>Milestone 5: Issue final I&I solicitation package identifying the selected COTS product. Milestone reflects modification to approach as reflected in Milestone 3. Final I&I solicitation package will be issued immediately following award of COTS contract. The target date has changed due to extended period of COTS software evaluation which directly impacts timing of product acceptance test, I&I RFQ issuance, and the I&I contract award.</p> <p>Milestone 6: Receive, evaluate, and award the I&I contract. The target date has changed due to the extended period of COTS software evaluation which directly impacts the timing of the issuance of the I&I RFQ and the award of the I&I contract.</p> <p>Milestone 7: Develop and conduct COTS acceptance testing with full DOJ pilot simulation. The Product Acceptance Testing (PAT) scenarios have been developed with Departmentwide input. However, the target date has changed due to the extended period of COTS software evaluation which directly affects this activity.</p> <p>Milestone 8: Initial implementation of COTS software for UFMS for designated program/component will begin during the 4th quarter of FY 2004.</p> <p>Milestone 9: Components reported as not meeting federal accounting standards or systems requirements and having material weaknesses in system controls/security will implement compensating internal controls and financial system improvements to effect substantial compliance with the Federal Financial Management Improvement Act (FFMIA) by June 30, 2004.</p>							
Milestones			Original Target Date	Current Target Date	Actual Date of Completion		
1. Planning phase, including milestones.			05/30/02	08/15/02	08/15/02		
2. Develop requirements for issuance of COTS solicitation.			02/21/03	02/21/03	02/14/03		
3. Develop requirements for issuance of draft I&I solicitation.			03/27/03	04/15/03	04/15/03		
4. Receive/evaluate/award contract for COTS software.			05/30/03	2 nd Q/FY04			

5. Issue final I&I solicitation.	06/03/03	2 nd Q/FY04	
6. Receive/evaluate/award contract for I&I contractor.	08/29/03	3 rd Q/FY04	
7. Develop/conduct COTS acceptance testing.	10/17/03	2 nd - 3 rd Q/ FY04	
8. Begin initial implementation of COTS UFMS software.	10/01/04	4 th Q/FY04	
9. Bring systems into substantial compliance with FFMA.	04/01/03	3 rd Q/FY04	
<p>How We Will Know It Is Fixed Modern financial systems that comply with federal financial system requirements will be implemented, and system dependent audit recommendations will be closed.</p>			

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:		1/15/04
Issue Title DOJ Accounting Standards Compliance			Issue ID	Organization Department of Justice		
Date First Initiated 12/19/02	Original Target for Completion 09/30/03	Current Target for Completion 06/30/04	Actual Date of Completion	Issue Type (Organization Rating) Financial System Material Weakness		
Source Title FY 2002/FY 2003 Integrity Act Review and Financial Statement Audit Report		Date of Source Report FY 2002/FY 2003		Issue Type (DOJ Rating) Financial System Material Weakness		
Issue Description <p>The financial statement audit reports advised of material weaknesses in compliance with certain federal accounting standards by the Federal Bureau of Investigation (FBI); Offices, Boards, and Divisions (OBDs); Working Capital Fund (WCF); U.S. Marshals Service (USMS); and Asset Forfeiture Fund (AFF). Findings involve weaknesses in business processes and financial transaction recording and report, including seized asset accounting.</p>						
What We Will Do About It <p>For the OBDs and WCF, the Justice Management Division (JMD) will revise procedures and provide guidance and training to those processing obligation and revenue data. The FBI is hiring additional staff for its financial statement preparation process and has will revise its procedures for recording financial transactions and property data. The USMS will improve its business processes, procedures, and reporting practices. The AFF will enhance its monitoring and training processes and establish additional procedures to improve control over transaction processing and reporting.</p> <p>Milestone 1: Four of the eleven applicants selected through the preliminary process met the employee background requirements. The FBI solicited for additional accountant applicants during October 2003, to fill the remaining vacancies.</p> <p>Milestone 2: The FBI enhanced certain procedures. However, the audit revealed that additional enhancements are necessary.</p> <p>Milestone 3: Training and enhancing procedures were heavy areas of emphasis during FY 2003 and will continue during FY 2004.</p>						
Milestones			Original Target Date	Current Target Date	Actual Date of Completion	
1. The FBI will hire additional staff for financial statement reporting process.			06/30/03	03/01/04		
2. The FBI will revise its procedures for recording financial transactions and property data.			09/30/03	09/30/03	09/30/03	
3. The JMD will revise its procedures and provide guidance and training to those processing data for the OBDs and WCF.			09/30/03	06/30/04		
4. The USMS will improve its business process, procedures, and reporting practices.			06/30/04			
5. The AFF will enhance its monitoring and training processes and establish additional procedures to improve control over transaction processing and reporting.			06/30/04			
How We Will Know It Is Fixed <p>Management evaluation of these issues will be supported by audit review.</p>						

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:		11/19/03					
Issue Title FPI Adherence to Accounting Standards and Financial Management System Requirements				Issue ID 2000-6296	Organization Federal Prison Industries		
Date First Initiated 12/05/00	Original Target for Completion 03/01/01	Current Target for Completion 09/30/03	Actual Date of Completion 09/30/03 (CLOSED)	Issue Type (Organization Rating) Financial System Material Weakness			
Source Title FY 2000 Integrity Act Review <i>and</i> FY 2002 Financial Statement Audit			Date of Source Report 12/05/00 <i>and</i> FY 2002 reports	Issue Type (DOJ Rating) Financial System Material Weakness			
Issue Description This issue is CLOSED, pending concurrence of auditors. In May 2000, the Federal Prison Industries (FPI) implemented Millennium, which does not yet meet all the financial management requirements of Office of Management and Budget (OMB) Circular No. A-127. System generated reports require thorough review, analysis, and frequent corrections. FPI has weaknesses in system security, and weaknesses were reported in controls over inventories and accounts receivable, as well as in the financial statement preparation process.							
What We Will Do About It The FPI is working with its contractors to correct weaknesses in inventories, accounts receivables, and the financial statement reporting process. Substantial progress has been made in these areas. FPI will implement policies and procedures to improve risk assessment/system security management.							
Milestones				Original Target Date	Current Target Date	Actual Date of Completion	
1. Obtain system security certification.				12/31/00	12/31/00	12/31/00	
2. Obtain system security accreditation.				03/01/01	03/01/01	06/30/01	
3. Modify system procedures to comply with federal financial management requirements. Implement policies and procedures to improve risk assessment/system security management, including procedures for granting system access and providing employee security awareness training.				03/01/01	09/30/03	09/30/03	
4. Correct weaknesses in control over inventories.				03/15/02	01/31/03	12/13/02	
5. Correct weaknesses in control over accounts receivable.				03/15/02	01/31/03	12/13/02	
6. Refine financial statement reporting process.				03/15/02	01/31/03	12/13/02	
How We Will Know It Is Fixed Minimal errors will be found in accounting processing, recording, and reporting. FPI has received system security certification and accreditation. Management's evaluation of this issue will be verified by the FY 2003 financial statement audit.							

INSPECTOR GENERAL'S LIST OF THE MOST SERIOUS MANAGEMENT CHALLENGES AND RESPONSES



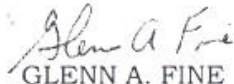
U.S. Department of Justice
Office of the Inspector General

Washington, D.C. 20530

November 5, 2003

MEMORANDUM FOR THE ATTORNEY GENERAL
THE ACTING DEPUTY ATTORNEY GENERAL

FROM:


GLENN A. FINE
INSPECTOR GENERAL

SUBJECT: Top Management Challenges

Attached to this memorandum is the Office of the Inspector General's (OIG) 2003 list of top management challenges facing the Department of Justice (Department). We have prepared similar lists since 1998, initially in response to Congressional requests. By statute, this list is now required to be included in the Department's annual Performance and Accountability Report.

The challenges are not presented in order of priority – we believe that all are critical management issues facing the Department. However, as with last year's list, it is clear to us that the top challenge facing the Department is its ongoing response to the threat of terrorism. Several other top challenges are closely related to and impact directly on the Department's counterterrorism efforts.

Eight of the challenges from last year's list remain. They are long-standing, difficult challenges that will not be solved quickly or easily. Two challenges from last year's list have been removed and replaced by two other challenges. We removed "Detention Space" because the responsibility for obtaining adequate and cost-efficient detention space for many immigration detainees has been transferred to the Department of Homeland Security, which now must address this difficult challenge. We also have removed "Department of Justice Reorganizations" from the list because a large part of that challenge was accomplished by the Department when it smoothly assimilated the Bureau of Alcohol, Tobacco, Firearms and Explosives into the Department while transferring the Immigration and Naturalization Service out of the Department.

In their place, we have added two new challenges: “Reducing the Supply of and Demand for Illegal Drugs” and “Security of Classified Information and Critical Infrastructure.” The first is a critical issue for the Department – to reduce the supply of illegal drugs coming into this country, the diversion of legal drugs for illicit use, and the demand for drugs. These multi-faceted problems have an enormous impact on law enforcement, health, and social issues in this country.

The other new challenge, “Security of Classified Information and Critical Infrastructure,” is related to but different from the counterterrorism challenge. Maintaining the security of classified information, while at the same time ensuring that such information is shared appropriately among law enforcement and intelligence agencies that have a need to know, is a difficult but critical task for the Department, particularly after the September 11 terrorist attacks.

We hope that this list and the accompanying analysis will assist Department managers in developing strategies to address the top management challenges facing the Department. We look forward to continuing to work with the Department to address these important issues.

Attachment

Top Management Challenges in the Department of Justice: 2003

1. Counterterrorism: The Department's top priority is preventing, detecting, and deterring future terrorist acts. Creation of the Department of Homeland Security (DHS) and the resulting shift of the Immigration and Naturalization Service (INS) to the DHS were only two aspects of extraordinary government-wide efforts during the past year to address this challenge.

Within the Department, the focus on counterterrorism has been clearly articulated and consistently stressed. The Department's Strategic Plan for 2001-2006 makes clear this is the top priority and notes the challenges facing the Department as it seeks to effectively manage its counterterrorism programs while coordinating with other intelligence agencies and law enforcement entities, both federal and local. In addition, the infusion of billions of dollars to help fund the Department's expanded counterterrorism efforts require managers to ensure that these funds are spent in an effective manner.

For its part, the OIG continues to audit and evaluate Department programs and operations that relate to counterterrorism and follow up on previous reviews to ensure that Department components take timely actions and address identified deficiencies. For example, in September 2002 the OIG issued an audit (OIG Report #02-38) that assessed the FBI's management of aspects of its counterterrorism program from 1995 through April 2002. The OIG review found that the FBI had never performed a formal comprehensive assessment of the risk of the terrorist threat facing the United States. We concluded that such an assessment would be 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 had developed an elaborate, multilayered strategic planning system, the FBI did not perform and incorporate into its planning system a comprehensive assessment of the threat of terrorist attacks on United States soil.

Since our audit was issued, the FBI has issued its national-level threat and risk assessment, which includes to some extent an assessment of the chemical and biological agents most likely to be used in a terrorist attack. We recommended that the FBI separately assess the threat and risk of all categories of weapons of mass destruction using intelligence information and

a multidisciplinary team of subject-matter experts. To date, the FBI has not fully complied with our recommendation but has made progress recently by completing a draft of a separate threat assessment of chemical and biological agents. In addition, the FBI reports that it has improved its hiring and use of intelligence analysts, and we are evaluating this issue as part of an ongoing audit. The FBI also reports that it nearly has completed revising its strategic plan, in accordance with our recommendation, which is intended to conform to the Department's strategic plan and its emphasis on preventing terrorism. As part of our follow-up work on these issues, we will review the FBI's updated strategic plan when it is completed.

The FBI also reported that it continues its efforts to close the gap between counterterrorism planning and operations through performance measures and standards and by holding managers accountable. All FBI divisions are now required to submit annual program plans with specific measures that will be used to gauge both program and field office performance. Once the plans are final, the FBI will develop a complete set of performance measures. During fiscal year (FY) 2004, the FBI intends to establish an integrated management system that more clearly links planning, performance, and accountability. We will continue to monitor these efforts.

While the Department appropriately is focusing significant efforts and resources to prevent acts of terrorism, its attention also is needed to prepare to respond to terrorist acts and other critical incidents should they occur. In 1996, the Department implemented the Crisis Management Coordinator Program (CMC Program), under which each United States Attorney's Office (USAO) was directed to designate a Crisis Management Coordinator to develop a critical incident response plan (Plan) and make other preparations to ensure that the USAOs were ready to respond to a critical incident, including acts of terrorism or natural disasters. To assess the Department's implementation of the CMC Program, the OIG is examining whether the USAOs have acted to improve their ability to respond quickly and appropriately to critical incidents by developing comprehensive plans and by training staff to carry out those plans. Our findings indicate that most USAOs have not fully implemented effective response plans.

In a separate ongoing review, the OIG is examining a variety of terrorism-related task forces to determine how their law enforcement and intelligence functions support the Department's efforts to detect, deter, and disrupt terrorism. Specifically, this review is evaluating the purpose, priorities, accomplishments, and functioning of the Anti-Terrorism Task Forces (ATTF), the FBI's Joint Terrorism Task Forces and Foreign Terrorist Tracking Task Force, and the Deputy Attorney General's National Security Coordination Council.

Because the FBI plays such a central role in the Department's counterterrorism strategy, the OIG continues to expend significant resources to review FBI programs and operations, many of which affect its counterterrorism missions. For example, in September 2003, the OIG released an audit of the FBI's Casework and Human Resource Allocation (OIG Report #03-37). In summary, this review found that prior to the September 11, 2001, terrorist attacks the FBI devoted significantly more special agent resources to traditional law enforcement activities, such as white-collar crime, organized crime, drugs, and violent crime, than it did to terrorism-related programs. The OIG is following up on this audit with an examination of the FBI's efforts to reprioritize and refocus its investigative resources on counterterrorism-related issues in the aftermath of the September 11 terrorist attacks. In this review, the OIG will seek to identify the operational changes in the FBI resulting from this reprioritization effort, including the types of offenses that the FBI is no longer investigating at pre-September 11 levels. We plan to survey federal, state, and local law enforcement agencies regarding the impact on their operations of the FBI's reprioritization.

Two additional ongoing OIG reviews focus on the FBI's efforts to meet other aspects of its varied counterterrorism-related challenges. First, because much information relevant to counterterrorism and counterintelligence is in languages other than English, the OIG is examining the extent and causes of FBI translation backlogs and the FBI's efforts to hire additional translators. This review will evaluate whether FBI procedures ensure appropriate prioritization of translation work, accurate and timely translations of pertinent information, and proper security of sensitive information.

Second, the OIG is reviewing the FBI's hiring and training of intelligence analysts and reports officers. Our 2002 counterterrorism audit identified concerns about the FBI's intelligence capability and recommended that the agency improve its intelligence analysis capabilities. The current audit is evaluating how effectively the FBI recruits and trains the various categories of intelligence analysts and reports officers in support of the FBI's counterterrorism mission. Looking ahead, the OIG plans to examine additional facets of the FBI's counterterrorism initiatives, including its role in conducting counterterrorism exercises.

As noted above, the reprioritization of the Department's counterterrorism priority has resulted in significantly increased Department funding for counterterrorism efforts. A challenge for the Department is to ensure that the increased funding is used economically, effectively, and for its intended purposes. In one review completed this year, the OIG conducted a follow-up

audit of the Department's Counterterrorism Fund (Fund), which was created by Congress in 1995 after the bombing of the Murrah Federal Building in Oklahoma City, Oklahoma, to assist Department components with the unanticipated costs of responding to and preventing acts of terrorism. Since its creation, Congress has appropriated more than \$360 million to the Fund. Originally established to provide reimbursement solely to Department components, since 1996 more than \$167 million from the Fund has supported counterterrorism initiatives of non-Department agencies, including other federal agencies and state and local governments. Past terrorism events for which Department components received reimbursement include the Oklahoma City bombing, the U.S. embassy bombings in Africa, and the September 11, 2001, terrorist attacks.

The OIG's follow-up audit (OIG Report #03-33) reviewed Fund expenditures from 1998 through 2002 and found that the Department's Justice Management Division (JMD), the entity that administers the Fund, has improved its management of the Fund since the OIG's original audit in 1999. However, the follow-up audit recommended that JMD implement additional improvements to the claims review process to ensure that adequate resources are available for emergency situations resulting from acts of terrorism. We also tested more than \$38 million in Fund expenditures during the audit and identified over \$3 million in questioned costs. These costs included expenses unrelated to approved counterterrorism initiatives, expenses for which the component could not provide supporting documentation, and expenses that were denied or billed erroneously.

A somewhat different but related challenge for the Department in responding to the heightened terrorism threat is to use its law enforcement and intelligence-gathering authorities without inappropriately affecting the civil rights and civil liberties of individuals. Section 1001 of the USA PATRIOT Act (Patriot Act) directs the Department's Inspector General to "receive and review" allegations of civil rights and civil liberties abuses by Department employees and report to Congress every six months about these responsibilities under Section 1001.

In furtherance of its responsibilities under Section 1001, the OIG issued a special report on June 2, 2003, that examined the treatment of 762 aliens held on immigration charges in connection with the investigation of the September 11 terrorist attacks. The OIG examined the treatment of these detainees, including their processing, bond decisions, the timing of their removal from the United States or their release from custody, their access to counsel, and their conditions of confinement. The OIG's 198-page report focused in particular on detainees held at the BOP's Metropolitan Detention Center (MDC) in Brooklyn, New York, and at the Passaic County Jail

(Passaic) in Paterson, New Jersey, a county facility under contract with the INS to house federal immigration detainees.

As our report pointed out, the Department was faced with unprecedented challenges responding to the attacks, including the chaos caused by the attacks and the possibility of follow-up attacks. Yet, while recognizing these difficulties and challenges, we found significant problems in the way the Department handled the September 11 detainees. Among the report's findings:

- The FBI in New York City made little attempt to distinguish between aliens who were subjects of its terrorism investigation (called "PENTTBOM") and those encountered coincidentally to a PENTTBOM lead. The OIG concluded that even in the chaotic aftermath of the September 11 attacks, the FBI should have expended more effort to distinguish between aliens who it actually suspected of having a connection to terrorism from those aliens who, while possibly guilty of violating federal immigration law, had no connection to terrorism but simply were encountered in connection with a PENTTBOM lead.
- The INS did not consistently serve the September 11 detainees with notice of the charges under which they were being held within the INS's stated goal of 72 hours. The review found that some detainees did not receive these charging documents for weeks – in some instances not for more than a month – after being arrested. These delays affected the detainees' ability to understand why they were being held, to obtain legal counsel, and to request a bond hearing.
- The Department instituted a policy that all aliens in whom the FBI had an interest in connection with the PENTTBOM investigation required clearance by the FBI of any connection to terrorism before they could be removed or released. The policy was based on the belief – which turned out to be erroneous – that the FBI's clearance process would proceed quickly. The OIG review found that instead of taking a few days as anticipated, the FBI clearance process took an average of 80 days, primarily because it was understaffed and not given sufficient priority by the FBI.
- In the first 11 months after the terrorist attacks, 84 September 11 detainees were housed at the MDC in Brooklyn under highly restrictive conditions. These conditions included "lock down" for at least 23 hours a day; escort procedures that included a "four-man hold" with handcuffs, leg irons, and heavy chains when the detainees were moved outside their

cells; and a limit of one legal telephone call a week and one social call a month.

- BOP officials imposed a communications blackout for September 11 detainees immediately after the terrorist attacks that lasted several weeks. After the blackout ended, the MDC's designation of the September 11 detainees as "Witness Security" inmates frustrated efforts by detainees' attorneys, families, and even law enforcement officials to determine where the detainees were being held. We found MDC staff frequently – and mistakenly – told people who inquired about a specific detainee that the detainee was not held at the facility when, in fact, the opposite was true.
- With regard to allegations of abuse at the MDC, the evidence indicated physical and verbal abuse by some correctional officers against some detainees, particularly during the first months after the attacks and during intake and movement of prisoners. Although the allegations of abuse have been declined for criminal prosecution, the OIG is continuing to investigate these matters administratively.
- By contrast, the OIG review found the detainees confined at Passaic had much different, and significantly less harsh, experiences than the MDC detainees did. Passaic detainees housed in the general population were treated like "regular" INS detainees who also were held at the facility. Although we received some allegations of physical and verbal abuse, we did not find the evidence indicated a pattern of abuse at Passaic.

The OIG report made 21 recommendations to the FBI, BOP, and the DHS's Bureau of Immigration and Customs Enforcement. The recommendations dealt with issues such as developing uniform arrest and detainee classification policies, improving information-sharing among federal agencies on detainee issues, improving the FBI clearance process, clarifying procedures for processing detainee cases, revising BOP procedures for confining aliens arrested on immigration charges who are suspected of having ties to terrorism, and improving oversight of detainees housed in contract facilities. The OIG has received and analyzed responses to the recommendations, and has requested additional information on some of the recommendations. In general, we found that the agencies agreed with the recommendations and are taking steps to implement them.

Finally, in addition to directing the Inspector General to receive and review allegations of civil rights and civil liberties abuses by Department employees, Section 1001 of the Patriot Act directs the OIG to publicize how people can contact the OIG to file a complaint and requires the OIG to submit a

semiannual report to Congress discussing its implementation of these responsibilities. In July 2003, the OIG issued its third Section 1001 report summarizing its activities from December 16, 2002, through June 15, 2003. The report described the status of OIG and Department investigations of alleged civil rights and civil liberties abuses by Department employees. In addition, the report highlighted several OIG reviews undertaken in furtherance of its Section 1001 responsibilities.

In the year ahead, the OIG will continue to evaluate how effectively the Department is meeting aspects of its varied counterterrorism challenge through OIG audits, inspections, and special reviews, as well as through the OIG's semiannual reports to Congress required under Section 1001 of the Patriot Act.

2. Sharing of Intelligence and Law Enforcement Information: Immediately after the September 11 terrorist 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. In October 2001, the President signed the 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. It also attempts to break down the wall which prevents the sharing of intelligence information with law enforcement officers.

Since then, the Attorney General, the FBI Director, Members of Congress, the Secretary of DHS, and other officials have consistently and repeatedly stressed the critical importance of sharing information to help prevent future acts of terrorism. This is a difficult challenge, given the multitude of federal and state entities that have or need access to intelligence and law enforcement information as well as the sensitive nature of much of the information. Even within the Department, getting information to the right individuals and entities so that they can use it effectively is an ongoing challenge. But the Department's ability to share law enforcement and intelligence information is critical to its capacity – and the capacity of other federal, state, and local governments – to prevent, mitigate, and respond to terrorist attacks. Moreover, while emphasizing timely sharing of intelligence and law enforcement information, the Department has to balance that with maintaining the security of sensitive information and limiting that information to those with a “need to know,” as we discuss below in management challenge 9.

In a review that reflected the importance of sharing intelligence and law enforcement information, in December 2002 the Senate Select Committee on

Intelligence and the House Permanent Select Committee on Intelligence released the results of its Joint Inquiry into the activities of the U.S. Intelligence Community in connection with the September 11 terrorist attacks. The 832-page report, much of it declassified and publicly released in July 2003, presents the Joint Inquiry's findings and conclusions. One of these findings was that prior to September 11 2001, information was not shared sufficiently.

The Joint Inquiry report concluded that information sharing is a problem not only across the intelligence community, but also within individual agencies and between the intelligence community and law enforcement agencies. Among the report's recommendations was that the FBI should increase the exchange of counterterrorism-related information between the FBI and other federal, state, and local agencies. The Joint Inquiry also recommended that the Attorney General and the FBI Director take action to ensure that the FBI better disseminate the results of searches and surveillances authorized under the Foreign Intelligence Surveillance Act to appropriate personnel within the FBI and throughout the intelligence community.

As a variety of OIG reviews also have shown, the Department's challenge in this area is formidable. While the Department has made significant strides in this area, especially in its coordination with state and local law enforcement agencies, much critical work remains, including ensuring adequate sharing of information between the Department and the newly created DHS.

For example, in the OIG's 2002 report on the FBI's counterterrorism program (OIG Report #02-38), we recommended that the FBI develop criteria for evaluating and prioritizing incoming 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 the 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.

Since issuance of our audit, the FBI has made improvements to its training process for intelligence analysts. In addition, it hired a new Executive Assistant Director for Intelligence from the National Security Agency who

has embarked on substantial improvements to the intelligence processes with the FBI.

The OIG's June 2003 review of the treatment of September 11 detainees also identified certain weaknesses in Department information sharing. This report recommended that federal immigration authorities work closely with the Department and the FBI to develop a more effective process for sharing information during future national emergencies that involve alien detainees. As part of its ongoing follow-up work with respect to this review, the OIG has requested specific information regarding the status of information-sharing mechanisms between the Department and the DHS.

An August 2003 OIG special review that examined the FBI's performance in deterring, detecting, and investigating the espionage activities of former FBI agent Robert Hanssen made additional recommendations to enhance information sharing. The OIG review concluded that Hanssen escaped detection not because he was extraordinarily clever in his espionage, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed FBI internal security program. In this review, the OIG discussed the need for improved coordination and information sharing within the Department related to counterintelligence investigations. Specifically, the OIG recommended that the Department's Criminal Division should be a full participant in FBI counterintelligence investigations.

In an ongoing review, the OIG is examining the FBI's progress in addressing deficiencies in its intelligence-sharing capabilities identified by the FBI, Congress, the OIG, and others subsequent to the September 11 attacks. This audit will determine the extent to which the FBI has identified impediments to the sharing of counterintelligence and other information, the extent to which the FBI has improved its ability to share intelligence information internally, with the Department, with the intelligence community, and with state and local law enforcement agencies, and the extent to which the FBI is providing useful threat and intelligence information to intelligence and law enforcement agencies.

In another ongoing review, the OIG is examining the FBI's handling of intelligence information that it had prior to the September 11 attacks. This review is examining aspects of the FBI's ability to process and share intelligence information. Among the issues we are reviewing at the request of the FBI Director 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.

In an example of the critical need to share information across agencies, the OIG has examined the status of the Department's efforts to integrate the FBI's and former INS's automated fingerprint 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 integrate automated fingerprint systems. We noted the importance of expeditiously combining the FBI's Integrated Automated Fingerprint Identification System (IAFIS) with the INS's Automated Biometric Identification System (IDENT) to enable the fingerprint systems to share information. A follow-up OIG review in December 2001 (OIG Report #I-2002-003) concluded that integration of IDENT and IAFIS had proceeded slowly and remains years away.

In the most recent review of these integration efforts, issued in June 2003, the OIG found that integration is still progressing slowly (OIG Report #I-2003-005). A fully integrated IDENT/IAFIS system would provide immigration 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 would provide state and local law enforcement agencies with valuable immigration information as part of a response from a single FBI criminal history search request. The lack of an integrated automated fingerprint system hinders the Department, the DHS, and state and local law enforcement agencies from sharing valuable immigration and law enforcement information about detained or apprehended persons. Our recent review found that the IDENT/IAFIS integration project is at least two years behind schedule.

According to JMD officials, the deployment date has been delayed until at least December 2003 because the INS staff and contractors working on the project were redirected in June 2002 to a competing priority. We found that despite the mounting delays, JMD did not prepare a revised schedule for completing the integration of IDENT and IAFIS. Moreover, the integration project may be at risk of further delay because JMD did not plan for continuing its stewardship of the project after the INS transferred to the DHS and now relies on informal working relationships with the DHS for system planning and implementation. The continued delays create additional risks to public safety and national security.

Finally, an ongoing OIG review of the operation of the FBI's Legal Attaché program is examining aspects of information sharing on an international level. Among other issues, the OIG is assessing the Attaché program's effectiveness in establishing liaisons with foreign law enforcement agencies.

3. Information Technology Systems Planning and Implementation: Information technology (IT) systems play a vital role in supporting the Department's varied operational and administrative activities. Employees rely on complex and often interrelated Department IT systems to meet challenges ranging from sifting through thousands of leads in a criminal investigation to developing annual financial statements. While the Department is making progress in this area, information technology systems planning and implementation continues to be a top management challenge across the Department.

In the past, OIG reviews have found numerous deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training. These deficiencies can severely impede the FBI's ability to effectively accomplish its mission because the FBI must be able to use its IT systems to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. Since FY 2002, the Department listed the FBI's management of IT as a material weakness.

A December 2002 OIG audit of the FBI's management of its IT investments (OIG Report #03-09) found that the FBI has not effectively managed its IT investments because it has not fully implemented a series of critical management processes. Specifically, the audit found that the FBI: 1) did not have fully functioning IT investment boards that are engaged in all phases of IT investment management; 2) had not followed a disciplined process of tracking and overseeing each project's cost and schedule milestones; 3) failed to document a complete inventory of existing IT systems and projects and did not consistently identify the business needs for each IT project; and 4) did not have a fully established process for selecting new IT project proposals that considered both existing IT projects and new projects. FBI officials acknowledged to the OIG that prior to March 2002, individual FBI divisions determined their IT needs in a "stovepipe" without knowledge of the business needs and priorities of the FBI as a whole.

The OIG audit also concluded that because the FBI had not fully implemented the critical processes associated with effective IT investment management, it had spent hundreds of millions of dollars on IT projects without adequate assurance that these projects would meet their intended goals. In addition, the FBI did not have adequate assurance that its IT projects were being developed on schedule and within established budgets.

In the same audit, the OIG found that the FBI is making strides toward correcting these deficiencies. For example, the OIG found that since March 2002, when it began pilot testing a new IT investment management process,

the FBI has made measurable progress towards implementing key practices necessary for an effective IT management system, especially in the area of selecting new IT projects. At the beginning of the OIG audit in January 2002, the FBI was executing only 4 of the 38 required “key practices” for building an IT investment foundation. By June 2002, the FBI was executing 14 of the 38 key practices. As part of its audit, the OIG offered 30 specific recommendations for actions the FBI should take to improve its IT investment management.

Following through and correcting previously cited deficiencies takes dedicated resources and agency commitment. In a September 2003 OIG audit, the OIG examined the FBI’s implementation of various IT recommendations (OIG Report #03-36). We found that while the FBI has implemented many of the recommendations in prior OIG reports (93 out of 148), it still needs to take additional significant actions to ensure that the IT program effectively supports the FBI’s mission. For example, until recently the FBI lacked an effective system of management controls to ensure that OIG recommendations were implemented. However, the FBI Director has committed the FBI to enhancing its internal controls to ensure that OIG recommendations are implemented in a timely and consistent manner. To this end, the FBI recently developed a system to facilitate the tracking and implementation of recommendations for improvement. In addition, the FBI expects that its IT modernization efforts will correct many of the deficiencies identified over the years by the OIG.

Due to the importance of sound information systems planning and implementation across all Department components, the OIG plans to conduct additional reviews on IT throughout the Department. This fiscal year, the OIG plans to audit the Drug Enforcement Administration’s (DEA) IT investment management process. As part of this review, the OIG will examine the DEA’s strategic planning and performance measurement activities related to IT management. In addition, we also plan to audit JMD’s implementation of IT investment management processes.

4. Computer Systems Security: Computer security has been a Department Material Weakness in one form or another since 1989. The threat to Department networks and databases from unauthorized access remains, as hackers and potential terrorists attempt to develop new technologies that could potentially breach the Department’s computer systems.

Since FY 2001, the OIG has performed security assessments and penetration testing of Department computer systems as mandated initially by the *Government Information Security Reform Act* (GISRA) and, as of December 2002, by the *Federal Information Security Management Act* (FISMA). The

FISMA directs the OIG to perform an annual independent evaluation of the Department's information security program and practices and report the results to the Office of Management and Budget (OMB).

In meeting these responsibilities, the OIG has conducted 22 computer security audits of Department IT systems over the past 3 years. For FY 2003, we selected five mission-critical Department computer systems – three classified systems and two sensitive but unclassified systems – to review. In addition, we reviewed the Department's oversight initiatives with respect to computer security. Overall, we concluded that the Department's IT security program requires additional improvement at both the Department and component levels, particularly in program oversight and vulnerability management to protect computer systems and reduce the number of vulnerabilities within the Department's IT systems. While we noted progress in certain areas, continued improvements are needed to help reduce the total number of vulnerabilities within the Department's IT systems.

Without effective IT system security oversight and security management controls, system vulnerabilities may not be identified or tracked properly and corrective action plans may not be implemented in a timely and effective manner. Consequently, the underlying data within these IT systems may not be reliable and data manipulation may go undetected. In light of our audit results, we also remain concerned that the Department's functions have not been centralized sufficiently to provide the vigorous enforcement oversight – supported by a substantial, technically proficient work force – that the Department needs.

In July 2003, in a separate audit we examined SENTRY, the BOP's primary mission support database that processes over 1 million transactions each day (OIG Report #03-25). The system tracks critical information on more than 165,000 inmates in federal prisons including inmate location, medical history, behavior history, and release data. Our audit assessed the system's application controls and examined whether SENTRY data are valid, properly authorized, and completely and accurately processed. The audit identified weaknesses in 4 of the 27 control areas that we tested: supervisory reviews, audit logs, access controls, and computer matching of transaction data. We concluded that these weaknesses occurred because BOP management did not fully develop, document, or enforce BOP policies in accordance with current Department policies and procedures.

Our past audits have reported progress in the Department's oversight of computer security, particularly with the restructuring of the Chief Information Officer (CIO) position and initiatives undertaken by the new CIO. However, many of the deficiencies identified by the OIG in its recent

GISRA and FISMA reviews revealed repeated deficiencies from prior reviews. For example, our audits of the Department's systems in FY 2001 and 2002 revealed vulnerabilities in the management, operational, and technical controls that protect each system and its data from unauthorized use, loss, or modification. Of these three control areas, the vulnerabilities noted in technical controls are the most significant because these controls are used to prevent unauthorized access to system resources by restricting, controlling, and monitoring system access.

Additionally, our FY 2002 consolidated audit of the Department's computer security management procedures (OIG Report #03-19) identified inconsistencies in the oversight of computer security that we attributed to the bifurcation of responsibility between the JMD's Security and Emergency Planning Staff and its Information Management and Security Staff. We found security reviews of the Department's systems conducted by these offices were uneven or inadequate and major systems and applications lacked elementary protections that the Department's accreditation process is intended to ensure are in place.

Our consolidated report made nine recommendations, including that:

- the Department's CIO should have greater authority over classified IT systems and the CIO's staff should be commensurately augmented;
- the tracking system used to record and monitor corrective action should be expanded in terms of both the IT systems it encompasses and the types of corrective actions it tracks;
- the use of automated technical control solutions should be expanded because of the vulnerabilities that can result when IT personnel are scarce, overextended, or inattentive;
- the Department should extend its specifications for system assessment and testing, contingency plans, emergency response preparations, and consequence management (including data retrieval and alternative site drills); and
- the Department should increase its oversight of components' and managers' compliance with established IT security rules. The Department agreed with the recommendations and is in the process of implementing corrective actions.

Finally, the OIG's review of the Hanssen case, described above in challenge 2, identified serious security flaws in the FBI's Automated Case Support (ACS)

computer system. This review found that Hanssen had improperly used the ACS system to track some of the FBI's most sensitive espionage investigations, including the investigation that was looking for him. The OIG found that access restrictions to the ACS system are subject to override by FBI Headquarters employees who, like Hanssen, may have no need to know about sensitive operations the access restrictions are designed to protect. In addition, the system is prone to human error, with documents concerning highly sensitive operations, such as the Hanssen investigation, being made available to many users because of improper uploading or inadequate restriction codes. We found that the ACS system's audit function, mandated by Department regulations and a principal tool against unauthorized usage, was rarely used before Hanssen's arrest. The FBI is implementing a new automated case system known as the Virtual Case File (VCF), a computerized database that will maintain information on FBI investigations in electronic case files. In developing and implementing VCF, it is vital for the FBI to rectify the types of security flaws in the ACS system identified by the OIG and others.

5. Financial Management: In FY 2002, for the second consecutive year the Department received an unqualified opinion on its financial statements. In addition, the number of material weaknesses on the Department's consolidated financial statements declined from three in FY 2001 to two in FY 2002. The Department also received unqualified opinions on all ten of the reporting components' financial statements that make up the consolidated report. Importantly, several components were able to reduce the number of material weaknesses and reportable conditions, reducing the overall number of material weaknesses from 13 to 9. In particular, the DEA eliminated the four material weaknesses reported in FY 2001. These results reflect a continued commitment by the Department to financial accountability and improvement of internal controls. The Department and its components deserve significant credit for these accomplishments.

However, important challenges remain. Antiquated and ineffective automated accounting systems and decentralized financial management threaten the Department's ability to maintain its unqualified opinion. For example, because of these deficient systems, problems related to financial accounting and reporting in FY 2002 were overcome only by significant year-end manual efforts. Many tasks had to be performed manually because the Department lacks automated systems to readily support ongoing accounting operations, financial statement preparation, and the audit process. Such manual efforts compromise the Department's ability to prepare financial statements that are timely and in accordance with generally accepted accounting principles, and which provide Department managers information

on an ongoing basis to allow them to more effectively manage Department programs.

In order to meet the accelerated reporting deadlines for the FY 2003 and FY 2004 financial statement audits, the Department has significant hurdles to overcome because of its continued dependence on these manual efforts. During FY 2003, quarterly financial statements were due 45 days after the close of a quarter, and for FY 2004 the *Performance and Accountability Report* is due by November 15, 2004 – nearly 2½ months earlier than the current OMB reporting deadline.

To succeed within the expedited time frames, the Department must move away from manual processes to prepare financial statements more timely and, in turn, auditors must be able to test and rely upon internal control processes throughout the year. Recent interim audit tests performed for the FY 2003 audit were discouraging, given that many components failed portions of the testing. While additional year-end testing and manual efforts to fix problems is possible for the FY 2003 audits, it will not be possible in FY 2004 because component audits need to be completed within 14 days of the end of the fiscal year in order to meet the OMB's accelerated deadlines.

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 and other required financial reporting. In FY 2002, the Department initiated the Unified Financial Management System (UFMS) project to replace the seven major accounting systems currently used throughout the Department in an effort to address these deficiencies. Currently, none of the Department's accounting systems are integrated. Consequently, production of Department-wide information must be done manually or by duplicative inputting of data from one system into another.

In fact, several of the older systems in use by Department components predate the current accounting requirements and do not support the production of timely, relevant information that is needed for preparing financial statements or performing accrual accounting transactions. For example, property transactions in several components are entered twice into separate accounting and property systems – systems that need to be periodically reconciled, often manually and sometimes line-by-line.

As another example, the U.S. Marshals Service (USMS) continues to use two different major accounting systems. The older of the two systems, the Financial Management System, is used by staff in USMS field offices and was scheduled to be replaced approximately 5 years ago by STARS, the

Headquarters' accounting system. However, efforts to implement the STARS system throughout the USMS were halted in 1998 due to difficulties encountered in implementing STARS at Headquarters. While the USMS has been able to develop a linkage between these two systems in order to be compliant with the Standard General Ledger requirements and have more timely access to detailed field office information, this patch is not a desired solution. The USMS financial systems still do not include key financial data related to property and procurement, and consequently the USMS has to perform manual data calls for this information to ensure that the financial statements are complete.

When fully implemented, the Department's UFMS will replace the majority of Department financial systems with a single, integrated, user-friendly system. We believe such a uniform system is necessary to help address many of the Department's longstanding weaknesses. However, some of the challenges that may arise as a result of the Department's transition to the UFMS include: 1) unexpected funding shortfalls and competing initiatives; 2) implementing the system without disrupting daily operations; and 3) hiring and training staff qualified to operate the new system.

As a result of the Department's reliance on manual processes and multiple, ineffective financial systems, its capability to provide current, timely, and accurate financial information to managers remains limited. The Department also continues to utilize extraordinary efforts to obtain audit opinions and satisfy financial reporting requirements. It will be difficult for the Department to maintain a clean audit opinion for FY 2004 and future years and meet the expedited reporting dates unless it modernizes and streamlines its financial management systems.

6. Grant Management: The Department awards approximately \$6 billion dollars annually in grants to more than 6,000 state and local governments as well as profit and not-for-profit entities. The grants fund a wide variety of activities, including community policing, drug treatment, reimbursement to states for incarcerating illegal aliens, counterterrorism training, and reimbursement to victims of crime. Managing such an extensive grant-making operation efficiently and effectively continues to be a major challenge for the Department, given the large amount of money involved and the diversity and complexity of the grant programs.

To assist the Department in meeting this challenge, an August 2003 OIG audit (OIG Report #03-27) examined the two offices primarily responsible for managing the Department's grant programs – the Office of Justice Programs (OJP) and the Office of Community Oriented Policing Services (COPS) – to identify activities that could be streamlined to increase efficiency.

The OJP has experienced dramatic growth since it was established in 1984. Its funding programs are divided into two main categories: formula grants and discretionary grants. Formula grants are awarded to state and local governments based on a predetermined formula using, for example, a jurisdiction's crime rate or population. States are generally required to pass through a significant portion of formula awards to local agencies and organizations in the form of sub grants. Discretionary grants are awarded on a competitive basis to public and private agencies and private non-profit organizations. However, certain discretionary programs are awarded on a noncompetitive basis, consistent with congressional earmarks.

The COPS Office was established in 1994 as a result of the Violent Crime Control and Law Enforcement Act of 1994. The single largest component of the 1994 Crime Act – the Public Safety Partnership and Community Policing Act of 1994 – authorized \$8.8 billion over 6 years to fund additional community oriented policing officers and to advance community policing nationwide, and COPS continued to receive annual appropriations from FY 1995 – 2003 totaling approximately \$11.3 billion. To implement the COPS grant program, the Attorney General created the COPS Office as a separate office from OJP.

Our audit determined that the Department's federal financial assistance programs are fragmented, resulting in reduced efficiency and increased costs to award and administer federal financial assistance funds to state and local agencies. We found structural overlap between OJP and the COPS Office, overlap in grant programs between the COPS Office and OJP, lack of on-line grant application processing in the COPS Office, overlap in OJP's organization structure, and inefficiencies in OJP's automated grant management systems. We also found overlap between the types of grants awarded by the COPS Office and OJP. For example, the COPS Universal Hiring Program grants and Making Officer Redeployment Effective grants are sometimes duplicative of grants awarded by OJP under the Local Law Enforcement Block Grants program. Yet, both COPS and OJP officials told us that no formal communication procedures exist between the two agencies to ensure that grantees do not receive funds for similar purposes from both agencies.

We found that COPS had not developed a capability to receive grant applications on-line and to download the application information directly into its grant management system. Instead, grantees must submit applications on paper and COPS must manually input the data into its tracking system.

In addition, the audit found that OJP did not have a fully effective automated system to manage its federal financial assistance funds and, in fact, we found that OJP had more than 70 automated application systems in place. Some of these systems were developed by the individual components within OJP, and they duplicate information in other OJP systems. Despite having more than 70 automated systems to help manage its federal financial assistance funds, OJP still relied primarily on a manual system for processing grants.

Our report contains eight recommendations to improve the Department's grant-making activities, including taking steps to enhance coordination between COPS and OJP to eliminate duplication of effort and ensure that awards are not made to the same grantee for similar purposes. OJP agreed with our recommendations and is in the process of implementing corrective actions. Although the COPS Office took exception to some of the information and conclusions in the report, it agreed with the recommendations directed to it and is in the process of implementing corrective actions. Specifically, the COPS Office, as well as OJP, agreed to coordinate and exchange information about grant programs to ensure duplicative awards are not made to the same grantee by both agencies. In addition, the COPS Office agreed to continue to develop an on-line application system for COPS grants. Further, OJP is working to implement, by the end of December 2003, an enhanced grant management system with modules that will expand the system to manage grants from beginning to end.

In other reviews over the years, the OIG has devoted considerable attention to auditing individual Department grant programs to examine grantee compliance. For example, more than 375 OIG audits of COPS grants have resulted in significant dollar-related findings. 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. In the first six months of FY 2003, our audits had even greater dollar-related findings – more than \$17 million in questioned costs and more than \$11 million in funds to better use. In light of these findings and because of the large amounts of money earmarked for this program, the OIG will continue its program to audit COPS grants.

In addition to reviewing COPS grants, the OIG audits other types of Department grant programs. For example, the OIG currently is auditing OJP training and technical assistance grants. This review includes both an internal audit that will evaluate the OJP's efforts to award and monitor the training and technical assistance grants, and a series of external grant audits that will examine compliance by recipients with the terms of the grants.

The OIG also audits activities of the organizations that receive funding from the Department. The OIG's workplan for FY 2004 includes internal audits of several broad categories of OJP programs and grants, including grants for DNA backlog reduction, victims' services, and assistance to tribal governments. The OIG also intends to evaluate OJP's oversight of the grants and to perform individual audits testing grantees' compliance with the terms of the grant. For example, the OIG plans to initiate an audit of Antiterrorism and Emergency Assistance Program grants issued by OJP's Office for Victims of Crime. In conjunction with this internal audit, the OIG intends to conduct a number of individual audits of grant recipients.

7. Performance-Based Management: A significant challenge for the Department is to ensure, through performance-based management, that its programs are achieving their intended purposes. This is a challenge throughout the federal government, and it is also one of the Administration's most important management initiatives. As a regular part of OIG audits, we continue to examine performance measures for the component or program under review and to determine whether the performance results are supported by reliable measurement methods or systems. Additionally, as part of our annual financial statement audits, we collect information about the existence and completeness of performance measurement data.

OIG audits generally have found that the performance measures need improvement. Many are not focused on outcomes or are not quantifiable and verifiable. For example, in an audit completed in September 2003, the OIG reviewed the DEA's implementation of the GPRA (OIG Report #03-35). We found that the DEA had developed a strategic goal and objectives that were consistent with the Department's strategic goals and objectives, but the DEA's strategic goal and objectives were not definitive enough to allow for an assessment of whether they were being achieved. In addition, even though the DEA had established performance indicators for all of its budget decision units, it had not established:

- specific criteria for its field divisions to designate organizations as "priority target" organizations, a key element of its strategic goal;
- specific criteria for its field divisions to report on the primary performance indicator – priority target organizations disrupted or dismantled;
- an effective system to collect, analyze, and report performance data for all of its performance indicators;

- procedures to verify the performance data for all of its performance indicators; and
- accurate performance data for one of the five field divisions included in our review.

As a result of these deficiencies, the ability of the DEA, the Department, Congress, and the public to assess the effectiveness of the DEA's performance is diminished. We made seven recommendations to the DEA, including that it establish a strategic goal and objectives that are quantitative, directly measurable, or assessment-based; and establish specific criteria for determining what constitutes a priority target organization and a disrupted or dismantled priority target organization. The DEA concurred with our recommendations and stated that its new draft FY 2003-2008 Strategic Plan includes a general long-term goal and four specific strategic goals with two- and five-year quantitative, time-specific objectives. The DEA also has prepared definitions and specific criteria for what constitutes a priority target organization and a disrupted/dismantled organization. The DEA stated that the definitions and criteria are under review and will be included in a new Priority Target Handbook. The DEA plans to complete these actions by November 2003.

Reporting verifiable performance-based accomplishments also is critical to the Department's planning and priority setting. In an ongoing review of the U.S. Attorneys' Offices (USAOs) Critical Incident Response Plans (Plans), described above in the first management challenge, the OIG found that the Department overstated the degree of implementation of the USAOs' crisis response planning in the Department's Annual Performance Report for FY 2001 by suggesting a much higher performance level than actually was achieved. Providing accurate and verifiable performance data is a critical component of performance-based management.

8. Human Capital: Hiring, training, and retaining adequate personnel to handle the myriad duties of the Department are ongoing challenges. The increasing technical and sophisticated nature of the Department's work, coupled with the competition for qualified employees – often against private sector companies or other government agencies such as the Department of Homeland Security that may be able to offer greater monetary awards – only increases the Department's challenge in this area. Without a continued focus on recruitment, retention, and training, the Department runs the risk of losing ground in its efforts to address several other top management challenges, such as Computer Systems Security, Financial Management, and Information Systems Planning and Implementation. Furthermore, lack of adequately trained personnel could impede the Department's

counterterrorism efforts, its effort to upgrade its IT systems, and its ability to share intelligence and law enforcement information.

For example, in January 2003, as part of its Major Management Challenges and Program Risks series, the General Accounting Office expressed its concern about the Department's ability to attract and retain qualified special agents, intelligence analysts, and language professionals (GAO Report #03-105) due to the demand for employees with language skills throughout government, especially proficiency in Middle Eastern and Asian languages. The GAO recommended that the FBI look to sharing language resources with other agencies as a way of meeting its needs for language services.

In October 2003 the OIG initiated an audit of the FBI's hiring, training, and staffing of intelligence analysts and reports officers to ensure that these critical positions are being staffed in a timely manner with qualified personnel. The review will examine: 1) how analyst and reports officer hiring requirements and qualifications were established; 2) progress made toward meeting the hiring goals and retaining the personnel; 3) progress made toward establishing a comprehensive training program and meeting the training goals; and 4) how analysts and reports officers are staffed and utilized to support the FBI's counterterrorism mission.

The National Commission on Terrorism in its report *Countering the Changing Threat of International Terrorism* stated that, "All U.S. Government agencies face a drastic shortage of linguists to translate raw data into useful information. This shortage has a direct impact on counterterrorism efforts." Indeed, shortly after the September 11 attacks, the FBI issued a public call for Middle Eastern and Central Asian linguists. In the past, at the FBI shortages of linguists have resulted in thousands of hours of audiotapes and pages of written material not being reviewed or translated in a timely manner. To examine this issue, the OIG has initiated an audit of the FBI Language Services program to review. The objectives of the audit are to determine the extent and causes of any FBI translation backlog; evaluate whether FBI procedures ensure appropriate prioritization of work, accurate and timely translations of pertinent information, and proper security of sensitive information; and assess the FBI's efforts to hire additional translators.

In another area, our ongoing audit work in the financial management area continues to find that several Department components lack adequate staff to perform many of the tasks needed to produce financial statements. Consequently, the Department continues to rely heavily on the use of contractors to prepare financial statements which, in addition to affecting the expense associated with producing the statements, contributes to diminishing

the institutional knowledge and expertise. In addition, Department components have difficulty recruiting and retaining highly qualified information technology specialists who are knowledgeable about the latest hardware and software. As a result, the components have found it difficult to address some of the IT issues identified in the financial statement audits.

In 2003, the OIG continued to examine another important aspect of the Department's efforts to successfully manage human capital – its ability to develop fair and consistent methods of addressing allegations of employee misconduct. In FY 2001, the OIG completed a review of the disciplinary system of the USMS (OIG Report I-2001-011) – the first in a series of reviews of components' disciplinary systems. Our review of the USMS found misconduct cases where the consistency of the discipline or the degree of discipline imposed raised serious concerns, and the reasons for the final discipline decisions were not adequately documented. In addition, we found significant periods of unexplained elapsed time that appeared to prolong case adjudication. We made 12 recommendations to help the USMS improve its disciplinary system.

Most recently, the OIG examined the process by which the DEA identifies, refers, and investigates employee misconduct and imposes and enforces disciplinary actions in response to substantiated allegations of employee misconduct. The review evaluated the DEA's compliance with procedures for reporting allegations of misconduct to its Office of Professional Responsibility as well as the timeliness of the process from the referral of allegations to the implementation of disciplinary actions. The review also examined the appropriateness and consistency of disciplinary actions. We found that the DEA's system for investigating employee misconduct generally functioned well in that its investigations generally appeared to be thorough and well documented, and provided a sound basis for making disciplinary decisions.

However, we found problems in various cases that revealed weaknesses in DEA's disciplinary system. These weaknesses included inadequate guidance and dual mitigation which resulted in penalties that appear to be too lenient; the improper consideration of external factors by Board members and a Deciding Official when making disciplinary decisions; a failure to adequately document disciplinary decisions by the Board and Deciding Officials; a failure of DEA management to monitor the timeliness of the disciplinary process; and a lack of management oversight over the Deciding Officials. We made eight recommendations to help the DEA ensure that its disciplinary decisions are reasonable, free of inappropriate external influences, well documented, and timely.

9. Protecting the Security of Department Information and Infrastructure: A difficult challenge for the Department is the need to not only share intelligence and law enforcement information with a wider audience but also to protect the security of that information. Striking a balance between these competing objectives is critical to the Department's efforts to prevent future terrorist acts. In addition, the security of the Department's infrastructure – including its buildings, computers, and communications systems – presented a significant challenge well before the September 11, 2001, terrorist attacks.

For example, in April 1997 the OIG issued a classified report examining the FBI's performance in uncovering the espionage activities of former Central Intelligence Agency (CIA) Directorate of Operations officer Aldrich Ames. The review found that throughout nearly the entire 9-year period of Ames' espionage, the FBI devoted inadequate attention to determining the cause of the sudden, unprecedented, and catastrophic losses suffered by both the FBI and the CIA in their Soviet intelligence programs. One of the recommendations made by the OIG in the report focused on the FBI's inability to provide the OIG review team with a definitive answer concerning the distribution of various top secret documents. Given the sensitive nature of such documents, the OIG recommended that the FBI develop and maintain a better record-keeping system for tracking dissemination of its documents.

Six years later, the OIG released its review of the Hanssen case, which found this and other recommendations from the Ames matter had not been sufficiently implemented. Our Hanssen review found that over the course of more than 20 years, former FBI supervisory special agent Robert Philip Hanssen compromised some of this nation's most important counterintelligence and military secrets, including the identities of dozens of human sources, at least three of whom were executed. Hanssen's espionage began in November 1979 – three years after he joined the FBI – and continued intermittently until his arrest in February 2001, just two months before his mandatory retirement date.

In August 2003, the OIG released the results of its review of the FBI's performance in deterring, detecting, and investigating Hanssen's espionage activities. The OIG's 674-page report, classified at the Top Secret/Codeword level, revealed that there was little deterrence to espionage at the FBI during Hanssen's 25-year career. The FBI did not employ basic personnel security techniques – such as counterintelligence polygraph examinations and financial disclosure reviews – and the one background reinvestigation Hanssen underwent during his career was not thorough.

The FBI's information security program likewise offered little deterrence to Hanssen's espionage. Because of inadequate document security, Hanssen felt

comfortable removing hundreds of pages of classified documents from FBI offices, including numbered original Top Secret documents. In addition, inadequate computer security permitted Hanssen to conduct thousands of searches on the FBI's computer system for references to his own name, address, and drop and signal sites to see if he was under suspicion and to search for information concerning the FBI's most sensitive counterintelligence cases. The computer system's audit function, mandated by Department regulation and a principal tool against unauthorized use as well as espionage, was rarely used before Hanssen's arrest.

The OIG found that Hanssen escaped detection not because he was extraordinarily clever and crafty, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. The OIG made 21 recommendations to help the FBI improve its internal security and enhance its ability to deter and detect espionage in its midst and protect sensitive information. For example, the OIG recommended that the FBI create and implement programs enabling it to account for and track hard copy documents and electronic media containing sensitive information to prevent the unauthorized removal of sensitive information from FBI facilities. In addition, we recommended that the FBI implement measures to improve computer security, including an audit program to detect and give notice of unauthorized access to sensitive cases on a real-time basis and procedures to enforce the "need to know" principle in the context of usage of FBI computers.

We also recommended that the FBI consider enhanced security measures to protect its information from misuse or compromise, including more frequent polygraph examinations, more frequent and thorough background reinvestigations, and more detailed financial disclosures for employees who enjoy unusually broad access to sensitive information. In response to these security-related recommendations, the FBI reported that it has initiated a financial disclosure program and expanded the pool of counterintelligence-focused polygraph examinations. In addition, the FBI reported taking a number of steps to improve background investigations, including automating the collection of information acquired during background investigations.

However, we found that many of the changes that the FBI says it is implementing are either ongoing or still in the planning stages. Moreover, some of the FBI's responses do not address the core concern underlying our recommendations. For others, we are closely examining the FBI's response and plan to request additional information and monitor the FBI's ongoing changes.

In another review recently initiated at the request of the FBI Director, the OIG began examining the FBI's controls over safeguarding classified information and preventing espionage in its China program. This review stems from the indictment of a former FBI Agent in Los Angeles on charges of gross negligence in handling classified information. The OIG review will, among other issues, examine allegations that the agent improperly removed classified information from FBI offices and allowed a Chinese informant access to sensitive and classified information. The informant was indicted on charges of obtaining, copying, and retaining U.S. national defense documents without authorization.

With respect to critical infrastructure, the OIG has conducted several reviews of the Department's efforts to protect its critical infrastructure in the event of a terrorist attack or other threats. Presidential Decision Directive 63 requires the Department and other government departments and agencies to prepare plans for protecting their critical infrastructure. The plans must include an inventory of mission-essential assets, a vulnerability assessment of each asset, and steps to remediate the vulnerabilities. Issued by the President, the National Plan for Information Systems Protection calls for a similar assessment of information system vulnerabilities and the adoption of a multi-year funding plan.

In an audit issued in November 2001 – Departmental Critical Infrastructure Protection Planning for the Protection of Physical Infrastructure (OIG Report #02-01) – the OIG concluded that the Department had not adequately planned for the protection of critical physical assets. Specifically, the Department had not 1) adequately identified all of its mission-essential physical assets, 2) assessed the vulnerabilities of each of its physical assets, 3) developed remedial plans for identified vulnerabilities, and 4) developed a multi-year funding plan for reducing vulnerabilities. We concluded that, as a result, the Department's ability to perform vital missions is at risk from terrorist attacks or similar threats. We recommended that the Department properly inventory its critical physical assets, complete vulnerability assessments, and develop remedial plans to address the weaknesses identified. After initially disagreeing with our recommendations, the Department has now embarked upon, but has not yet completed, an appropriate inventory of its critical physical assets.

In an OIG audit completed in October 2003, we examined the adequacy of the Department's efforts to protect its critical computer-based infrastructure. We found that the Department has not achieved "full operating capability" – that is, the ability to protect critical infrastructures from intentional acts that would significantly diminish the ability to perform essential national security missions and ensure general public health and safety. The audit concluded

that the Department needs to complete critical infrastructure protection efforts in risk mitigation, emergency management, and interagency coordination. Among the recommendations we made to help improve the Department's efforts to manage critical infrastructure protection are that the Department should:

- develop a risk mitigation tracking system to inventory classified mission-essential infrastructure systems;
- develop a multi-year funding plan based on resources required to mitigate vulnerabilities as identified in Plans of Actions and Milestones;
- develop and test contingency plans for all critical IT assets; and
- contact other agencies to determine whether any Department assets are critical to their missions.

The Department needs to focus on these and other related issues as it seeks to strike the appropriate balance between sharing intelligence and law enforcement information with a wider audience to meet its counterterrorism challenge while at the same time protecting the security of that information.

10. Reducing the Supply of and Demand for Drugs: An ongoing challenge for the Department, along with other federal and state governments and non-government entities, is to reduce both the supply of and demand for drugs. This is a difficult mission that will not be solved easily or quickly. With regard to reducing supply, the Department's challenge extends beyond illegal drugs such as cocaine and heroin to reducing the diversion or misuse of legal drugs, including prescription medication. It also is widely recognized that enforcement alone to reduce the supply of illegal drugs and diversion of legal drugs is only part of the challenge, and that federal efforts to reduce the demand for drugs also are necessary.

During the past two years, the OIG has completed several reviews that highlight the difficulties facing the Department in attempting to address these challenges.

In addition to the millions of users of illegal narcotics, the illegal diversion of prescription drugs for non-medical purposes is a growing and staggering problem. According to the Substance Abuse and Mental Health Services Agency, emergency rooms across the country recorded a 163 percent increase in the number of visits tied to the abuse of prescription drugs between 1995 and 2002. Furthermore, prescription drugs are now a factor in one-fourth of

all drug overdose deaths reported in the United States. The DEA Administrator, in a speech to the American Pain Society in March 2002, noted that the number of people who abuse controlled pharmaceuticals each year approximately equals the number who abuse cocaine – 2 to 4 percent of the U.S. population.

Therefore, an important and growing challenge to the Department is to reduce the diversion of controlled pharmaceuticals. Diversion occurs when legally produced pharmaceuticals are illegally obtained for non-medical use. Diversion commonly involves physicians or pharmacists selling prescriptions to drug dealers or abusers, employees stealing from drug inventories or pharmacies, individuals improperly obtaining multiple prescriptions from different doctors or over the Internet, and individuals forging prescriptions. Within the DEA, the Office of Diversion Control is responsible for overseeing the distribution system for controlled pharmaceuticals and regulated chemicals, and for preventing the diversion of those substances.

In September 2002, the OIG issued a review of the DEA's investigative response to the diversion of controlled pharmaceuticals (OIG Report #I-2002-010). Our review found that the DEA's enforcement efforts did not adequately address the problem of controlled pharmaceutical diversion. Despite the widespread problem of pharmaceutical abuse, the DEA dedicated only 10 percent of its field investigator positions to diversion investigations. In addition, we found that since 1990 the number of diversion investigators as a percentage of total DEA investigators decreased by 3 percent. While the DEA has traditionally focused the majority of its resources on disrupting illicit drug trafficking operations, we concluded that it is critical for the DEA to devote more resources to counteract the widespread problem of controlled pharmaceutical diversion.

We also found the DEA failed to provide sufficient DEA special agents to assist diversion investigators in conducting investigations of controlled pharmaceutical diversion. Diversion investigators lack law enforcement authority and therefore must request either DEA special agents or local law enforcement officers to perform essential activities such as conducting surveillance, issuing search warrants, managing confidential informants, and performing undercover drug purchases. We found that difficulties in obtaining law enforcement assistance caused delays in developing cases for prosecution. The quality of investigations also has suffered because of the need to use investigators external to the diversion control program who lack experience in conducting controlled pharmaceutical investigations, which often requires establishing the criminal intent of doctors, pharmacists, and other medical professionals. DEA officials acknowledged these problems and over the past 25 years have proposed solutions ranging from vesting

diversion investigators with criminal investigative authority to assigning special agents to diversion units on a full-time basis. However, as of October 2003 the DEA still has not implemented an effective solution. The DEA advised the OIG that the reclassification of diversion investigators to special agents requires more discussion before a decision is made.

In addition, our review found that the DEA provides minimal intelligence support to its diversion investigators, instead focusing its intelligence efforts on developing and analyzing intelligence information on illicit drug trafficking. The one potential intelligence resource currently available to diversion investigators is the Automation of Reports and Consolidated Orders System (ARCOS). The ARCOS contains information on the inventories, acquisitions, and dispositions of certain controlled pharmaceuticals, as reported quarterly by manufacturers and distributors. These quarterly reports show transactions for broad categories of controlled pharmaceuticals but not specific drugs. ARCOS details the flow of DEA-controlled pharmaceuticals from their point of manufacture through commercial distribution channels to the sale or distribution to dispensing or retail outlets (such as pharmacies, health care practitioners, and hospitals). However, diversion investigators told the OIG that ARCOS reports are limited in their value as an intelligence resource because of problems of completeness, accuracy, and timeliness. Diversion staff at Headquarters and in DEA field offices also told the OIG that they do not have the adequate resources to analyze and develop ARCOS data into useful intelligence products.

With regard to reducing the supply of illegal drugs, in September 2003 the OIG issued an audit examining the DEA's performance measures assessing its impact on reducing the supply of illegal drugs. The audit entitled, "The DEA's Implementation of the Government Performance and Results Act" (GPRA) (OIG Report #03-35), concluded that the DEA failed to meet key aspects of the GPRA and noted that while the DEA developed a strategic goal and objectives that were consistent with the Department's, the DEA's strategic goal and objectives were not definitive enough to allow for an assessment of whether they are being achieved.

For example, even though the DEA had established performance indicators for all of its budget decision units, it had not established: 1) specific criteria for its field divisions to designate organizations as "priority target" organizations, a key element of its strategic goal; 2) specific criteria for its field divisions to report on the primary performance indicator – priority target organizations disrupted or dismantled; 3) an effective system to collect, analyze, and report performance data for all of its indicators; 4) procedures to verify performance data for all of its indicators; and 5) realistic goals for its performance indicators.

As a result of these deficiencies, the ability of the Department, Congress, and the public to assess the effectiveness of the DEA's performance in reducing the supply of illegal drugs was diminished. We recommended, among other things, that the DEA establish a strategic goal and objectives that are quantitative, directly measurable, or assessment-based and develop specific criteria for determining what constitutes a priority target organization and a disrupted or dismantled priority target organization. The DEA concurred with our recommendations and is updating its strategic plan. The new strategic plan will include, according to the DEA, one general long-term goal and four strategic goals with quantitative, time-specific objectives that will address the OIG's recommendations.

In FY 2004, the OIG will continue to examine other supply-reduction aspects of this challenge by reviewing the operations of the High Intensity Drug Trafficking Area Task Forces, a program designed to help federal, state, and local law enforcement organizations invest in infrastructure and joint initiatives to confront drug-trafficking organizations. The objectives of the audit will be to determine the relationship between DEA's mission and the Office of National Drug Control Policy's mission for the High Intensity Drug Trafficking Area (HIDTA) program; DEA's overall relationship to the HIDTA program; the efficiency and cost effectiveness of HIDTA's delivery of funds to federal, state, and local law enforcement agencies; and the impact on agencies that participate in HIDTA task forces as a result of changes in law enforcement priorities in response to the events of September 11, 2001.

Attempting to reduce the supply of drugs alone will not solve the problem of illegal use of drugs; reducing the demand for illegal drugs is a critical component of the strategy to reduce drug abuse in the United States. In a February 2003 audit, the OIG examined the Department's drug demand reduction activities, one of the objectives identified in the DEA's current Strategic Plan. While early federal drug control efforts concentrated primarily on enforcement, federal drug demand reduction efforts today include drug abuse education, prevention, treatment, research, rehabilitation, drug-free workplace programs, and drug testing.

The OIG reviewed the Department's drug demand reduction activities to: 1) identify all Department programs that related to drug demand reduction, quantify the total obligations for each program, and verify that financial information provided to the ONDCP was prepared appropriately; 2) determine whether the Department's performance measures are adequate to determine the success of its programs; 3) identify whether Department drug demand reduction activities were duplicative and whether Department components were coordinating drug demand reduction efforts; and 4) review

the DEA activities and funding dedicated to drug demand reduction. During its audit, the OIG examined drug demand reduction programs in the BOP, COPS, OJP, and the DEA.

The ONDCP reported that the total federal drug demand reduction budget for FY 2001 was \$5.9 billion, of which the Department reported spending \$336 million for 19 drug demand reduction programs administered by the DEA, BOP, COPS, and OJP. Our audit of the Department's drug demand efforts found that the Department's report to the ONDCP did not accurately reflect its drug demand reduction activities, overstating by more than 50 percent the Department's actual funding of drug demand reduction programs. We identified 10 programs with total reported obligations of \$223 million that were not directly related to drug demand reduction. As a result, the Department's obligations directly related to drug demand reduction for the remaining Department programs were actually \$163 million, not the \$336 million reported in FY 2001.

The OIG audit also found that the performance indicators did not adequately measure the effectiveness of the Department's drug demand reduction programs. Further, the DEA did not establish any performance indicators for its drug demand reduction programs, even though drug demand reduction is one of the DEA's strategic objectives.

In addition, we found that the Department had not established a formalized mechanism for sharing drug demand reduction program information among its components.

Finally, we found that the DEA spent only \$3 million on drug demand reduction efforts in FY 2001 – two-tenths of one percent of its \$1.4 billion budget. The DEA's drug demand reduction efforts were largely conducted by its Demand Reduction Section, which consisted of 8 headquarters staff and 27 Demand Reduction Coordinators located in DEA field offices or other operational offices. The OIG's audit questioned the impact the DEA can achieve on reducing the demand for drugs with such a small percentage of its funding devoted to this effort. In response to this concern, the DEA indicated that it is completing an evaluation to determine the impact of the drug demand reduction program.

Within the past year, the OIG also has focused on efforts by components other than the DEA to reduce drug supply and demand. In January 2003, the OIG issued an evaluation of the BOP's drug interdiction activities (OIG Report #I-2003-002). Drug use by federal inmates represents a serious health and prison management problem. Drugs are in every prison. Moreover, while the BOP's national rate for positive inmate drug tests in 2001 was 1.94 percent, the statistics vary widely among BOP facilities. For

example, the high-security U.S. Penitentiary in Beaumont, Texas, posted a positive inmate drug test rate of 7.84 percent. In addition, 50 federal inmates have died from drug overdoses since 1997 and the BOP has recorded more than 1,100 “drug finds” in its institutions since 2000.

We determined that visitors, BOP staff, and the mail are the three primary ways drugs enter BOP institutions. The OIG concluded that the BOP fails to search visitors adequately, and that most of the BOP institutions we visited have an insufficient number of cameras, monitors, and staff to adequately supervise inmate-visiting sessions. In addition, the OIG concluded that the BOP has not taken sufficient measures to prevent drug smuggling by its staff. The report noted that interdiction activities common in many state correctional systems – such as random searches of staff or their property, or conducting random drug tests of staff – currently are not used by the BOP.

The OIG also concluded that an insufficient number of BOP inmates receive drug treatment to reduce their demand for drugs – a critical component of the BOP’s drug interdiction strategy – partly because the BOP underestimates and inadequately tracks inmates’ treatment needs. The BOP has estimated that 34 percent of all federal inmates need drug treatment. However, the OIG review determined that this figure is outdated and under represents the number of BOP inmates who need drug treatment.

In addition, the report concluded that the BOP does not provide adequate non-residential drug treatment in BOP facilities due to insufficient staffing, lack of policy guidance, and lack of incentives for inmates to seek such drug treatment. Even though the BOP states that non-residential treatment is a major component of its strategy to reduce inmates’ demand for drugs, non-residential treatment was limited or not available at five of the institutions visited by the OIG.

The OIG report made 15 recommendations to help improve the BOP’s efforts to prevent drugs from entering its institutions, including implementing “pat” searches of visitors; investing in additional cameras, monitors, and ion spectrometry technology to detect drugs; implementing policies to restrict the size and content of property that staff bring into institutions; implementing a policy regarding searching staff and their property when they enter BOP institutions; implementing random drug testing for staff; and implementing additional non-residential treatment programs for inmates in the general population. The BOP agreed with many of the recommendations, and is in the process of implementing various corrective actions.

In sum, reducing the supply of illegal drugs, reducing the diversion of legal prescription drugs for illegal use, and reducing the demand for legal drugs are critical ongoing challenges for the Department.

Responses to the Office of the Inspector General's List of the Ten Most Serious Management Challenges

1. Counterterrorism

The Department must manage its counterterrorism programs while coordinating with other intelligence agencies and law enforcement entities, as well as ensure that the CT funds are spent in an effective manner.

Issue 1.1: As of September 2002, the FBI had not performed and incorporated into its planning system a comprehensive assessment of the threat of terrorist attacks on United States soil. Such an assessment would be useful to define the nature, likelihood, and severity of the threat, as well as to identify intelligence gaps and determine appropriate levels of resources to effectively prevent and combat terrorism.

Action: The FBI completed a comprehensive national assessment of the terrorist threat to the US homeland based on comprehensive intelligence. The national threat assessment, "The Terrorist Threat to the U.S. Homeland: An FBI Assessment" was distributed beginning 12/18/02. Terrorist groups were prioritized in tiers by their intent to harm the U.S. homeland, their links to al Qaeda, and their capabilities. The prioritization of groups does not mean that those lower-tiered groups are necessarily less threatening. Each threat to the U.S. must be investigated, and each is considered significant until proven otherwise. In addition, the FBI's Counterterrorism Division had each field office complete a field threat assessment. The Field Threat Assessment complements the national threat assessment by assessing the risk of the threat facing the United States on a field division level. Each field division reported the terrorist presence, and the methods/operations in use by terrorists and/or their supporters in their respective areas. These two assessments along with the FBI's Annual Field Office Report will assist the FBI in identifying the nature, likelihood, and severity of the threat, as well as to identify intelligence gaps, and assist in determining appropriate levels of resources to effectively prevent and combat terrorism.

Issue 1.2: The Department needs to prepare to respond to terrorist acts and other critical incidents, as well as focus its efforts and resources to prevent acts of terrorism. Most U.S. Attorneys' Offices have not fully implemented effective response programs under the Crisis Management Coordinator (CMC) Program, implemented in 1996.

Action: EOUSA, Counterterrorism Section (CTS), and the United States Attorneys' Offices (USAOs) have undertaken extensive and comprehensive joint efforts during the past 2 years to enhance the Department's overall ability to respond to critical incidents. Legal training provided to United States Attorneys (USAs) and Assistant United States Attorneys (AUSAs), many of whom were CMCs, on crisis response responsibilities in terrorism incidents include EOUSA co-sponsored training with the Centers for Disease Control in April 2003 on responding to chemical or biological incidents; Department training for prosecutors and investigators on the USA PATRIOT Act and other changes in law relative to intelligence and law enforcement techniques and information sharing; and a broad array of training provided by EOUSA's Office of Legal Education and JTN broadcasts to USAOs and Department attorneys. In addition, CTS and EOUSA have scheduled crisis response training at the National Advocacy Center in March 2004. Other actions include a January 2003 antiterrorism conference for USAs, co-sponsored by CTS and EOUSA, in which a portion was devoted to a crisis response exercise; a March 2003 CMC-specific video-conference; and updated and specific guidance in the May 2003 revised "Guide to Developing a Model Crisis Response Plan" provided to USAOs. As a result, numerous USAOs are revising their plans.

Organizationally, CTS has reorganized its operations to include a Policy, Legislation, and Planning group to provide focus on crisis response issues and planning; and the Department has requested that the CMC Program and the Antiterrorism Advisory Council (ATAC) Program in the USAOs be merged and/or realigned to allow the CMC to operate under the ATAC in each district and to work closely with the District Office Security Managers to coordinate efforts on crisis response planning.

Issue 1.3: Prior to 9-11, the FBI devoted significantly more special agent resources to traditional law enforcement activities than it did to terrorism-related programs. Since 9-11, the FBI has reprioritized and refocused its investigative resources on counterterrorism-related issues, and this impacts other federal, state, and local law enforcement agencies.

Action: Since 9/11/2001, the FBI has shifted 671 field agents from field criminal investigations to augment counterterrorism-related investigations, implement critical security improvements, and support the training of new agents. These 671 agents were reallocated primarily from FBI drug investigations (553 agents moved), although some were shifted from white collar and violent crimes programs (59 from each program). Although the reallocation of criminal investigative resources is expected to have a significant impact upon white collar crime investigations (e.g., financial institution fraud) and support of state and local law enforcement in violent crime investigations, so far FBI drug investigations have felt the most immediate effects. Even though the performance goals of dismantling high-priority drug-trafficking organizations (i.e., CPOT-linked organizations) are on-track, dismantlements of other significant drug-trafficking organizations in FY 2003 were short of the targets set prior to the reallocation. The original FY 2003 target for dismantling non-CPOT-linked drug-trafficking organizations was 160 organizations; the FBI achieved 87 dismantlements of non-CPOT-linked drug-trafficking organizations in that time period. There is no doubt that the reallocation of agents from drug investigations impacted upon the FBI's accomplishments in FY 2003.

Issue 1.4: Much information relevant to counterterrorism and counterintelligence is in languages other than English. The FBI must ensure appropriate prioritization of translation work, accurate and timely translations of pertinent information, and proper security of sensitive information to avoid continued translation backlogs.

Action: The FBI's Foreign Language Program (FLP) centrally coordinates over 1,200 translators with operational division managers. This ensures its finite translator base is strategically aligned with priorities set on a national level. Monthly performance measures and reporting requirements have been instituted to identify translation performance gaps, to keep appropriate FBIHQ and field office managers informed of any translation deficiencies, and to benefit the FLP's workforce and budget planning. A comprehensive control system has been instituted to evaluate translation outputs for quality and security assurance. Each of these areas will be regularly evaluated and improved in FY 2004 and beyond by applying lessons learned.

Issue 1.5: The FBI needs to enhance its intelligence analysis capability.

Action: The FBI has established an Executive Assistant Director for Intelligence (EAD-I), an Office of Intelligence and Intelligence Program. Under the direction of the EAD-I, the "Human Talent for Intelligence Production Concept of Operations" was developed and approved. This CONOPS is the framework for the career development of the FBI's analytical cadre from recruitment to retirement. Based on this document, recruitment strategies for FY 2004 are in development, standardized minimum qualification requirements have been established and implemented, and one Intelligence Analyst position with a clear career path and functions has been established. The Office of Intelligence is working with the Training Division's College of Analytical Studies on enhancing the Basic Intelligence Analysts Course and identifying other appropriate training opportunities for Intelligence Analysts.

Issue 1.6: The Department must ensure that its increased funding for counterterrorism is used economically, effectively, and for its intended purposes. The Department's Counterterrorism Fund, created by Congress in 1995 after the bombing of the Murrah Federal Building in Oklahoma City and originally established to provide reimbursement solely to Department components, has, since 1996, used \$167 million from the Fund to support counterterrorism initiatives of non-DOJ agencies. Although JMD has improved its management of the Fund, additional improvements to the claims review process are needed.

Action: The Department has made every effort to ensure the AG's Counterterrorism Funds is used for its intended purposes. Any funds used to support CT efforts of non-DOJ agencies are either approved through the notification processes approved by OMB and the Hill or earmarked in a conference bill. JMD will continue to examine ways to enhance its oversight of the CTF.

Issue 1.7: The Department, in responding to the heightened terrorism threat, must use its law enforcement and intelligence-gathering authorities without inappropriately affecting the civil rights and civil liberties of individuals. A June 2003 OIG report recommended developing uniform arrest and detainee classification policies, improving information-sharing among federal agencies on detainee issues, improving the FBI clearance process, clarifying procedures for processing detainee cases, revising BOP procedures for confining aliens arrested on immigration charges who are suspected of having ties to terrorism, and improving oversight of detainees housed in contract facilities.

Action: The Department is committed to safeguarding the civil rights and civil liberties of all individuals. The Department's responses to the Inspector General's (IG) recommendations are outlined in the Department's written submissions to the IG dated July 21, 2003, and November 20, 2003.

2. Sharing of Intelligence and Law Enforcement Information

To help prevent acts of terrorism, the Department must share information with multiple entities in a timely manner while maintaining the security of sensitive information and limiting that information to those with a “need to know.”

Issue 2.1: The FBI lacks criteria for initially evaluating and prioritizing incoming threat information and lacks a protocol for when to notify higher levels of management, other units and field offices, and other agencies.

Action: 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. On 12/02/02, the CID established the 24/7 Counterterrorism Watch (CT Watch) for this purpose. A threat, as defined by PDD-39, and the Attorney General’s Guidelines, is any indication of planned violence against U.S. persons or facilities, including any persons or facilities located in the U.S. or damage to the U.S. national security or infrastructure. A threat can originate from individuals, terrorist groups, or other criminal elements. Threats are received and handled by several components of the FBI’s National Threat Center Section. These include the CT Watch, the Threat Monitoring Unit, the Strategic Information Operations Center (SIOC), and the Terrorism Watch and Warning Unit. All of these entities are purposefully integrated into the Section to ensure all threats, regardless of source and manner of communication, are appropriately reviewed, prioritized, and addressed. The CT Watch is the recipient of all terrorist-related threat and suspicious activity reporting for the FBI. It is the FBI’s 24-hour global command center for terrorism prevention operations. As the FBI’s “Threat Central,” it is the focal point for the receipt, preliminary analysis, and immediate assignment for action of all international and domestic terrorism threats, ensuring timely alert to FBI and DOJ executives, other government leaders/agencies, and field offices/Joint Terrorism Task Forces (JTTFs). The Threat Monitoring Unit has personnel assigned to the CT Watch and maintains the responsibility of tracking all threat and suspicious activity, in conjunction with the CT Watch. Details regarding criteria for evaluating threat and suspicious activity were detailed in an FBI memorandum to the IG earlier this year in response to the OIG’s report, “A Review of the FBI’s Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management.”

Issue 2.2: 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.

Action: The FBI has made improvements to its training process for intelligence analysts. Also, it has hired a new EAD-I who has embarked on substantial improvements to the intelligence processes with the FBI.

Issue 2.3: Long-standing systemic problems in the FBI's counterintelligence program and a flawed internal security program that resulted in the Robert Hanssen espionage activities emphasized the need for improved coordination and information sharing within the Department.

Action: The FBI's Security and Counterintelligence divisions are strengthening their cooperative relationship with the establishment of several initiatives. The FBI's Counterintelligence Division (CD) created the Counterespionage Section which is organized by country and issue. Within this section the internal penetration unit is tasked with strictly investigating all anomalies, Section 811 referrals, and any other allegations that the FBI has been penetrated by a foreign intelligence service. The FBI Security Division made 11 Section 811 referrals to CD in 2002. The divisions also revised policy for handling Recruitments in Place and defectors; developed a prototype to capture clearance-related information and sharing the information for investigative needs; expanded the requirement for counterintelligence-focused polygraph examinations; ensured that counterintelligence and counterespionage programs are nationally driven, centralized, and managed at the Headquarters level; and implemented a comprehensive security education and awareness training program.

Issue 2.4: The lack of an integrated automated fingerprint system hinders the Department, DHS, and state and local law enforcement agencies from sharing valuable immigration and law enforcement information about detained or apprehended persons.

Action: IDENT/IAFIS workstations enabling DHS to conduct checks of IAFIS within 10 minutes have been deployed to more than 100 DHS field sites. DHS has plans to continue extensive deployment of this capability during FY 2004. Included in the 100 sites that are currently operational are 41 "metrics" sites from which data is being collected to estimate the DOJ and DHS operational impacts of improved identification capabilities at the border. Data collection and analysis will continue through FY 2004, leading to projections of "downstream" impacts and decisions as to how best continue the integration effort, including how DHS apprehension data can be shared with other federal, state and local law enforcement. At this time, DHS is intending to use the IDENT system as an initial foundation for its new US VISIT Program. JMD and FBI are working with DHS to determine the impact of that program on the future of IAFIS and the integration project.

3. IT Systems Planning and Implementation

Employees rely on complex and often interrelated IT systems to meet challenges ranging from sifting through thousands of leads in a criminal investigation to developing annual financial statements.

Issue 3.1: The FBI must be able to use its IT systems to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. Deficiencies in the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training can impede the FBI's ability to meet this goal. To effectively manage its IT investments, and avoid "stovepipe" systems, the FBI must implement critical management processes. This has led to spending hundreds of millions of dollars on IT projects without adequate assurance that these projects would meet their intended goals.

Action: The FBI's new Investment Management Program (IMP) is in place. IMP policies and procedures are available on the FBI intranet and have been communicated to all FBI divisions through briefings with each Assistant Director. Building on the lessons learned from the "select phase" pilot in FY 2003 and the tenets of the General Accounting Office ITIM Framework, the FBI is extending investment management key practices to the "control phase." The first executive Program Management Review was completed in November 2003, and will be held each quarter. Plans for training FBI employees in key practices, such as writing effective business cases, conducting cost/benefit analyses, and applying earned value management are planned to begin in December 2003. Closer partnership with the Finance Division will drive more effective prioritization and management of the FBI's IT portfolio and all projects, whether IT or not, with life cycle costs of \$10 million or more. The FBI is also working closely with the Justice Management Division to align its IMP process with the DOJ ITIM process for all phases (select, control, and evaluate). The Department and the FBI are committed to the development, implementation, and maintenance of solid enterprise architecture (EA) programs. Within the FBI, EA plays an important role in effectively managing large and complex modernization programs. Furthermore, the FBI and JMD are developing a detailed work plan for addressing EA throughout the FBI. As evidence of the improved processes, 17 of 30 open OIG recommendations from the 2002 ITIM audit have been closed.

4. Computer Systems Security

DOJ's IT security program requires additional improvement at both the Department and component levels, particularly in program oversight and vulnerability management, to protect computer systems and reduce the number of vulnerabilities within the Department's IT systems.

Issue 4.1: The Department's functions have not been centralized sufficiently to provide the vigorous enforcement oversight supported by a substantial, technically proficient work force that the Department needs.

Action: In May 2003, the CIO restructured the Department IT Security Program to assume responsibility for policy and oversight of IT security. An updated policy has been developed and is awaiting signature by the AAG/A to reflect this centralization of IT security. A Deputy CIO position, with direct responsibility for IT security, was filled in June 2003. The CIO realigned internal resources to identify additional positions to support the Deputy CIO and the IT Security Staff. This represents an increase of 100% over the original staffing level. Aggressive recruiting is underway to identify a technically proficient workforce to meet the Department's needs.

Issue 4.2: Vulnerabilities exist in the management, operational, and technical controls that protect each departmental system from unauthorized use, loss, or modification.

Action: The IT Security Council (ITSC) and seven Project Management Teams were designated to carry out key activities and manage implementation of 17 individual IT security standards. The teams are currently establishing independent test cases, schedules, and metrics for each of 230 management, operational, and technical risk control objectives and implementing a web-based Automated Security Evaluation and Remediation Tracking (ASSERT) system to support updating of independent test cases, managerial oversight of corrective action plans and FISMA reporting.

Issue 4.3: There are inconsistencies in the oversight of computer security due to the bifurcation of responsibility between the JMD Security and Emergency Planning Staff and the JMD Information Management and Security Staff.

Action: In an effort to eliminate the bifurcation of responsibilities between JMD staffs, the CIO restructured the Department IT Security Program to assume responsibility for oversight of computer security. An updated policy has been developed and is awaiting signature by the AAG/A to reflect these changes in the program. Oversight Responsibility for National Security Systems transitioned to the CIO in revised DOJ Order 2640.2E (release pending).

Issue 4.4: Weaknesses in SENTRY, BOP's primary mission support database, occurred because BOP management did not fully develop, document, or enforce BOP policies in accordance with current Department policies and procedures.

Action: BOP recognizes the weaknesses identified in 4 of the 27 Federal Information System Controls Audit Manual control areas tested. Although these areas are not considered major weaknesses and the SENTRY system is assessed as low risk, BOP and the Department (Office of the CIO) continue to work collaboratively to correct the areas. By ensuring even low risk assessments are given appropriate reviews, BOP and the Department establish assurances that security vulnerabilities will not impair BOP's ability to fully ensure the integrity, confidentiality, and availability of data contained in SENTRY. In addition to the weaknesses identified, BOP will enforce the BOP Policy Standards and existing access control policy, update the SENTRY System Security Guide and provide the Information Security Officer with the exception reports from the system audit logs.

Issue 4.5: The FBI's Automated Case Support (ACS) system has security flaws, discovered during the review of the Hanssen case. These include the ability to override access restrictions to ACS, improper uploading of documents or inadequate restriction codes, rare use of the audit function.

Action: The FBI Information Assurance Program is providing active certification support to the Trilogy/Virtual Case File (VCF) Program to include the Beta Test of the Local Area Network (LAN) and the development of New Agents' training. The Certification Unit provides the security consultation services to deliver the assurance of confidentiality, integrity, and availability through the security certification process which monitors the implementation of security policy and the remediation of the vulnerabilities identified in the ACS and related legacy systems and networks.

5. Financial Management

Antiquated and ineffective automated accounting systems and decentralized financial management threaten the Department's ability to maintain its unqualified opinion.

Issue 5.1: The Department lacks automated systems to readily support ongoing accounting operations, financial statement preparation, and the audit process. Its capability to provide current, timely, and accurate financial information to managers remains limited. It will be difficult for the Department to maintain a clean audit opinion for FY 2004 and future years and meet the expedited reporting dates unless it modernizes and streamlines its financial management systems.

Action: DOJ is planning a major systems replacement project which will provide a single Unified Financial Management System across the agency, and which will support timely access to key financial and selected performance data for leadership decision making. The first step in this process is the implementation of the Hyperion Financial Management (HFM) tool to facilitate the preparation of the FY 2004 individual and consolidated financial statements. DOJ accelerated the FY 2003 deadline for submitting the audited financial statements to the Office of Management and Budget by 30 days. During March 2003, DOJ issued the FY 2004 financial statement preparation time line designed to meet the accelerated November 15th deadline and the accelerated quarterly reporting deadlines. DOJ has also implemented revisions to internal business practices to improve quarterly accounting data and accelerate quarter and year-end closeouts.

Issue 5.2: Problems related to financial accounting and reporting in FY 2002 were overcome only by significant year-end manual efforts. This will not be possible for FY 2004 because component audits must be completed within 14 days of the end of the fiscal year.

Action: Senior managers are performing ongoing financial reviews and program evaluations. Financial oversight reports are available and offices are encouraged to monitor expenditures and allotments on a monthly basis to improve the integrity of the accounting data.

Issue 5.3: Component financial and other automated systems are not integrated and do not readily support the production of financial statements and other required financial reports. Consequently, production of Departmentwide information must be done manually or by duplicate inputting of data.

Action: In FY 2002, the Department initiated the Unified Financial Management System (UFMS) project to replace the seven major accounting systems used throughout the Department. Key milestones in completing the implementation of the UFMS project include the award of the Commercial Off-the-Shelf Software (COTS) contract in the 2nd quarter of FY 2004, the award of the Integration and Implementation (I&I) contract and completion of the product acceptance testing in the 4th quarter of FY 2004.

Issue 5.4: Several of the older systems used by components predate the current accounting requirements and do not support the production of timely, relevant information that is needed for preparing financial statements or performing accrual accounting transactions.

Action: The objective of the UFMS Program is to significantly improve DOJ-wide financial management and program performance reporting by making financial reporting more timely, relevant and accessible and to re-engineer DOJ business practices to move away from the widely different and outdated systems and practices, adopting uniform business practices.

6. Grant Management

The size, diversity, and complexity of DOJ's grant programs result in challenging management demands.

Issue 6.1: The Department's federal financial assistance programs are fragmented, resulting in reduced efficiency and increased costs to award and administer federal financial assistance funds to state and local agencies.

Action: Funds from both COPS and OJP assist state, local, and tribal law enforcement. COPS grants are unique because every grant dollar awarded by the COPS Office must, by statute, be used to advance community oriented policing, a strategy credited with reducing crime and the fear associated with crime and with building trust between law enforcement and citizens. In addition, funds under the COPS Office hiring programs support 3 years of officer salaries to advance community policing. In contrast, while a grantee can choose to use OJP LLEBG funds to support community policing activities if the grantee so desires, it is not a requirement that recipients of LLEBG funds must engage in community oriented policing. In addition, LLEBG grants are 1-year grants. Potential grantees are selected for awards from different pools, under different funding criteria. All state, local, federally recognized tribal, and public law enforcement agencies, as well as jurisdictions serving special populations (e.g., transit, university, public housing, schools, and natural resources), are eligible to apply directly to the COPS Office for funding. In addition, jurisdictions wishing to establish new police agencies are eligible to apply for COPS hiring and technology grants.

OJP began an internal reorganization in FY 2001 intended to streamline its functions. OJP merged programs and staffs of the Corrections Program Office and the Drug Courts Program Office into the Bureau of Justice Assistance to consolidate overlapping functions, reduce management redundancy, and improve coordination and communication. An Office of the Chief Information Officer (OCIO) was created to address important mission-critical systems and the need for an agency-wide grants management system and management information system. OJP merged the Office of Congressional and Public Affairs and other information dissemination functions into one office. OJP will merge the programs, functions, and staff of the Executive Office for Weed and Seed and the American Indian/Alaska Native Affairs Desk into the Community Capacity Development Office. Also, OJP plans to merge several administrative and support functions into the Office of Management and Administration. Collectively, these actions will move OJP toward greater centralization of management and improved communication and coordination across organizations and programs.

Issue 6.2: There are overlaps between OJP and the COPS Office, and no formal communication procedures exist between them to ensure that grantees do not receive funds for similar purposes from both agencies.

Action: Prior to the audit, the COPS Office and OJP already had a practice of informally coordinating with each other on a variety of other matters. Accordingly, in furtherance of this practice of mutual collaboration and coordination, both offices agree to formalize their coordination by, first, comparing program descriptions as soon as they become available in the fiscal year to identify programs that contain the same allowable uses and, second, if necessary as a result of the first step, ensuring that the relevant program managers from each office coordinate on a case-by-case basis to guarantee that duplicate awards are not made to the same grantee for the same purpose.

Issue 6.3: COPS has not developed a capability to receive grant applications on-line and to download the information directly into its grant management system. Grantees must submit applications on paper and COPS must manually input the data into its tracking system.

Action: To allow agencies to apply for COPS funding at Grants.gov, COPS is identifying the agency specific data not used on standard grant forms so that COPS grant application forms can be available for applicant submission. (Target date of 5/1/2004.) COPS will be compliant with OMB directive of 11/7/2003 that all grant funding opportunities be posted at the eFind portion of Grants.gov using the standard OMB approved template. With assistance of the Business Practices Group, COPS will begin implementation of a single grant application package for all grant programs based on the SF 424 which will allow for easier integration with Grants.gov.

Issue 6.4: OJP does not have a fully effective automated system to manage its federal financial assistance funds and has multiple automated application systems in place. Despite having these automated systems to help manage its funds, OJP still relies primarily on a manual system for processing grants.

Action: In continuing to respond to the President's goal to improve the delivery of government services to citizens, OJP's Grants Management System (GMS) has become a more streamlined, Web-based tool that makes processing grants easier and faster. The system provides automated support throughout the grant life cycle for OJP staff, grant applicants and grantees. This support includes applicant registration, application submission and review, award approval and distribution, payment, monitoring, closeout, and decision support. By using GMS, the award process, which took an average of 3 months to complete under the old paper-based system, now averages 3 weeks to complete. In FY 2003, 96 percent of OJP grants were administered through a centralized paperless system.

7. Performance-Based Management

The Department must ensure, through performance-based management, that its programs are achieving their intended purposes.

Issue 7.1: Many performance measures are not focused on outcomes or are not quantifiable and verifiable. This is a critical component of performance-based management. Also, performance-based accomplishments are necessary to the Department's planning and priority setting.

Action: In tandem with the revision to the strategic plan, the Department developed long-term outcome oriented performance measures and targets. These measures were approved by OMB and many were included in related program PART evaluations.

Issue 7.2: Deficiencies in DEA's performance measures diminish the ability of the DEA, the Department, Congress, and the public to assess the effectiveness of the DEA's performance.

Action: In its new Strategic Plan, reviewed favorably by DOJ and OMB, DEA established strategic goals and objectives that are quantitative and directly measurable. Goals for disrupting and dismantling Priority Target Organizations (PTOs) are based on a trend analysis of actual performance results, and these trend analyses will continue each quarter on a routine basis. The Priority Target Activity and Resource Reporting System (PTARRS) has acceptable controls for the Domestic Enforcement DU indicator, and now includes the International Enforcement indicators as well. DEA is consolidating reporting capabilities of several already existing Diversion Control systems, and procedures and controls are in place to verify the performance data reported. Work continues on an impact assessment methodology (using several existing DEA systems) which will support reporting on reduction in drug availability, and include appropriate controls for data verification. DEA was one of the agencies reviewed during 2002 by OMB with its Program Assessment Rating Tool (PART) for implementation of the GPRA program. In January 2003, DEA developed an action plan for improvement. Progress has been so significant that DEA's current PART score from OMB is 59% (using the FY 2005 version of the tool) a 127% improvement. The increase in the strategic planning section was from 1% to 9% out of a possible 10% weighted score. DEA's budget requests (FY 2004 and 2005) are explicitly tied to accomplishment of the annual and long-term goals, and resources needs are presented in a complete and transparent manner in the budget. DEA has also improved its collection of performance information, and used it to manage the program and improve performance, as well as to collaborate and coordinate effectively with related programs, such as the Bureau of Immigration and Customs Enforcement, as well as the HIDTA and OCDETF programs. With regard to strong financial management practices, DEA is on track to receive a good audit opinion again this year. Concerning the overall FY 2005 assessment, OMB has indicated they recognize DEA's diligence and progress in more than doubling its PART score. Accordingly, OMB gave favorable consideration to DEA's FY 2005 OMB budget request.

8. Human Capital

All DOJ components must hire, train, and retain adequate personnel to handle the myriad duties of the Department. The increasing technical and sophisticated nature of the Department's work, coupled with the competition for qualified employees increases this challenge. This challenge negatively affects other management challenges, including countering terrorism.

Issue 8.1: The demand for employees with language skills throughout government, especially proficiency in Middle Eastern and Asian languages, affects the Department's ability to attract and retain qualified special agents, intelligence analysts, and language professions.

Action: In September 2003, DOJ awarded a contract for a Department wide Workforce Analysis and Planning Initiative. The project will link workforce requirements to DOJ strategic goals, identify skill gaps (such as lack of language skills) by each occupational series, and recommend ways to fill identified gaps. The project is expected to be completed by July 2004. The FBI's National Recruiting Team targets diverse and specialty conferences, career fairs, and other meetings of those with the "most wanted" skill sets and backgrounds for Special Agent (SA) and other positions. Ongoing efforts include targeting foreign language departments within colleges and universities, and advertising on foreign language web-sites, newsletters and magazines. Field Offices implemented local advertising and recruitment strategies in FY 2003 and have been advised to immediately process SA linguists for testing. In August 2003, the FBI issued a press release announcing its immediate need for Agent applicants who possess a fluency in Middle Eastern languages and other languages critical to the FBI's mission. The Bureau has also contracted with an advertising agency to develop a foreign language media plan for recruitment and marketing strategies. The FBI has aggressively recruited and processed several thousand translator applicants since October 1, 2000. During this period, it has more than doubled its complement of translators proficient in Middle Eastern and Asian languages. These efforts will continue through FY 2004 and beyond, consistent with the availability of additional funding, to ensure sufficient translator resources are available to meet growing translation demands in a wide array of languages.

Issue 8.2: Past FBI shortages of linguists have resulted in thousands of hours of audiotapes and pages of written material not being reviewed or translated in a timely manner.

Action: (See response to Issue 8.1 above.)

Issue 8.3: Several components lack adequate staff to perform many of the tasks needed to produce financial statements. Consequently, the Department continues to rely heavily on contractors to prepare financial statements which, in addition to affecting the expense associated with producing the statements, contributes to diminishing the institutional knowledge and expertise. Components have difficulty recruiting and retaining highly qualified IT specialists who are knowledgeable about the latest hardware and software. As a result the components have found it difficult to address some of the IT issues identified in the financial statement audits.

Action: The Department has established continuous milestones to improve job performance in the financial management area. These include financial management training programs, Financial Management Information System training for new employees, Department-wide training

programs to all employees on applicable systems information and methodology. While several bureau staffs receive support and oversight from contractors to prepare the financial statements, the demands for personnel resources have also increased. Personnel resources are needed to meet the challenges of quarterly reporting and accelerated due dates. Management has been supportive by approving adequate resources to meet these challenges.

Issue 8.4: The Department lacks fair and consistent methods of addressing allegations of employee misconduct.

Action: In November 2000, the Department implemented a training program to help components achieve greater consistency and success through specific guidance on taking defensible disciplinary actions and applying relevant disciplinary factors effectively. This training has helped improved the Department's ability to take action and successfully defend the actions it takes and litigates before third parties, such as the Merit Systems Protection Board. Since implementing the training, the Department has improved its affirmance rate by 18.3%.

Issue 8.5: The discipline imposed by the USMS in addressing allegations of employee misconduct is inconsistent, and reasons for the discipline decisions are not adequately documented. There are periods of unexplained elapsed time that appear to prolong case adjudication.

Action: This was closed in March 2002. As a result of the OIG study, the USMS provided clear instructions to all USMS managers and the Discipline Panel regarding documentation requirements for misconduct cases. The Employee Relations team implemented new procedures for discipline actions involving suspensions and time lines for misconduct case adjudication, not to "drive the process," but to ensure it moved along at the proper pace to ensure due diligence.

Issue 8.6: DEA's disciplinary system has inadequate guidance and dual mitigation, resulting in penalties that appear to be too lenient; improper consideration of external factors by the Board and Deciding Officials when making disciplinary decisions; failure to adequately document disciplinary decisions by the Board and Deciding Officials; failure to monitor the timeliness of the process; and a lack of oversight over the Deciding Officials.

Action: DEA is awaiting the final draft of the OIG's discipline audit and will provide formal comments once it is received. DEA's Office of Chief Counsel disagreed with the working draft regarding the OIG's interpretation of dual mitigation. Meanwhile, DEA is preparing an action plan to address the following: updating agency guidance; instituting a revised table of penalties to ensure that penalties are appropriate; reinforcing existing DEA policy to ensure that the Board of Professional Conduct and the Deciding Officials consider only the appropriate factors when making disciplinary decisions; implementing the personnel database that will monitor the timeliness of all phases of the discipline process (currently OPR tracks its performance for timeliness); and ensuring that the Deputy Administrator's Office reinforces its oversight of the Deciding Officials.

9. Protecting the Security of DOJ Information and Infrastructure

The Department needs to share intelligence and law enforcement information with a wider audience, and, at the same time, protect the security of that information. To do both, the Department must secure its buildings, computers, and communications systems.

Issue 9.1: Throughout the years of Aldrich Ames' espionage, the FBI devoted inadequate attention to determining the causes of the sudden, unprecedented, and catastrophic losses suffered by both the FBI and the CIA. In particular, the FBI was unable to provide the OIG review team with a definitive answer concerning the distribution of various top secret documents. The OIG review of the Hanssen case found this and other recommendations from the Ames matter had not been sufficiently implemented. The FBI did not employ basic personnel security techniques. The FBI also had inadequate document security and computer security. The computer system's audit function was rarely used.

Action: The FBI's Security Division was created in December 2001. With the creation of this new infrastructure, the FBI has intensified its focus on security by introducing new programs. For example, the personnel security function has expanded its capabilities to protect the FBI against counterintelligence and counterterrorism threats. Specifically, the Security Division has expanded the polygraph program, initiated a financial disclosure program, created an analytical integration unit to offer enhanced analysis of complex cases, and adopted a more risk based approach to personnel security matters. In addition, the Security Division has appointed an Secure Compartmentalized Information (SCI) Program Manager who is focused on ensuring compliance with the FBI, DOJ, and Director, Central Intelligence Directives related to the creation, handling, and destruction of Top Secret/SCI materials. When necessary, the program manager enhances or revises FBI policy or guidance in order to comply with commonly accepted intelligence community standards. Finally, the FBI has established the Enterprise Security Operations Center (ESOC) with a mission to monitor and protect the FBI's information systems from external attacks and insider misuse and assure the availability, confidentiality, and non-repudiation of FBI information through techniques such as near real time network monitoring, intrusion detection, and data auditing. ESOC IOC will implement the following capabilities: intrusion detection and network defense, monitoring advanced indications and warnings, Computer Incident Response Capability (CIRC), audit capability, storage, correlation, analysis, and data aggregation, reporting capability, vulnerability, and penetration assessments, e.g., Red Teaming, malicious code and virus protection, and incident re-creation and testing. The ESOC began monitoring the FBI's most sensitive information system in October 2003.

Issue 9.2: The Department's ability to perform vital missions is at risk from terrorist attacks or similar threats because it has not adequately planned for the protection of its critical physical assets.

Action: The Department has completed an inventory of its critical physical assets and is developing plans to strengthen vulnerabilities.

Issue 9.3: To strike the appropriate balance between sharing information and protecting the security of that information, the Department must achieve full operating capability, which is the ability to protect critical infrastructures from intentional acts that would significantly diminish the ability to perform essential national security missions and ensure general public health and safety.

Action: The Department has initiated an effort toward full operational capability. Included in this effort will be the identification of all critical assets, completion of key milestones for establishing interdependencies, review of vulnerability assessments, development of mitigation and contingency plans. The Department is intricately involved in the Department of Homeland Security Project Matrix. The Department completed Step 1 in September 2003 and started Step 2 in October. Step 2 involves identifying the infrastructure necessary to perform and provide each nationally critical function or service.

10. Reducing the Supply of and Demand for Drugs

The challenge with regard to reducing supply extends beyond illegal drugs to reducing the diversion or misuse of legal drugs. And, reducing the supply is only part of the challenge; efforts to reduce the demand for drugs also are necessary.

Issue 10.1: The illegal diversion of prescription drugs for non-medical purposes is a growing and staggering problem. In order to counteract the widespread problem of controlled pharmaceutical diversion, it is critical for the DEA to devote more resources to it. A September 2002 OIG report found that the DEA dedicated only 10 percent of its field investigator positions to diversion investigations. DEA failed to provide sufficient DEA special agents to assist diversion investigators in conducting investigations of controlled pharmaceutical diversion. Diversion investigators lack law enforcement authority and therefore must request either DEA special agents or local law enforcement officers to perform essential activities. Difficulties in obtaining law enforcement assistance caused delays in developing cases for prosecution. The quality of investigations also has suffered because investigators external to the diversion control program lack experience in conducting controlled pharmaceutical investigations. DEA provides minimal intelligence support to its diversion investigators. The one potential intelligence resource available to diversion investigators is the Automation of Reports and Consolidated Orders System (ARCOS). It contains information on the inventories, acquisitions, and dispositions of certain controlled pharmaceuticals, as reported by manufacturers and distributors. However, diversion investigators told the OIG that ARCOS reports are limited in their value as an intelligence resource because of problems of completeness, accuracy, and timeliness. Also, diversion staff at headquarters indicated that they did not have the adequate resources to analyze and develop ARCOS data into useful intelligence products.

Action: To counteract the widespread problem of controlled pharmaceutical diversion and address difficulties in obtaining law enforcement assistance, DEA has submitted a proposal to, and is awaiting a response from, the Department to convert the Diversion Investigators (DI) to full law enforcement status. In its FY 2005 Budget Submission to OMB, DEA requested an additional 2 new DI positions. DEA has dedicated specific resources to the re-engineering and modernization of ARCOS and the CSA program to develop and enhance a network with state and local enforcement and regulatory counterparts; establish a data warehouse of all diversion information for use by field investigators; maintain the Diversion Control Program (DCP) website, which is a major conduit for information to the regulated communities; and provide registrants with the ability to report mandated information through electronic data interchange. DEA has explored additional intelligence capabilities to support DIs, Special Agents, other law enforcement agencies, and the general public. DEA plans to update the Controlled Substances Information System (CSIS). Also, through the E-Commerce Initiative, DEA will continue to develop and deploy a closed system for ordering and prescribing controlled substances to enable the safe electronic transmission of prescriptions and ordering of controlled substances.

Issue 10.2: An OIG audit found that the Department's performance indicators did not adequately measure the effectiveness of its drug demand reduction programs. Further, DEA did not establish any performance indicators for its drug demand reduction programs. The Department had not established a formalized mechanism for sharing drug demand reduction program information among its components.

Action: In July 2003, DEA implemented a quarterly reporting policy to authenticate the collection of data to support the pre-existing performance indicators in the DEA budget submission. These performance indicators measure the activity of DEA's demand reduction activities.

Issue 10.3: Two-tenths of one percent of DEA's \$1.4 billion budget is a very small percentage of its funding to impact reducing the demand for drugs.

Action: DEA is conducting an evaluation of its program, including an analysis of use of resources and assessment of impact within affected communities. The report will be completed in January 2004.

Issue 10.4: Drug use by federal inmates is a serious health and prison management problem. In a January 2003 report, the OIG concluded that BOP fails to search visitors adequately; most BOP institutions (that the OIG visited) have an insufficient number of cameras, monitors, and staff to adequately supervise inmate-visiting sessions; and BOP has not taken sufficient measures to prevent drug smuggling by its staff.

Action: Policy revisions and internal auditing guidelines are being completed to address the issues identified in the OIG's report.

Issue 10.5: An insufficient number of BOP inmates receive drug treatment to reduce their demand for drugs. BOP does not provide adequate non-residential drug treatment in BOP facilities due to insufficient staffing, lack of policy guidance, and lack of incentives for inmates to seek such drug treatment.

Action: BOP is in the process of implementing various corrective actions.

This page intentionally left blank.