

(WMDD) new Intelligence Analysis Section, the WMDD worked with the Directorate of Intelligence (DI) to establish an aggressive hiring strategy to identify individuals with experience in biological, chemical, or nuclear sciences.

Career paths that reward and develop technical experts in intelligence operations are essential to the FBI's ability to retain a world-class national intelligence workforce. Recently, the FBI implemented a national security career path, allowing analysts, agents, linguists and surveillance specialists to develop specialized skills and experience in priority areas. It is developing career paths for Intelligence Analysts (IAs) that will allow them to pursue technical, as well as management, paths in their chosen jobs. The FBI has achieved a key milestone by extending the IA career path in field office from the GS-12 level to the GS-14 level in field offices.

The DI training management has been included in the New Agents and National Academy Curriculum Committees. The DI also controls the curriculum for the intelligence career services (ICS) Cohort Program. The Training and Development Division is scheduling ICS Cohort Program and New Agent classes to start on the same days in FY 2007 so that some of the in-processing and administrative matters may be covered jointly. Throughout FY 2006, NSB supported 11 joint exercises for new agents and IAs, offering analysts and agents an opportunity to work together on simulated cases while learning each other's roles in the investigative process and the intelligence cycle. This initiative is a derivative of the interaction between New Agent Training and the ICS Cohort Program.

Issue: The effectiveness of the FBI – in particular the FBI's leadership in various areas including counterterrorism – has suffered because of a lack of continuity due to frequent turnover among all levels of management at headquarters and in the field.

Action: FBI special agents join the bureau at an average age of 30, and are eligible for retirement at age 50 with 20 years of service. These agents are most valuable to the FBI at the very stage when they are eligible to retire, when many are highly marketable in the private sector as well. Even the most dedicated agents may find it difficult to remain with the FBI after they are eligible for retirement, particularly when faced with the prospect of transferring to a high-cost area to advance their FBI career. Further, family and education obligations also may be at the highest levels at this point.

To address this issue, the FBI has launched a number of initiatives. Representatives of the FBI's Executive Development and Selection Program (EDSP) are developing a database designed to assist in Senior Executive Service (SES) succession planning. The FBI's Training and Development Division is formulating an "FBI Leadership Training Framework" that will provide the basis for a comprehensive leadership development program. The Strategic Leadership Development Plan will provide techniques for identifying leadership needs and problems; articulate a program designed to enhance leadership knowledge, skills, and abilities throughout an employee's career; and relate leadership development to the FBI's strategic mission in its top priority programs. The FBI is evaluating several possible measures to lengthen tenure in SES positions, particularly at FBI Headquarters, including the increased use of retention bonuses and other incentives. The FBI will continue to explore options for retention, including the enhanced use of a variety of financial incentives and staffing flexibility in order to help the FBI cope with these factors.

Issue: Although the FBI recently has made progress in improving its management of IT upgrades, agents and analysts will not benefit from a fully functional case management system for several more years.

Action: The FBI has established a realistic timetable to incrementally design, develop, integrate, test, and implement SENTINEL in four phases. Each phase will introduce new capabilities and provide greater access to existing information, while easing user transition, training, deployment, and support. Phase 1 is scheduled for delivery in April 2007, and will provide immediate benefits to agents, analysts, and supervisors by providing a web-based interface to legacy data. It also will allow users to better manage their workload by pushing their cases, leads, and action items to their personal workboxes. Phase 2, scheduled for May 2008, will provide greater document management and will automate workflow.

Issue: The FBI does not always allocate agents responsible for maritime security according to the threat and risk of a terrorist attack on a given seaport.

Action: The FBI's Counterterrorism Division is in the process of reformulating a previously submitted answer to this issue, which will be forwarded to FBI Inspection Division and subsequently to DOJ OIG by an 11/06/2006 deadline.

2. Sharing of Intelligence and Law Enforcement Information

Challenges to sharing information are addressed under Challenge 3, “Information Technology Systems Planning, Implementation, and Security,” and Challenge 9, “Civil Rights and Civil Liberties.”

3. Information Technology, Planning, Implementation, and Security

Issue: The OIG has found that the Department lacks the ability to track the cost of its major IT systems and exercises little direct control over components’ IT projects. Historically, Department components have resisted any form of centralized control over major IT projects, and the Department’s Chief Information Office (CIO) does not have direct operational control of component IT management. The OIG believes the Department should consider providing increased control to the CIO for certain high-risk functions and for individual components experiencing difficulty with particular IT systems. These high-risk functions may include hiring for critical positions, completion of system requirements, and oversight of contract administration.

Action: The DOJ traditionally has followed a de-centralized management approach, which is not conducive to intense control over component programs and systems. In the last four years, however, the Department has put some mechanisms in place to help the Deputy Attorney General (DAG) and the CIO provide better oversight of high risk or problem projects. One such mechanism, the Department Investment Review Board, chaired by the DAG with the CIO as Deputy Chair, meets approximately twice a month to review progress and issues related to major Department IT programs.

The CIO will put forward a recommendation to the DAG for improving the control, management, and oversight of large, expensive IT projects at both the Department and the component levels. For the Department to gain more control of high risk functions, there would need to be significant structural changes made to its budgeting, hiring, and contracting processes. Fundamental changes internally, with the components, and on the Hill are needed to help persuade the components to act more like a single organization and use “corporate assets” rather than expand their own infrastructure and support systems for their IT needs.

Issue: The FBI has not yet fully staffed the SENTINEL Program Management Office, and there is still uncertainty over risk mitigation, contingency planning, and total project costs of SENTINEL.

Action: The SENTINEL Project Management Office (PMO) has adjusted its staffing level to be funded for 73 positions. Currently, it has a staff of 65 persons, and has been actively recruiting an intelligence analyst and a training planner. Six Operations and Maintenance positions are being actively recruited. The PMO reviews staffing on a weekly basis and has successfully filled what it considers to be normal attrition since the inception of the project.

The FBI has instituted a risk management process to identify and mitigate the risks associated with the SENTINEL project. The process is managed by the SENTINEL Program Manager and a Risk Review Board that meets biweekly. The most significant risks identified are examined at monthly Program Management Review sessions and other SENTINEL oversight meetings, in accordance with the FBI’s Life Cycle Management Directive. In addition, the risks, along with other significant program information, are presented to the FBI Director and his senior leadership team weekly; to a combined senior review team from DOJ, OMB, and DNI monthly; to the CIO Advisory Council on a bimonthly basis; to the FBI Director’s Advisory Board when called on; and quarterly to any/all of the eight Congressional oversight committees that review the progress of SENTINEL. The PMO currently is developing contingency plans for all medium and high risks, in accordance with the FBI’s risk management plan.

The FBI is committed to delivering SENTINEL on schedule and within budget. The Independent Government Cost Estimate is an estimate showing realism for proposal evaluation purposes. Market changes in labor and rapid changes in commercial off-the-shelf (COTS) technology are the prime reasons for variances. The PMO has been updating the OMB300 and the annual budget request with actual costs as they are known to ensure the most accurate reflection of total project costs. The PMO is confident that it will be able to effectively monitor and manage SENTINEL resources.

Issue: The Department’s current wireless capabilities do not provide law enforcement officers and agents with the support they need because the 15- to 20-year-old communications systems infrastructure results in degraded coverage, reliability, and usability. Further, antiquated, stove-piped,

land mobile radio systems provide only limited federal-to-federal and federal-to-State and local interoperability.

Action: Through the Integrated Wireless Network (IWN), DOJ will replace the aging wireless systems of the ATF, DEA, FBI, USMS and OIG with a consolidated set of communications services that support DOJ's tactical law enforcement and counterterrorism missions. In the second quarter of FY 2007, the Department expects to procure the services of a systems integrator to develop and deploy the IWN. Meanwhile, DOJ has implemented a pilot system in the State of Washington and has taken several interim steps to consolidate and mitigate problems incumbent with the legacy systems.

Issue: The Department has some weaknesses in its management, operational, and technical controls for sensitive but unclassified and classified systems, as well as in its oversight program and related management controls. Components are not being held accountable for completing documentation and testing systems, and stronger monitoring of the Department's certification and accreditation process could identify and correct many of the reported system weaknesses.

Action: In 2005, the OCIO developed an oversight program and methodology for monitoring IT performance, including IT security. The Department's IT security methodology is closely aligned with the control requirements in the DOJ IT Standards, FISCAM, and existing automated tools used to support the FISMA requirements within the Department. In FY 2007, DOJ will continue to implement corrective actions for identified weaknesses in the areas of access controls, patch management, and baseline secure configurations, as well as improve overall testing of controls to ensure they are effectively designed and functioning properly. The DOJ IT Security Staff (ITSS) will accelerate the review of certification and accreditation documentation and control implementation for adequacy, completeness, and quality. Quality reviews will ensure that controls are adequately implemented; that implementation is adequately documented (e.g., control compliance descriptions and actual results in the system security plan); and that, where weaknesses are found in control implementation, plans of action and milestones (POA&Ms) are created, funded, and managed. Lastly, the OCIO will provide additional training to components in all areas of certification and accreditation, self assessments, control validation, and POA&M management.

The Department will continue to monitor progress through the IT Security Dashboard and the IT Management Scorecard. The ITSS and the Department's IT Security Council will continue to monitor IT security problem areas to identify systemic issues and formulate recommended solutions. For components with significant deficiencies, the CIO will continue its practice of monthly progress review meetings and, where appropriate, apply additional resources to bring about desired results.

The Department will initiate a CIO/CIO Council-sponsored assessment of the DOJ IT Security Program that will focus on priorities and program planning, implementation, and management. Furthermore, to bolster senior program official commitment to IT security implementation in the components, CIO performance work plans will include elements for IT security.

Issue: It is not clear what procedures the components follow internally when responding to data breaches or losses. A significant challenge many components face is the ability to identify the specific information contained on lost or stolen laptop computers and other IT equipment.

Action: The DOJ Computer Emergency Readiness Team (DOJCERT), the central organization within the Department to which components report data loss and computer security incidents, is in the process of establishing clearly defined guidance, comprehensive training, and regular meetings with component incident response teams (IRTs).

At the beginning of each FY, DOJCERT updates the Incident Response Plan (IRP) template that components follow in developing or updating their system IRPs. In this year's update, DOJCERT has added a new section focusing specifically on data loss reporting. It aligns with requirements set forth by OMB and US-CERT and defines specifically the information components need to gather when a data breach or loss occurs.

In addition, during FY 2007, DOJCERT will develop an Incident Response (IR) Handbook components can use when investigating incidents. It will identify the information to be gathered during and following an incident and techniques to compile all essential information, including the type of data included on lost equipment. It will also describe a method for identifying the level of residual risk associated with each incident as it is resolved. This will align with a new field in the DOJCERT Incident Reporting Database that will be used to measure the residual risk assigned to each incident.

To reinforce this written guidance, DOJCERT is incorporating it into the DOJ employees' annual training. Within the Department's annual Computer Security Awareness Training, DOJCERT has created a section addressing IR and discussing specifically the need to report lost or stolen IT equipment. Additionally, DOJCERT is working with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University to develop an IR training course within the virtual training environment. A section of the course will address data loss incidents. Component IRT members will complete the web-based course as part of their annual training requirement.

4. Violent Crime

Issue: The FBI's prioritization of counterintelligence and counterterrorism has resulted in shifting agents, analysts, and other resources from traditional criminal investigations to counterterrorism and counterintelligence activities. As a result, the Department is investigating and prosecuting significantly fewer traditional criminal matters than it did prior to September 11, 2001. State and local law enforcement officials have indicated that their investigative caseloads have increased following the FBI's post-September 11 reprioritization. Approximately 50 percent of respondents to an OIG survey of State and local law enforcement agencies indicated that the overall crime rate in their agencies' jurisdiction had increased during the 5-year period from FY 2000 - FY 2004: 41 percent of respondents said violent crime against persons had increased; 24 percent said gang-related crimes had increased; and 17 percent cited a rise in bank robberies. Many of these State and local officials have expressed concern about their agencies' ability to handle the increased workload and that the complex crimes that the FBI previously had handled often exceeded their departments' resources, expertise, and jurisdiction. In contrast, other local representatives said they did not believe the FBI's reduced involvement in these areas had negatively impacted their agencies' operations.

Action: Although the FBI has attained significant statistical accomplishments in the Violent Crimes Program, the number of agents it has dedicated to violent crimes has been significantly reduced. The FBI has offset these losses, in part, by aggressively combating violent crimes through the development of new violent crime task forces and leading nationwide initiatives such as the Innocence Lost child prostitution initiative, Project Welcome Home international fugitive return initiative, the Indian Gaming Working Group, and the creation of Child Abduction Rapid Deployment Teams. The FBI is leading the way in technological and intelligence innovations that will greatly assist all federal, State, and local law enforcement agencies in identifying crime trends, distributing law enforcement resources, and locating and apprehending perpetrators. Some of these innovations include the integration of fugitives into the Department of State passport lookout system, the Project Pinpoint intelligence mapping tool, the Choice Point Registered Sex Offender Locator Tool, and Violent Crime-Wireless Intercept Tracking Teams.

Issue: The Department has allocated less money to State and local governments for crime prevention. Several local leaders have noted that the shift of federal priorities to terrorism prevention has resulted in less federal funding to combat domestic crime, reductions in police department staffing levels, and more strain on the courts and corrections components of local criminal justice systems.

Action: OJP focuses its limited resources on those priorities and locations that can have the greatest impact. Its Strategic Plan, covering FY 2007 through FY 2012, provides a framework to focus funding to optimize the return on investment of taxpayer dollars.

The COPS Office, through its consistent interaction with law enforcement professionals, is aware of the needs of local law enforcement. As a result, COPS directs its limited funding to key areas. For example, in FY 2006, COPS funded a Tribal initiative that focused on the creation of various training and knowledge products aimed at addressing chronic public safety issues. The COPS Office will continue to focus its resources to maximize the impact of grant funding for State, local, and tribal law enforcement.

Issue: An OIG review determined that while the ATF's Violent Crime Impact Teams (VCIT) strategy may be an effective tool to reduce violent crime in targeted areas, there is inconsistent application by local VCITs of key elements of the strategy. The OIG also found that ATF's claim in January 2006 that it had met its stated goal was based on insufficient data. In light of the ATF's plans to expand the VCIT program to 15 additional cities in 2007, the Department must consistently implement and evaluate the VCIT strategy in these cities in order to improve the effectiveness of the ATF's efforts to target gun violence in specified urban areas.

Action: To address the OIG recommendation that “the Department must consistently implement and evaluate the VCIT strategy in these cities in order to improve effectiveness of the ATF’s efforts to target gun violence in specified urban areas,” ATF is issuing guidance to its Field Divisions directing VCITs to tailor the ten best practices – identified during ATF’s evaluation of the program – to local conditions. Additionally, ATF will use a survey to assess the intensity with which each of the best practices is being used.

Issue: There is a need for BOP, as well as State and local corrections facilities, to prepare inmates for life after prison. Studies show that more than half of all offenders are re-arrested within 3 years after release. According to reports from the Bureau of Justice Statistics, “The reentry of serious high-risk offenders into communities across the country has long been the source of violent crime in the United States.”

Action: The BOP has an active and evolving release preparation program to assist prisoners in reentering the community successfully. This program targets specific inmate needs and focuses on skills acquisition. Reentry skills are a point of focus from initial designation to the successful transition back to the community.

5. Financial Management and Systems

Issue: While the Department’s goal is to move to more of a year-round versus a year-end financial reporting effort, most components are still hobbled in meeting that goal by the lack of automated financial accounting processes. To address this issue, the Department has placed great reliance on the planned Unified Financial Management System (UFMS) as the fix for many of these automation issues. The UFMS would standardize and integrate financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes. However, the Department’s efforts over the past few years to implement the UFMS to replace the seven major accounting systems currently used throughout the Department have been subject to fits and starts.

Action: During FY 2006, the Department continued to demonstrate progress to remediate internal control weaknesses, which included corrective actions for tracking and measuring timely compliance and resolution. Departmental progress was demonstrated within the internal control framework, accrual accounting methodology, grant accounting and monitoring, and through establishment of financial management policies and procedures to enhance controls over financial reporting. A major key to the plan for improving audit performance is the development and deployment of a core financial system, the Unified Financial Management System (UFMS), throughout the Department. The UFMS will enhance financial management and program performance reporting by making financial and program information more timely, relevant, and accessible.

6. Detention and Incarceration

Issue: An OIG review found that BOP’s monitoring procedures, intelligence analysis, and foreign language capabilities were deficient. It found that BOP does not adequately read the mail or listen to the telephone calls, visitor communications, or cellblock conversations of terrorists or other high risk inmates. The review also found that BOP does not have sufficient resources to translate inmate communications in foreign languages and lacks staff adequately trained in intelligence analysis techniques to properly assess terrorist communications. Also, BOP is not screening for terrorist connections in organizations that assist it with recruiting religious services providers.

Action: The BOP’s response to the OIG’s report issued September 27, 2006, detailed its intended corrective action. The thirteen recommendations have been resolved and BOP is in the process of implementing the actions identified.

Issue: The Department must try to keep drugs out of federal prisons and rehabilitate drug-addicted inmates. In January 2003, the OIG issued a review that found the BOP did not search visitors or monitor visiting rooms adequately, did not search staff or take sufficient measures to prevent drug and other contraband smuggling by BOP staff, and did not provide adequate non-residential drug treatment to inmates.

Action: The BOP has implemented corrective action to resolve and close seven of the thirteen recommendations identified in the OIG’s report. The BOP is currently working on implementing corrective action on the six remaining resolved recommendations, all of which require changes to rules language and/or policy revisions.

Issue: The OIG believes the Department could realize significant cost savings if it addressed deficiencies in how prices are set in individual Intergovernmental Agreements (IGAs) with State and local agencies for detention bed space. It appears that the OFDT's revamping of the IGA pricing process through a statistical pricing model known as eIGA may result in the Department paying higher jail-day rates than necessary. Also, the OIG believes that the USMS needs to improve its procedures for establishing and monitoring IGAs. The OIG has encouraged the Department to attempt to recover overpayments made to State and local jails.

Action: OFDT does not agree that the electronic Intergovernmental Agreements (eIGA) process will lead to an unwarranted increase in rates. Under the current system, only the actual or allowable costs of individual jails are examined, so the reasonableness of costs is never challenged. However, under the eIGA approach, a price analysis is conducted using comparisons to similar jails with similar operations to determine a fair and reasonable jail rate without requiring an evaluation of individual cost elements. A price analysis supports a negotiation position that permits the Government and the jailer an opportunity to reach agreement on a fair and reasonable price that provides the greatest incentive for efficient and economical performance. (A fair and reasonable price does not require that agreement be reached on every element of cost.) In the eIGA process, federal government negotiators establish a fair and reasonable price by evaluating the offered rate through comparison to the eIGA Core Rate (government estimate); rates at other federal, State and/or local facilities; previously proposed rates; and previous Government private jail contract prices.

The current method of determining the rate – and rate increases – on the basis of cost provides an incentive to jailers to increase cost elements that are allowable federal prisoner housing costs in order to receive higher jail rates. The eIGA method provides maximum incentive for the jailer to control costs and perform effectively and imposes a minimum administrative burden upon each party.

With regard to “overpayments made to State and local jails,” the OFDT maintains that the agreements incorporated a “fixed rate” and, accordingly, the agreements with the State and local governments were negotiated, fixed-price agreements for the period in question, and the parties were bound. OFDT believes that, in the absence of fraud, the agreements are not subject to retroactive adjustment.

To enforce the need for districts to comply with established IGA management policy, USMS has initiated regular communication to the districts via telephonic and written methods. It has developed a much enhanced Justice Detainee Information System upgrade, which will provide reports designed to better track IGA information. In turn, using these reports, USMS can evaluate the effectiveness and efficiency of the program and make adjustments and corrections to problem areas. The IGA Branch is increasing its staffing to meet the substantial workload of the IGA program, and, in FY 2007, it expects funding for training, allowing IGA Branch staff to gain additional knowledge in areas such as price/cost analysis and negotiation techniques.

7. Supply and Demand for Drugs

Issue: For the second consecutive year, more State and local law enforcement agencies nationwide identified methamphetamine as the drug that poses the greatest threat in their area.

Action: DEA is very aggressive in training drug law enforcement counterparts with respect to methamphetamine investigations. Since FY 1999, DEA has trained a total of 9,704 State and local law enforcement officers in identifying and cleaning up clandestine laboratories. To expand and improve its efforts, DEA is beginning the construction of a new state-of-the-art clandestine lab training facility at the DEA Academy in Quantico, Virginia in the fall of 2006.

The DEA has redirected the focus of its Mobile Enforcement Teams to prioritize deployments to assist with methamphetamine investigations. Currently, the teams are focusing on targeting methamphetamine PTOs and clandestine laboratory operators in areas of the United States that have a limited DEA presence.

With the significant reduction in the number of domestic small toxic labs, DEA's Clandestine Laboratory Enforcement Teams will expand their efforts beyond dismantling methamphetamine labs to include the targeting of Mexican methamphetamine trafficking organizations. Current drug and lab seizure data suggests that roughly 80 percent of the methamphetamine used in the United States comes from larger labs, increasingly in Mexico, and that approximately 20 percent comes from small toxic laboratories. Since 2001, DEA has disrupted or dismantled in excess of 500 Priority Targets where methamphetamine was the primary drug involved.

