DOJ Management's Response to the Office of Inspector General's Top Management and Performance Challenges

1. Counterterrorism

1. Counterterrorism: A critical challenge facing the Department of Justice (DOJ or the Department) is its ongoing effort to detect and disrupt acts of terrorism.

Issue: The Federal Bureau of Investigation (FBI) continues its transformation into a more proactive, intelligence-driven agency. However, frequent rotations and turnover within its senior management ranks negatively affect this transition.

Action: The FBI has launched a number of initiatives to address this issue. Representatives of the FBI's Executive Development and Selection Program are working with the RAND Corporation to develop a database designed to assist in Senior Executive Service (SES) succession planning. In addition, 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. Another piece of the FBI's leadership development strategy is the Strategic Leadership Development Plan, which 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 (FBIHQ), including the increased use of retention bonuses and other incentives to encourage SES employees to remain in these positions longer. With strong, steady leadership, the FBI will be better poised to achieve its mission of protecting America.

Issue: The Terrorist Screening Center's (TSC) management of the terrorist watchlist continues to have weaknesses. For example, the TSC still relies on two versions of the watchlist database, and the Office of the Inspector General (OIG) identified several known or suspected terrorists who were not watchlisted appropriately. Although the TSC had increased its quality assurance efforts, it continues to lack important safeguards for ensuring data integrity.

Action: The TSC routinely evaluates its operations to increase efficiency and effectiveness, and will continue to take this same approach in the future. The TSC does not rely upon two versions of the watchlist database as the OIG indicates, but instead has only one consolidated government watchlist: the Terrorist Screening Database (TSDB). The TSDB is one system that contains two primary components. Each component has separate functions, but as of this date, neither can exist without the other. Thus, the components are part of the overall system, not separate systems.

As part of the Single Review Queue (SRQ), terrorist identity data is received into a component of the TSDB known as the Nomination Tracking Processor (NTP), where it awaits a review by a TSC Nominations and Data Integrity Unit (NDIU) analyst. SRQ personnel review both international terrorist records from the Terrorist Identity Datamart Environment (TIDE), provided by the National Counterterrorism Center (NCTC), and domestic terrorist records provided by the FBI's Terrorist Review and Examination Unit (TREX). After the record is reviewed in NTP, TSC adds it as an official record, and exports the record to one of the TSC's supported systems, such as the National Crime Information Center (NCIC).

The time to process the SRQ nominations from NCTC's TIDE, which includes thousands of records each day, takes several hours to complete. As such, during the time it takes to process the SRQ, there will always be disparities between the NTP and official recordkeeping components of the TSDB. However, these components are now reconciled each day through a formal process after the SRQ is completed.

The TSC has also created a Data Integrity Advisor position whose incumbent reports to the TSC Director. The Data Integrity Advisor examines all lines of business supporting data integrity at the TSC, including operations, information technology (IT), policy, and standard operating procedures. As a result, new standard operating procedures, training, sampling measures, and metrics have been implemented at the TSC to ensure the highest-quality data on known or suspected terrorists is available to the United States and its partners to detect and disrupt acts of terrorism.

As noted by the OIG, the TSC has consistently enhanced its quality assurance efforts, and continues to innovate in the critical area of data integrity. The TSC has noted the OIG's concerns and has fully addressed them operationally and strategically. The TSC is committed to a methodology that not only addresses current data integrity issues, but identifies and plans for improvements in this arena in the future.

Issue: The FBI has made progress in improving its hiring, training, utilization, and retention of Intelligence Analysts (IAs), although in some areas the progress had been slow and uneven. Improvement is needed in the time required to hire analysts. In addition, the FBI has struggled to design a satisfactory training program for its counterterrorism agents and analysts, and many special agents still do not fully understand or appreciate the role of analysts.

Action: The FBI has taken, or plans to take, a number of initiatives in selection and hiring, recruitment and retention, and training.

Selection and Hiring: The FBI's plan for selection and hiring for the Intelligence Career Service incorporates the best practices from Special Agent hiring and leverages the strengths of this proven system. The FBI has made significant progress in implementing its selection and hiring action plan by creating a suite of selection tools, piloting selection system tools, and facilitating a more focused selection process. The FBI is currently deepening its selection and hiring capabilities. In the next 6 months, the FBI will validate its selection system tools and validate specific job analysis information on the Intelligence Career Service positions to ensure that the selection system validation process complies with professional standards and legal guidelines.

Recruitment and Retention: The Directorate of Intelligence (DI) has shifted from a local recruiting model to a centralized, nationwide recruiting strategy. The DI now processes applicants centrally using the FBI jobs system and conducts regional events to interview and process successful applicants. Each new hire must sign a mobility agreement so that IAs, Language Analysts, and Surveillance Specialists can be redeployed consistent with the needs of the enterprise.

The DI has refined its competency-based recruitment strategy to target and provide incentives to applicants with critical skills in intelligence, foreign languages, technology, area studies, and other specialties. In addition, the DI is initiating a targeted recruitment strategy that blends national requirements of the Office of the Director of National Intelligence (ODNI) and mission priorities of the FBI. The strategy will address 12 target areas and four geographic regions as they apply to the Intelligence Career Service.

Finally, the DI continues to use the Pat Roberts Intelligence Scholars Program, which offers $25,000 scholarships to current FBI IAs to help fund their past, current, or future studies in a specialized critical skill or area of specialty the FBI deems critical. The purpose of this U.S. Intelligence Community (USIC) program is to enhance the FBI's retention of IAs with specialized critical skills. In 2007, the FBI awarded 16 scholarships to IAs and Language Analysts.

Training: To establish core intelligence training consistent with FBI's current mission, the DI, in collaboration with the Training Division and subject-matter experts, developed the Intelligence Basic Course (IBC) for new IAs and is in the process of developing the Leading Analysis Course for the supervisors of analysts. The FBI piloted the 10-week IBC for new IAs in June 2007, with the second iteration underway as of October 1, 2007. This course is based upon the ODNI competencies and adopts best practices of established Intelligence Community (IC) training—in particular, the Kent School at the Central Intelligence Agency (CIA). IBC focuses on the basic analytic tradecraft skills that will help IAs to produce more fully developed, forward-leaning analysis and deliver it effectively to a range of consumers.

To complement the IBC, a 2-week Leading Analysis Course is under development. This course will provide supervisors of IAs with a set of tools and managerial techniques they can use to enhance the rigor and quality of the analytic products generated by their offices. The course will address such issues as the role of analysis in the intelligence cycle, categorizing various types of analysis, avoiding analytic traps and mindsets, selecting and characterizing evidence, meeting the needs of various customers, the elements of effective warning, and understanding analysts and their core competencies. The Leading Analysis Course will be mandatory for all IA supervisors.

Regarding counterterrorism training in particular, New Agent Training recently has been modified to provide 100 additional hours of training in all national security-related areas. The FBI's Counterterrorism Division (CTD) and the U.S. Military Academy's Combating Terrorism Center have established a collaborative effort to develop a counterterrorism curriculum, exchange instructors, and work on knowledge development projects. This collaborative effort includes providing training to Joint Terrorism Task Forces (JTTFs), hosting a Counterterrorism Leadership Retreat, developing and delivering instruction to new agent trainees, continuing to develop FBI case studies, and creating a counterterrorism textbook.

Several initiatives are underway to enhance the working relationship between agents and analysts. Currently, senior agents and analysts attend a Navigating Strategic Change course that was developed for the FBI by the Kellogg School of Business. This collaborative learning experience was designed to highlight the complementary, but unique roles of the agent and analyst. In an effort to reach new agents and analysts, the FBI has improved the new agent and new analyst capstone training. This revised training exercise is led by experienced analyst and agent instructors. Most importantly, when new agent and new analyst training schedules do not coincide, analysts from field offices and FBIHQ participate in this exercise with the new agent trainees.

Issue: Although the FBI recently has made progress in improving the management of its IT upgrades, it will not benefit from a fully functional case management system for at least 2 more years.

Action: SENTINEL, a four-phased program, will provide FBI employees with its next-generation information sharing and case management system. Each phase will introduce new capabilities and provide greater access to existing information. Phase 1 of the SENTINEL system was deployed Bureau-wide in mid-June 2007. SENTINEL now provides a user-friendly, web-based interface to access information currently in the FBI's Automated Case Support (ACS) system. Information is pushed to users and is available through hyperlinks, putting more information at their fingertips and moving employees away from dependence on paper-based files.

The FBI has adopted an incremental development approach for Phases 2-4 to provide more rapid development and deployment of capabilities to users. This will reduce in scope and/or eliminate other duplicative projects planned or underway that could not afford to wait until SENTINEL reached its final operating capability (FOC). It also reduces the task of creating costly custom, throwaway code needed for ACS and SENTINEL to interact simultaneously while SENTINEL steadily assumes ACS services.

Phase 2, projected to be released in segments from October 2007 to July 2009, will introduce the Administrative Case Management capability to be able to open, close, and serialize documents to an administrative case (available toward the end of the final segment). Another capability will be the FBI Enterprise Portal, the main entry point for all FBI applications for FBI Enterprise users. It will provide links to information on applications, personal spaces (My Documents), e-mail, news, and SENTINEL functionalities.

Phase 3 will provide indexing and enhanced search capabilities, scanning capabilities, and deploying of a user-based forms tool. The system will reach full operating capability in Phase 4.

Issue: There have been serious failures of accountability in the FBI's misuse of national security letter (NSL) authorities. The FBI did not provide adequate guidance, controls, or training on the use of sensitive NSL authorities, and the FBI's oversight of NSLs was inconsistent and insufficient.

Action: Addressed in "Civil Rights and Civil Liberties" Section.

Issue: Congress and Department managers use terrorism-related statistics to make funding and operational decisions. Twenty of twenty-six statistics tested by the OIG were significantly overstated or understated. The Department components could not provide support for the numbers reported, could not provide support for a terrorism link used to classify statistics as terrorism-related, and could not document that the activity reported occurred in the period reported. The Department's collection and reporting of terrorism-related statistics were decentralized and haphazard. Department officials either had not established internal controls to ensure the statistics were accurately gathered, classified, and reported or did not document the internal controls used.

Action: NSD is responsible for nine of the statistics the OIG addressed. The Department consistently has used statistics compiled by the Counterterrorism Section – formerly part of the Criminal Division and now in the National Security Division (NSD) – when publicly quantifying its terrorism prosecutions and cases. These statistics represent defendants charged in terrorism or terrorism-related criminal cases with an international nexus which are tracked by the NSD. These cases have arisen from investigations, conducted primarily after September 11, 2001, that initially appeared to have an international connection, including certain investigations conducted by the FBI's JTTFs and other cases involving individuals associated with international terrorists or Foreign Terrorist Organizations. The Criminal Division began tracking these cases during the nationwide PENTTBOM investigation of the September 11, 2001, attacks. The initial cases tracked involved individuals identified and detained in the course of that investigation and subsequently charged with a criminal offense, though often not a key terrorism offense. Additional individuals have been added who, at the time of charging, appeared to have a connection to terrorism, even if they were not charged with a terrorism offense.

The OIG ultimately found that the Counterterrorism Section provided documentation that either accurately stated or, at times, understated the number of terrorism-related defendants or matters. While the records supporting the nine statistics maintained by the Counterterrorism Section (and that the OIG examined) initially were incomplete in some respects, the NSD reconstructed the data to support these nine statistics from objective resources, including the Automated Case Tracking System (ACTS), the Daily Report, and PACER, demonstrating that NSD had sufficient controls in place to provide the true picture.

The NSD's Counterterrorism Section has improved the procedures for gathering, verifying, and reporting terrorism-related statistics, already implementing many of the IG's recommendations. The decision to add defendants to the statistical chart is made on a case by case basis. In general, those charged with Category 1 offenses (as denoted in the *United States Attorneys' Manual*, USAM § 9.2-136) are added. Defendants charged with violating a variety of other statutes also are tracked on the chart if the cases at the time of charging appear to be terrorism-related cases with an international nexus. These cases may charge statutes listed in Category 2 of USAM § 9.2-136, as well as many other offenses including, but not limited to, fraud offenses, immigration offenses, firearms charges, drug crimes, false statements, perjury, and obstruction offenses, as well as general conspiracy charges under 18 U.S.C. § 371. The chart contains individuals who, at the time of charging, appeared to have a connection to terrorism, even if they were not charged with a terrorism offense. The chart is updated on a daily or weekly basis according to very specific procedures. Additions to the chart are reviewed (and approved), as necessary/appropriate, by the Deputy Chief for Policy, Legislation and Planning in consultation with the Chief.

The FBI has made tremendous strides toward improving the systems and internal controls related to terrorism reporting. The core elements of the FBI's statistical reporting system are the case management and supporting IT systems. The FBI's ongoing enhancements to these systems, most commonly referred to as the SENTINEL project, serve as an integral part of its efforts to improve statistical reporting.

In addition to the above-mentioned improvements, one effort of note is the recent establishment of the CTD's Strategy, Communication and Policy Management Office (SCPMO). A major objective of this office will be to formulate and publish defined statistical policy and procedure guidelines governing the gathering, verifying, and reporting of terrorism-related statistics. The SCPMO will act as a central repository for terrorism-related statistics and will be able to verify accuracy based on past statistical trends.

Another effort of note is the implementation of the case review process. This process involves a review by officials at FBIHQ and DOJ of each pending investigation every 90 to 120 days. This review looks at investigative findings and facilitates a discussion with each field office on its investigative plan and effort to mitigate any potential threat to national security. Along with periodically reviewing the background, elements, and progress of each counterterrorism case, a thorough analysis of the case's statistical accomplishment is conducted.

The Executive Office for U.S. Attorneys (EOUSA)/U.S. Attorneys have responded to each of the IG's recommendations. The IG has formally agreed that the actions EOUSA has taken have resolved the issue and considers the issue closed.

2. Restoring Confidence in the Department of Justice

2. Restoring Confidence in the Department of Justice An immediate challenge facing DOJ leadership is the need to restore confidence in the Department and its operations, both with Department employees and with the public.

Issue: The Department has faced significant criticism of its actions and ongoing congressional and internal investigations on a variety of topics, including the removal of U.S. Attorneys and allegations of improper hiring practices for career attorney positions at the Department. These and other allegations regarding the integrity and independence of the Department have affected the morale of Department employees and public confidence in the decisions of Department leaders.

Action: Senior Management Offices take very seriously any allegations of wrongdoing in the Department. In order to avoid the appearance of impropriety and to protect the Department from suggestions of improper bias, former Attorney General Gonzales referred allegations of wrongdoing. The Department's OIG and Office of Professional Responsibility (OPR) are conducting a joint investigation of those allegations. Since the referral, the Office of the Attorney General (OAG) and Office of the Deputy Attorney General (ODAG) have fully supported that joint investigation.

Furthermore, while awaiting the findings of the OIG and OPR investigations, the Department has taken a number of steps to change procedures and policies to ensure that some of the previous mistakes do not reoccur. For example, within the previous 7 months, the Department:

- Revised the process by which Board of Immigration Appeals Judges and Immigration Judges are appointed;
- Revised the hiring process for the Honors Program and Summer Law Interns Program;
- Directed EOUSA to ensure that the vetting process for the hiring of Assistant U.S. Attorneys (AUSAs) by interim and Acting United States Attorneys remains within EOUSA and not with political appointees in the senior management offices.
- Rescinded the internal OAG delegation order and amended the Code of Federal Regulations (CFR) to allow for that change;
- Instituted new training about hiring practices and procedures for all political appointees; and
- Undertook a process to review and revise the policy governing communications between the Department and the White House.

Issue: Recent resignations by the Attorney General, the Deputy Attorney General, and the Associate Attorney General leave the Department without any of its three most senior Senate-confirmed leaders. As of October 1, 2007, only three of the Department's eleven presidentially appointed Assistant Attorney General (AAG) positions were filled by Senate-confirmed appointees. Further, 23 of the 93 U.S. Attorney positions were occupied by interim or acting U.S. Attorneys. Vacancies in many key leadership positions have resulted in delayed decision-making or lack of decision-making on a variety of important issues.

Action: Although the Department also would like to see Senate-confirmed appointees in every AAG position, the Senior Management Offices disagree with the proposition that vacancies have affected decision making within the Department. Each Department component has an officer, whether confirmed or not, who is providing leadership and ensuring that important issues are addressed. The President has nominated a number of qualified individuals to serve in important posts, including Attorney General; Director of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and Assistant Attorney General, Environment and Natural Resources Division. Regardless of how long the confirmation process may take, the critical work of the Department will continue and the men and women serving in leadership positions will work tirelessly to ensure the right decisions are made. The results that the Department has achieved, and continues to achieve, demonstrate that important issues continue to be addressed and resolved in a timely and appropriate manner.

3. Financial Management and Systems

3. Financial Management and Systems: The most important challenge facing the Department in this area is to successfully implement an integrated financial management system to replace the disparate and, in some cases, antiquated financial systems used by Department components.

Issue: The Department lacks sufficient automated systems to readily support ongoing accounting operations and preparation of financial statements. The Department has placed great reliance on the planned Unified Financial Management System (UFMS) as the fix for many of its automation issues. The UFMS is intended to standardize and integrate financial processes and systems to more efficiently support accounting operations, facilitate preparation of financial statements, and streamline audit processes. It also will enable the Department to exercise real-time centralized financial management oversight while maintaining decentralized financial management execution. However, 3 years after the Department selected a vendor for the unified system, it has made little progress in deploying the UFMS. The Department notes that problems with funding, staff turnover, and other competing priorities have caused the delays in implementing the UFMS.

Action: During FY 2007, DOJ continued to demonstrate progress toward development and deployment of a core financial 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.

In the past year, UFMS delivered a fully tested and government accepted Foundation Build 1.0. This is the core functionality of UFMS that will be deployed to each component. It includes 28 standard financial management and procurement business processes, reference data, interfaces, reports, and system architecture features needed to: 1) implement core financial management and procurement functions, 2) maintain unified interface and data standards, and 3) support standard Departmentwide and common component reporting needs. Specifically, it includes core financial management and procurement software modules (e.g., General Ledger, Accounts Payable, and Acquisitions), the Foundation Build Framework (e.g., Administration Tools), interfaces (e.g., Payroll), processes (e.g., Purchase Card, Budget Execution), reference data (e.g., Interest Reason Codes), standard departmentwide reports (e.g., Fund Status), and an operational data store.

Additional accomplishments in FY 2007 include the completion of planning activities at the Asset Forfeiture Program (AFP) and the Drug Enforcement Administration (DEA), both having recently transitioned into a full implementation phase. The AFP pilot is scheduled to go “live” in November 2007 and DEA is scheduled to go “live” in October 2008. Planning also is underway at the FBI, with plans to begin full implementation efforts in early 2008.

Plans for the UFMS include that system implementation will be conducted in three waves. Wave I already is underway; it includes AFP Phase 1 (pilot), DEA, and the FBI. Future component implementation plans in Wave II include ATF; the U.S. Marshals Service; and AFP (Phase 2). Wave III will follow with the Office of Justice Programs (OJP), the Federal Bureau of Prisons (BOP), and the Offices, Boards, and Divisions (OBDs). The UFMS Program Management Office (PMO), in conjunction with the Justice Management Division’s (JMD) Finance Staff, currently is evaluating opportunities to implement a number of offices within the OBD’s in Wave II in early FY 2009.

To help ensure the success of the UFMS program, the PMO receives guidance from the Department's senior leadership and employs the consultation of an Independent Verification and Validation contractor. Additionally, the UFMS PMO briefs and solicits the advice of the Office of Management and Budget (OMB) on a monthly basis.

4. Grant Management

4. Grant Management: Grant management is a continuing top challenge, with the Department awarding approximately $3 billion in grants in FY 2007 and approximately $23 billion in the previous 7 years.

Issue: During 2007, the Office of Community Oriented Policing Services (COPS) improved its grant closeout process. However, OJP and the Office of Violence Against Women (OVW) still need to implement procedures to ensure that grants are closed within 6 months after the grant end date and that grantees are prohibited from drawing down grant funds after the end of the 90-day liquidation period unless an extension is requested by the grantee and approved by the awarding agency.

Action: The OIG's report regarding grant closeout management was based on the status of expired grants as of December 2005. The issues mentioned in the report were issues that OJP already had acknowledged as areas of concern and had been taking many efforts to improve. During FY 2007, OJP continued its aggressive grant closeout initiatives, which resulted in improved policies and procedures for financial and programmatic closeout, implementation of a grant closeout module in OJP's web-based Grants Management System (GMS), and closure of over 7,000 OJP and OVW grant awards. As noted in correspondence from the OIG dated June 8, 2007, the OIG considered the audit recommendations regarding grant closeout as resolved, as OJP management and the OIG have agreed that corrective actions already implemented and planned would address the audit recommendations.

In FY 2004, OVW became a stand-alone component, separate from OJP, and became responsible for such functions as tracking its own grant closeout status, assuring the quality of its closeout documentation, and following up with grantees for required final closeout report submissions. Other services are still performed by OJP's Office of the Comptroller (OC) via contract to OVW, and the division into separate components has resulted in changes to the manner in which the two entities share information.

Regarding the grant close-out process, in FY 2006, OVW conducted an internal evaluation it, leading to revisions in FYs 2006 and 2007. OVW revamped and streamlined its internal closeout process to minimize the time lapse between grant end dates and closeout dates. Enhancements included: improving the information flow; developing a "Closeout Desk Guide" to standardize and streamline the internal closeout process; developing a closeout tracking tool which allows management to track OVW's closeouts and monitor progress according to various programs and other criteria; and, dedicating specific staff resources to the closeout process. OVW continues to work with OJP's OC to improve the overall process.

OVW understands that it must take additional measures, both internally and externally, to discharge its obligation to promptly close out grants. In FY 2007 OVW began using the new close out feature of the GMS. As of October 1, 2007, OVW had closed out more than 1,200 additional grants using this new feature and had approved more than 250 additional close-outs, which are in-process at OJP. OVW continues reengineering its closeout process so that expired grants will be closed within 6 months of the end date.

OVW has developed automated processes, using data provided by OJP, to identify and track grants that are approaching and past the grant expiration date on a graduated scale based on regulatory guidance. As part of this process, OVW has integrated a quality review of expired grant file documentation to ensure that all required forms have been submitted for programmatic and financial closeout. In addition, items identified through status tracking and quality reviews are used as a basis for grantee outreach and follow-up to facilitate timely closeout. These initiatives have necessitated increased data sharing, communication, and collaboration between OJP and OVW that will result in improved grant closeout compliance within 6 months of the grant end date.

In FY 2007, OVW began using another improved feature of GMS – the automatic cut off for all draw downs once the 90-day liquidation period ends, unless an extension is approved. This cut off also applies to grantees with unacceptably delinquent cost reports. These enhancements, coupled with an ongoing management focus on improving close-outs, are yielding significant results for OVW in this area.

Issue: OJP continues to experience problems with oversight of its grant programs, including problems with the improper use of grant funds, difficulties in meeting grant objectives, and poor performance measurement of grant effectiveness.

Action: OJP's current grant portfolio consists of approximately 20,000 active grants totaling $12.4 billion. OJP is aware of only a relatively small number of grants that have undergone an OIG investigation, and some of those grants were referred by OJP to the OIG as a result of issues identified through OJP's grant oversight. For example, during FY 2007, OJP referred five grantees (10 grants) to the OIG's Investigations Division, of which three grantees currently are under investigation. Beginning in FY 2007, OJP and the OIG held meetings to identify monitoring visit findings that should be investigated by the OIG. Based on the positive outcome of the meetings, OJP and the OIG agreed that they would continue meeting during FY 2008.

Whenever potential or actual improper use of grant funds is identified through OJP's financial and programmatic monitoring, single audits, or OIG grant audits, OJP quickly works with the grantees to ensure that they address issues related to improper use of funds. Further, in support of the Department's National Procurements Fraud Task Force Grant Fraud Committee, during FY 2007, OJP referred seven grantees to the OIG for an internal control review because of concerns with the grantees' administration of grant funds.

Issue: During the past year, OJP made little progress in staffing its new Office of Audit, Assessment, and Management (OAAM). Created by Congress, this office was intended to improve internal controls and streamline and standardize grant management policies and procedures across OJP.

Action: Congress approved the latest organizational structure of OJP, which includes the new OAAM, in April 2007. In addition to the accomplishments the OIG mentioned, OJP implemented many other improvements that further the mission of OAAM. The improvements include: (1) tightening controls to improve progress report submission by instituting automatic system holds on grant fund drawdowns when grantees are delinquent in submitting progress reports; this prompted the submission of over 50 percent of the 1,400 delinquent June 30, 2007, semi-annual progress reports; (2) facilitating grant management training for over 400 OJP grant managers to emphasize effective post-award program management strategies and practices; (3) working with COPS to create a joint programmatic and financial monitoring plan; and (4) exceeding the statutory 10 percent monitoring requirement by programmatically and fiscally monitoring over $1.2 billion of open awards in coordination with COPS. Also, in October 2007, the Deputy Director for the Grants Management Division entered on duty, and the four vacant positions in the Audit and Review Division have been filled.

5. Violent Crime

5. Violent Crime: The Department faces a significant challenge in reducing the recent rise in violent crime while shifting substantial resources from its criminal investigations to meet its counterterrorism-related responsibilities.

Issue: The FBI has reported that it has been working to update its resource utilization practices to more precisely match its investigative needs. The FBI also said that it continues to modify its strategic planning methods to ensure that future resource allocations more closely meet field investigative demands. Specifically, in FY 2006, the FBI began a new strategic planning initiative called the Strategic Management System (SMS) to integrate strategic planning across operational and administrative areas. However, the FBI has not yet implemented SMS throughout all of its programs.

Action: The FBI has undertaken an organization-wide effort to incorporate the Balanced Scorecard/SMS Bureau-wide. This effort is focused on identifying customer expectations, strategic objectives, performance measures; and strategic initiatives. SMS sustainment includes institutionalizing systems to ensure that programs are managed to this "strategy map." As of October 2007, key components of each operational division at FBIHQ, as well as the Director's Strategic Leadership Team, have engaged in the development and sustainment of the SMS process. Further, efforts are currently underway to incorporate the SMS framework and resulting strategy maps into both the inspection and budgeting process at the FBI. As of September 2007, a corporate-level "Strategy Execution Team" has been put in place to enhance implementation of the most critical of those initiatives identified by the SMS process.

Issue: The OIG found that coordination efforts among the Department's four law enforcement components were not fully effective at preventing duplication of efforts by their violent crime task forces. The Department issued a new policy in May 2007 in response to the OIG report, that requires all U.S. Attorneys to report to the Department on violent crime task force coordination efforts, coordination problems, and guidance or policies adopted or revised to address the problems.

Action: Thirty-two U.S. Attorney's Offices have confirmed that only one violent crime task force is operating in their district. Thirty-three U.S. Attorney's Offices have convened meetings in their districts to address coordination and deconfliction issues. All but one of the remaining districts reported that co-location and regular meetings enable them to resolve these issues. One district has requested assistance from Washington, and the ODAG has reached out to that U.S. Attorney's Office. As a result of the coordination meetings, twenty-three districts have implemented policies and procedures with regard to task force coordination and deconfliction; other districts already had adequate policies and procedures in place.

Issue: In May 2006, an OIG evaluation concluded that while ATF's Violent Crime Impact Teams (VCIT), which seek to decrease homicides and other violent firearm crimes in targeted urban areas, may be an effective tool to reduce violent crime in target areas, there was inconsistent application by ATF of key elements of the VCIT strategy. In light of ATF's planned expansion of the VCIT initiative from 25 to 30 cities in 2008, a specific challenge for the Department is to fully implement VCIT as designed and to evaluate VCIT in order to gauge its effectiveness.

Action: In 2007, the Department announced the addition of four additional VCITs across the country, raising the total number of cities with teams from 25 to 29. Since the VCIT launch in 2004, the Teams have arrested more than 12,100 gang members, drug dealers, felons in possession of firearms, and other violent criminals, including over 2,200 identified as "worst of the worst" criminals. Also, VCITs have recovered more than 14,700 firearms.

To ensure that ATF consistently applies the VCIT program's key elements, ATF conducts semiannual surveys to evaluate the VCIT's consistent use of best practices and to solicit additional best practices. Also, ATF has developed a training course for VCIT field managers and staff on tailoring best practices to local conditions, reporting required information to Headquarters, and performing local evaluations of performance.

ATF has assigned an analyst to support the VCIT program, to continually gauge its effectiveness, and to coordinate a consistent message to VCITs across the country. The analyst analyzes VCIT workload statistics, activity narratives, and crime data from the target areas and has implemented a strategy ("VCIT Top Gun") to identify and highlight VCIT performance and achievements.

6. Detention and Incarceration

6. Detention and Incarceration: In order to meet its goal of providing a safe, secure, and humane confinement environment, the Department must achieve sufficient and economical prison and detention space, properly trained correctional officers, and appropriate management of high-risk inmates to protect the public from further criminal activities and to protect staff and inmates from harm.

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 Office of the Federal Detention Trustee's

(OFDT) revamping of the IGA pricing process through a pricing model known as eIGA may result in the Department paying higher jail-day rates than necessary. The OIG has also encouraged the Department to attempt to recover prior overpayments made to state and local jails.

Action: The Department views the basis of eIGA differently than the OIG does. The eIGA is designed to reach a fair and reasonable price for fixed-rate agreements based on price analysis conducted by comparing similar jails and operations. Price analysis supports a negotiation position that provides the Government and the jailer with an opportunity to reach agreement on a fair and reasonable price, providing 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, comparing it 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 previous method of determining the IGA rate – and rate increases – was based on cost, and it provided the jailers with an opportunity to increase cost and receive higher jail rates. Regardless of the reasonableness of the cost, as long as it was actual and allowable, the Federal Government would reimburse the jail facility. The eIGA method, on the other hand, 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." As such, the agreements with the state and local governments were negotiated, fixed-price agreements for the period in question, and binding to the parties. OFDT believes that, in the absence of fraud, the agreements are not subject to retroactive adjustment. Accordingly, as the OIG acknowledges, the Department's Civil Division is reviewing the IGAs in question to determine if fraud or other facts warrant legal recovery.

While the OIG believes it is necessary to understand a jail facility's "actual costs," collecting such information is not necessary when establishing a fixed-rate agreement based on price reasonableness. Regardless, OFDT has modified eIGA to collect the elements identified by the OIG, namely, average daily costs, indirect costs, and certain revenue. Further, OFDT has ensured that the eIGA negotiators received training in price-reasonableness as well as in the proper use of the additional collected cost information during negotiations with the facility.

The OIG's *Top Management and Performance Challenges in the Department of Justice – 2007* document states the average daily population in detention space is expected to increase from the current 56,000 detainees to 63,145 in FY 2008. The latest projections show that the anticipated average daily population for FY 2008 will be less than 60,000.

Issue: The Department should ensure that employees who work in the correctional environment benefit from appropriate safety precautions. More than 15 months after OIG Special Agent William "Buddy" Sentner was shot and killed by a BOP correctional officer who brought a gun into a federal prison in Florida, the BOP has not yet implemented basic security measures such as requiring all staff to pass through a metal detector before entering a BOP facility.

Action: BOP continues to progress towards implementing a policy that requires all staff entering institutions to pass through metal detectors and have their belongings examined by an x-ray device. On July 6, 2007, federal regulations authorizing these actions to occur randomly became effective. (See 72 FR 31178-01.) The agency is engaged in its statutory obligation to bargain with the union over the impact and implementation of the search procedures on bargaining unit staff.

Issue: Sexual abuse of inmates by BOP staff remains a problem in BOP facilities. An April 2005 OIG report highlighted the problem of sexual abuse of inmates and deficiencies in federal law that result in lenient sentences or unprosecuted cases. Congress enacted legislation in 2006 that increased the penalties and broadened federal jurisdiction for prosecuting staff sexual abuse of federal inmates.

Action: BOP takes all allegations of sexual abuse seriously and will continue to investigate those suspected of sexual abuse of inmates. We have issued Program Statement 5324.06, *Sexually Abusive Behavior Prevention and Intervention*

Program, which provides guidelines to address sexual abuse of inmates. Specifically, it addresses the security, treatment, and management issues related to inmate victims and inmate and staff perpetrators. These issues are taught to all staff in annual refresher classes, introduction to supervision courses, and new Associate Wardens and Warden training. Psychologists and Chaplains also are provided extensive training.

7. Sharing of Intelligence and Law Enforcement Information

7. Sharing of Intelligence and Law Enforcement Information: The Department's efforts to upgrade its IT systems remain a key factor in its ability to more fully meet its information-sharing challenge, and the Department still faces significant challenges to ensure the timely, effective, and secure sharing of vital intelligence and law enforcement information.

Issue: Despite over 6 years of development and more than $195 million in funding, the OIG concluded that the Integrated Wireless Network (IWN) project does not appear to be on the path to providing the intended seamless interoperable communications system. The $5 billion joint project among the DOJ, the Department of Homeland Security (DHS), and the Department of Treasury is intended to address federal law enforcement requirements to communicate across agencies, allow interoperability with state and local law enforcement partners, and meet mandates to use federal radio frequency spectrum more efficiently. The causes for the high risk of project failure include uncertain and disparate funding mechanisms for IWN, the fractured partnership between the Department and DHS on IWN, and the lack of an effective governing structure for the project.

Action: The Department supports the IWN program as the most appropriate strategy for providing DOJ agents with secure, reliable, and interoperable communications in the field, and has been working diligently to address the valid concerns regarding funding and the interagency partnership raised in the OIG's March 26, 2007, report. Specifically, DOJ is doing the following:

- In addition to traditional land mobile radio law enforcement solutions, the Department has been actively assessing alternative, less costly wireless technologies that can be deployed through the IWN program. It is likely that DOJ will implement a hybrid of several technologies to meet agent communications needs in a cost-effective manner. Regardless of the technology chosen, the IWN is a capital intensive program; it will require significant investments over multiple years. DOJ will continue to work with its law enforcement components and OMB to identify a strategy to provide a practical and sustainable level of funding for the program.

- Senior Department officials have worked with counterparts from DHS to develop a new interagency partnership agreement that accounts for the operational requirements and internal management strategies of the participating agencies. This agreement stresses commitment to achieve effective interoperability among and between federal, state, and local law enforcement/homeland security agents, as well as cost efficiency through practical sharing of resources. On August 23, 2007, the Deputy Secretary for Homeland Security, signed the *Memorandum of Understanding between the Department of Justice, Department of the Treasury, and the Department of Homeland Security regarding Joint Wireless Programs*. Currently, the memorandum of understanding (MOU) is being reviewed by the Treasury's Deputy Secretary. DOJ is confident that this revised partnership will be ratified prior to 2008.

- When the above-mentioned MOU is ratified, it should address the OIG's concerns regarding no "practical mechanisms to resolve disagreements between the departments." Under the new agreement, project participation by agencies – including roles and responsibilities – will be determined at start-up. Furthermore, these projects will be governed by the Joint Wireless Programs Coordinating Council (JWP-CC) which will be comprised of the Chief Information Officer (CIO) from each Department, select executives from operating components, and other Department executives as designated by the Deputy Secretaries or the Deputy Attorney General (DAG). The JWP-CC will perform numerous oversight functions including conducting a quarterly program review and an annual overall assessment of joint wireless program activities. All decisions of the JWP-CC will be made by consensus and any issue that cannot be resolved will be referred to the Deputy Secretaries and the DAG for consideration.

The OIG's report also cited concerns regarding the frustrations of the radio program managers and senior managers from four DOJ components regarding IWN program delays, the nature of the IWN partnership, and their inability to influence IWN Executive Board decisions. In response, the Department has examined its relationship with the components and currently is offering new opportunities to involve them in IWN management decisions. In September 2007, the Department hosted a Wireless Summit for executive, technical, and field agent representatives from each DOJ law enforcement component. This two-day event addressed law enforcement requirements and future wireless technologies, and provided an overview of the IWN strategic plan. Based on the positive feed-back, the Department intends to make the Wireless Summit an annual event and currently is scheduling meetings with each component to discuss the future of the IWN and their role in the project.

8. Information Technology Systems Planning, Implementation, and Security

8. Information Technology Systems Planning, Implementation, and Security: If the Department is to build on the advances it has made in IT systems planning, implementation, and security, it must closely manage these projects to ensure the systems are cost-effective, well-run, secure, and successful in achieving their objectives.

Issue: The Department places excessive reliance on contractors to develop, monitor, and run internal Department systems. The OIG has found numerous systems run by contractors in which Department employees do not always understand either the mechanics or the overall processes required to make the systems perform as intended. For example, audits of the TSC and the Department's watchlisting processes found that contractors are performing a significant portion of the information systems management and data analysis.

Action: The TSC has an extremely competent, innovative, and highly qualified contract staff. Its successes are, in part, directly attributable to its ability to identify, hire, and retain outstanding contract employees. Many of these employees have brought cutting-edge technology and business practices that are found in the TSC's software development methodology, standard operating procedures, and organizational structure. The TSC has created a one-badge atmosphere where contract staff and government employees of all agencies are treated equally, contributing to high morale and enhanced mission focus.

It is important to note the OIG did not criticize the TSC's use of contract staff in its recent audit. The TSC has grown from an operation of approximately 10 individuals in 2003 to more than 330 in 2007, with strategic growth plans pointing to more than 450 by the end of calendar year 2008 to meet increased watchlisting demands from the private sector and foreign partners, and to accommodate DHS's Secure Flight Program. The TSC is administered by the FBI, which is supplying 46 employees in support of it. Of the TSC's other signatory departments, only DHS has supplied it with more than two employees, committing to provide at least 45.

The TSC has taken great care in constructing its contracts, inserting key personnel clauses that allow the TSC to conduct in-depth interviews prior to the hiring of contract personnel. The TSC also has created an environment that fosters long-term retention of contract employees, creating continuity where many contract environments create turbulence. The TSC and the United States owe a great debt to the quality and performance of its contract staff, as well as its commitment to the mission of detecting and disrupting acts of terrorism.

The Department relies on contractors for a significant number of IT development and maintenance tasks – just as the construction business sub-contracts to specialists to pour cement and install plumbing – because it is the most cost-effective way to get results while managing the risk on large development efforts. However, for all large projects, the tasks that involve oversight (technical and cost) and direction setting always are staffed by government personnel. In addition, all large projects are subject to scrutiny by Executive Steering Committees which meet monthly or quarterly to review progress. The Department Investment Review Board (DIRB), co-chaired by the DAG and the CIO, oversees the high risk, high value programs, and meets regularly with programs that have the potential to miss deadlines or run over budget.

Issue: The cost information the Department provides on its IT systems to Congress, OMB, and senior management within the Department is unreliable. Specifically, IT system cost reporting within the Department is fragmented, uses inconsistent methodologies, and lacks control procedures necessary to ensure that cost data for IT systems is accurate and complete. The lack of complete and verifiable cost data undermines the effectiveness of oversight of IT projects by various entities, including the DIRB, Department and component CIOs, Congress, and OMB.

Action: The Finance Staff will work with the Office of the Chief Information Officer (OCIO) to review cost accounting policies and procedures that could be improved to ensure project teams at the component level report costs more accurately. A working group from the Chief Financial Officer (CFO) and OCIO staffs is being formed to evaluate existing Department and component policies and procedures for IT cost reporting, define the scope of work for improvement, and develop a work plan to address this recommendation. The group will clearly identify the meaning of "system costs" to Department management and, as required, answer the questions posed by DOJ external reports. A systemic solution to report costs uniformly in the various contexts will be predicated on the IT system boundaries, identification of data elements required at the transaction level in the accounting system, policies to require their incorporation, and system edits to require/validate them. The working group will meet in early November, with the objective of developing a plan of action by the end of the first quarter FY 2008.

9. Civil Rights and Civil Liberties

9. Civil Rights and Civil Liberties: Striking the appropriate balance between meeting its critical counterterrorism-related responsibilities and respecting civil rights, civil liberties, and privacy rights remains a key challenge for the Department.

Issue: An OIG review detailed significant improper or illegal uses of NSL authorities from 2003 through 2005, including violations involving the issuance of NSLs without proper authorization, improper requests under the statutes cited in the NSLs, and unauthorized collection of telephone or Internet e-mail transactional records. The OIG also identified many instances in which the FBI improperly obtained telephone toll billing records pursuant to more than 700 so-called "exigent letters" signed by personnel in the FBI's CTD without first issuing NSLs. The OIG found that the FBI's acquisition of this information circumvented the requirements of the NSL statute, violated the Attorney General's Guidelines, and contravened internal FBI policy. The OIG also found that the FBI issued some of these "exigent letters" in non-emergency circumstances, failed to ensure that there were duly authorized investigations to which the requests could be tied, and failed to ensure that NSLs were issued promptly after the "exigent letters" were sent. Moreover, the letters inaccurately represented that the FBI had already requested subpoenas for the information when, in fact, it had not. The FBI concurred with all of the OIG's recommendations and agreed to implement corrective actions. In addition, the Attorney General directed the Department's NSD and the Privacy and Civil Liberties Office (PCLO) to work with the FBI to implement corrective actions.

Action: The Department continually examines the policies and procedures related to various law enforcement activities, including counterterrorism investigations, to ensure appropriate safeguards for privacy and civil liberties exist and are perpetually improved. At the direction of the Attorney General, the NSD and PCLO have worked closely with the FBI to take corrective actions regarding the use of NSLs. Both the NSD and PCLO participate in a joint DOJ/ODNI working group to examine how NSL-derived information is used and retained by the FBI. Both also contribute to national security reviews of FBI field offices and Headquarters. These regular reviews represent a new level and type of oversight of national security investigations by career DOJ lawyers with years of intelligence and law enforcement experience.

NSD is establishing a dedicated Oversight Section within its Office of Intelligence, consisting of attorneys and staff members specifically dedicated to ensuring that the Department fulfills its national security oversight responsibilities across the board. NSD's Oversight Section also is responsible for reviewing all FBI referrals of Intelligence Oversight Board (IOB) violations in order to identify recurring problems and to assess the FBI's response to such violations. The

NSD's review effort focuses on whether the IOB referrals suggest that a change in policy, training, or oversight mechanisms is required. NSD reports semiannually to the Attorney General on such referrals and has been directed to inform the Department's Chief Privacy and Civil Liberties Officer of any referral that raises serious civil liberties or privacy issues.

The FBI also is increasing its focus on compliance with laws, rules, and regulations through its newly established Office of Integrity and Compliance. This Office will promote compliance in all FBI programs and activities. There is more detail about this office in the following discussion.

In its March 9, 2007, report, the OIG made 10 recommendations to the FBI. The FBI agreed to all of them. Below are the recommendations (shown in italics), followed by a description of the response to each. Following that are descriptions of additional measures taken since the issuance of the report.

Require all Headquarters and field personnel who are authorized to issue NSLs to create a control file for the purpose of retaining signed copies of all NSLs they issue.

The Deputy Director and General Counsel, in a call to the field, mandated that signed copies of NSLs be retained by issuing divisions. A Records Management Division (RMD) electronic communication (EC), dated March 9, 2007, also mandated that signed copies of NSLs be retained in the relevant investigative file. The requirement that signed copies of NSLs be retained is reiterated in a June 1, 2007, Office of General Counsel (OGC) EC providing comprehensive guidance on NSLs.

In addition, the RMD EC mandates that NSLs be uploaded into ACS as an NSL "document type." The NSL "document type" has been created in ACS to facilitate recordkeeping and reporting. With this new document type, NSLs can now be sorted and counted by field office in ACS. This reporting capability will be used to help verify current NSL reporting and will assist in NSL reviews.

Improve the FBI-OGC NSL tracking database to ensure that it captures timely, complete, and accurate data on NSLs and NSL requests.

Improve the FBI-OGC NSL database to include data reflecting NSL requests for information about individuals who are not the investigative subjects but are the targets of NSL requests.

In the short-term, OGC, National Security Law Branch (NSLB) has corrected deficiencies in the existing database found in the course of the OIG review. NSLB has made all fields pertinent to reporting and tracking mandatory entry fields, ensuring that data is entered in all pertinent fields. NSLB has also changed the default on US Person status to "US Person" as opposed to "Non-US Person," and changed the default on number of requests to "1" as opposed to "0." These changes should reduce the potential for error inherent in the database.

NSLB also has assigned additional personnel to the task of entering data into the database. The additional personnel have helped to relieve the burden of data entry and allow for additional time to enter data and therefore to take additional care to ensure that entry is correct. NSLB has conducted training for all personnel who enter data into the database to ensure that they understand the data that is being entered and can recognize when incorrect data has been provided for entry. The training also emphasized the use of the data, including the reporting requirements, to reinforce the need for error-free entry.

Ten analysts reviewed a 10 percent sampling of the data in the OGC NSL database. This review compared those records found in the database to those found in ACS and results indicate that NSLs have been underreported in the database. Those errors identified which relate to information not yet reported to Congress have been corrected.

In an EC dated March 16, 2007, the Deputy Director mandated that field offices conduct monthly counts of NSLs issued in order to reconcile numbers contained in the OGC database. These monthly counts, which began in April, are being compared to data in the OGC database to determine any inaccuracies in the database. Any discrepancies are being reconciled. Discrepancies are being used to correct systematic issues and to improve guidance and training on NSL reporting, both to the field and to Headquarters personnel involved in NSL reporting data entry. This monthly count will continue until the NSL sub-system to the Foreign Intelligence Surveillance Act (FISA) Management System (FISAMS), discussed below, comes online.

In the long-term, the FISA Unit of NSLB has developed an NSL sub-system in the FISAMS to address reporting and other issues in the NSL process. This sub-system prompts the drafter to enter information about the subject, the predication for the NSL, the type of NSL, the companies and specific targets of the NSL. The sub-system routes the NSL request through the various required reviews in a fashion similar to the current FISA workflow in FISAMS. Upon completion of all approvals, the NSL sub-system generates the EC and the NSLs for signature by the Special Agent in Charge (SAC), Assistant Director in Charge (ADIC), or designated FBIHQ approving official. The system automatically uploads the EC and NSLs into ACS upon approval. All information necessary to produce the required Congressional reporting will be collected as part of this process. This sub-system has been deployed in several field offices and in FBIHQ. It is expected to be available Bureau-wide by the end of calendar year 2007.

Consider issuing additional guidance to field offices that will assist in identifying possible IOB violations arising from use of NSL authorities, such as:

(a) *Measures to reduce or eliminate typographical and other errors in NSLs so that the FBI does not collect unauthorized information*;

In its June 1, 2007, Comprehensive NSL EC, the OGC mandated that both the model NSL cover ECs and the model NSLs available on the NSLB website be used in the drafting of NSLs. Consistent use of these models should reduce the occurrence of typographical errors in NSLs and their cover ECs. New training also emphasizes the potential for over-collection due to typographical errors and the need to assure information is appropriately requested. In addition, the NSL sub-system of the FISAMS allows for the creation of NSLs and cover ECs based on a single entry of information. This feature should greatly reduce typographical errors inherent in the current manual process.

(b) *Best practices for identifying the receipt of unauthorized information in the response to NSLs due to third-party errors;*

In an EC dated January 3, 2007, OGC mandated that NSL-derived information be reviewed prior to uploading the information into any database. The Comprehensive NSL EC reiterates this policy, and the need to review NSL-derived information prior to uploading is included in NSL training. OGC and the National Security Branch (NSB) are reviewing the findings of the Inspection review of NSLs to determine if additional procedures or training would improve compliance regarding this issue.

(c) *Clarifying the distinctions between the two NSL authorities in the Fair Credit Reporting Act (15 U.S.C. §§ 1681u and 1681v) (FCRA); and*

In an EC dated March 5, 2007, OGC and the NSB clarified the distinction between sections 1681u and 1681v of the FCRA and mandated a review of NSLs issued under FCRA to determine if full credit reports were improperly requested or obtained by the FBI. In addition, NSL training includes this issue and emphasizes the need for an international terrorism nexus to a national security investigation in order for a full credit report request under 1681v to be proper. The distinction also is highlighted in the Comprehensive NSL EC. Moreover, all field offices were required to review all counterintelligence files to determine whether such NSLs had been issued. Any full credit reports that were improperly obtained were required to be removed from the files and potential IOBs were required to be reported. Approximately 300 potential IOB (PIOB) violations were reported as a result of this audit, review of which is ongoing.

(d) *Reinforcing internal FBI policy requiring that NSLs must be issued from investigative files, not from control files.*

In an EC dated February 23, 2007, OGC mandated that NSLs be issued from open investigative files, and the NSL cover EC must not refer solely to a control file number. This policy is reiterated in the Comprehensive NSL EC and is contained in NSL training.

Consider seeking legislative amendment to the Electronic Communications Privacy Act (ECPA) to define the phrase "telephone toll billing records information."

The FBI and DOJ have drafted a proposed amendment to clarify the phrase “telephone toll billing records information” in ECPA. This proposed language provides clear types of information the FBI can obtain pursuant to section 2709 of ECPA. The FBI previously has submitted similar proposals.

Consider measures that would enable FBI agents and analysts to:

a) Label or tag their use of information derived from NSLs in analytical intelligence products, and
b) Identify when and how often information derived from NSLs is provided to law enforcement authorities for use in criminal proceedings.

A DOJ/ODNI NSL Retention Working Group was formed to examine issues regarding NSL retention. Although this group found that tagging of NSL derived information was not feasible at this time, it has recommended that the FBI require NSL-derived information to be placed in an NSL specific sub-file of the investigative file.

Take steps to ensure that the FBI does not improperly issue exigent letters.

In a March 1, 2007, EC, OGC prohibited the use of so-called “exigent letters” and set forth procedures for obtaining ECPA protected information under 18 U.S.C. § 2702 in emergency situations. This policy is reiterated in the Comprehensive NSL EC and is included in NSL training. In the course of the FBI-wide special review, the Inspection Division (INSD) included questions designed to ascertain whether exigent letters were used beyond the Communications Analysis Unit (CAU). This review found no instances where exigent letters were used in the field.

Take steps to ensure that, where appropriate, the FBI makes requests for information in accordance with the requirements of NSL authorities.

The Comprehensive NSL EC contains information on the requirements of NSL authorities. In addition, NSL training contains the requirements of the NSL authorities. OGC and NSB will review the findings of the Inspection special review on NSLs to determine if additional procedures or training would improve compliance regarding this issue.

Implement measures to ensure that FBI-OGC is consulted about activities undertaken by FBI Headquarters NSB, including its operational support activities, that could generate requests for records from third parties that the FBI is authorized to obtain exclusively though the use of its NSL authorities.

The two units in NSLB overseeing counterterrorism operations remain imbedded with their respective Counterterrorism Sections. In addition, OGC mandated that NSLB attorneys involved in counterintelligence matters regularly attend operational meetings to provide legal advice and oversight. The Comprehensive NSL EC mandates that all NSLs and NSL cover ECs issued by Headquarters components be reviewed and approved by NSLB attorneys.

Ensure that Chief Division Counsel (CDC) and Assistant Division Counsel (ADC) provide close and independent review of requests to issue NSLs.

The Comprehensive NSL EC mandates that CDCs and ADCs provide independent legal review of NSLs. The EC states that the legal review is separate and independent from the investigative review conducted by SACs. The NSL training also emphasizes the requirement that legal review be conducted by CDCs, ADCs, or NSLB attorneys. In a March 15, 2007, conference call and follow on email, the General Counsel reminded all CDCs, and ADCs of their need to provide independent legal review of NSLs. SACs also have been informed of their role in the NSL approval process and their need to respect the independence of the CDCs and ADCs.

Additional Measures Taken

Ongoing Review of NSL Matters: In the course of the NSL Audit conducted in March 2007, the FBI INSD generated approximately 2100 "checklist" items. Of that number, the CDCs in the field offices determined approximately 600 were non-PIOBs and, thus, not reportable to FBIHQ. Nevertheless, OGC is reviewing the CDC's determinations in those instances to ensure accuracy. The approximately 1500 remaining have been or are being reported to FBIHQ for adjudication as PIOBs. Approximately 900 draft adjudications of these PIOBs have been written. In addition, the Director ordered an audit of all NSLs in counterintelligence investigations as to which either the FBI requested full-credit reports or the credit reporting agencies provided full-credit reports. This audit yielded more than 300 PIOBs, which OGC currently is adjudicating.

The 22 potential IOBs identified by the OIG have been adjudicated by NSLB and five were determined to be reportable to the IOB. NSLB is currently developing an analytic approach to IOB violations in order to identify historic trends. This approach will assist in developing and focusing future training.

Exigent Letter Reconciliation: The CTD, INSD, and NSLB continue to review those situations where exigent letters were used. In some instances, NSLs or grand jury subpoenas were issued after the exigent letters. NSLB is reviewing those files for legal sufficiency. In other cases, valid NSLs have not been issued and now may not be issued because the underlying investigation is closed and/or it has been determined that the records were not properly provided under circumstances satisfying ECPA's emergency disclosure provision. If a number is not relevant to a pending investigation nor was provided under an emergency situation, then subscriber and toll billing records received in response to an exigent letter will be purged from FBI files and databases. If either of those conditions are met, then the FBI may retain the relevant information. NSLB is reviewing an overarching PIOB for CAU’s use of exigent letters. INSD is participating in a joint review with OIG regarding the use of exigent letters.

The FBI has devoted significant resources to this effort:

- A large group of FBI analysts is reviewing all of the exigent letters the FBI has copies of in order to determine whether, in fact, subsequent legal authority was issued to address the records obtained with an exigent letter. This initial review of the letters is complete, and these phone numbers have been sent to CTD and NSLB for additional review and action. To the extent there are records that have not yet been addressed, appropriate steps will be taken (i.e., if the records were relevant to an investigation and that investigation is still open, an NSL will be issued; if not, the records will be charged out of the system).

- NSLB and CTD are working together to correct the so-called “blanket NSLs” that were issued with respect to blocks of telephone numbers. These “blanket NSLs” were issued without an authorizing EC documenting the rationale for obtaining the underlying records. Where appropriate, CTD will issue corrective NSLs with supporting ECs to address records pertaining to the numbers listed on these “blanket NSLs." Thus far, six corrective NSLs have been issued to provide legal authority for the retention of the information. These corrective NSLs have been reviewed for legal sufficiency and are accompanied by ECs, in accordance with FBI policy. An additional five “blanket NSLs” are still under review. Similar action will be taken for those phone numbers contained in the exigent letters for which legal authority has not been found. Where the FBI can identify no legal basis for retaining records resulting from an exigent letter or “blanket NSL,” those numbers will be removed from FBI files and databases.

Joint NSLB-NSD Reviews of NSL Use: OGC is meeting regularly with NSD to determine the best approach to FBI NSL policy and other aspects of national security law. NSD has been consulted on the development of new policy regarding NSLs to address issues revealed by the OIG report. In addition, NSD and NSLB will conduct at least 15 national security reviews of FBI field offices in calendar year 2007 which will include the use of NSLs. All these reviews are accompanied by NSL training. Additional funding of $60,000 was made available for the conduct of NSL reviews and NSL training in field offices. As of October 19, 2007, such reviews had been completed in 12 field offices (Little Rock, Charlotte, Milwaukee, New Orleans, New Haven, Albany, Knoxville, Cleveland, Jacksonville, Las Vegas, Memphis and Boston) and Headquarters.

Comprehensive Guidance: As mentioned above, OGC issued a June 1, 2007, EC providing an overview of FBI NSL policy and setting for new policies addressing issues raised by the OIG report. A draft of this policy was briefed to Congressional staff and privacy groups. The FBI incorporated comments from Congressional staff and privacy advocates in the final version of the policy. This policy will be converted from EC form to conform to the FBI's new Corporate Policy Directive format.

FBI NSL Working Group: The FBI OGC has formed a working group to facilitate the continued implementation of the OIG's recommendations, improve the NSL process, and identify issues involving the use and reporting of NSLs.

Increased NSL Training: NSLB has developed a new NSL training module incorporating the findings of the OIG. This training addresses the common errors discussed in the OIG report, such as typographical errors, confusion regarding 1681v, and legal review and approval. The training discusses the prohibition on the use of exigent letters and lays out procedures for properly obtaining information in emergency situations in accordance with 18 U.S.C. § 2702. OGC has mandated that all NSLB attorneys visiting field offices conduct NSL training during their visit. Since March of 2007, 23 of the FBI's 56 field offices and at least 2379 agents, analysts, and other employees involved in NSLs received live training from NSLB on NSL issues. While some Headquarters units had already received NSL training following the OIG report, mandatory training to personnel in the Counterterrorism, Counterintelligence, and Cyber Divisions was conducted in early May. NSLB and Training Division are currently developing an online virtual academy course on NSLs. Once developed, this training will be required for all personnel involved in drafting and approving NSLs and will supplement live training.

Increased Oversight Role: OGC has obtained two new SES positions within NSLB. One position will head a new section overseeing operational aspects of national security law while the other will head a national security law training and policy section. The addition of these two positions will add senior personnel in positions overseeing national security matters.

Creation of the Office of Integrity and Compliance: The FBI Director has proposed an Office of Integrity and Compliance Program to promote FBI compliance with the laws, rules, and regulations not only in NSLB but in all FBI programs and activities. It is noted that the Office is a proposed activity until such time as it is finally approved by the Administration and the Congress. In addition to establishing the Office, he has approved the creation of five committees along existing business lines, chaired by Executive Assistant Directors, to identify possible weaknesses in the compliance control environment (policies/training/monitoring), and to put corrective action plans in place to address these perceived weaknesses. These committees meet quarterly and each has met twice. Additionally, the Director established and chairs a Compliance Council, which meets twice a year. The Council will receive reports from the Committees on the issues identified and the remedial action being taken, and it will provide feedback on these and any other issues. In addition, human resource policies have been, or are in the process of being, changed, including rewarding outstanding accomplishment in compliance and ethics, making initial corrective action plans part of the cascading objectives of those accountable for corrective action plan implementation, and non-retaliation policies. Further, training programs emphasizing the responsibility of all employees to know the rules, comply with the rules, and report possible compliance issues are being developed. Anonymous and confidential channels for reporting compliance issues are also being developed.

10. Cybercrime

10. Cybercrime: With rapid technological advances and the widespread use of the Internet, cybercrime is a growing source of criminal activity and an emerging challenge for the Department and law enforcement nationwide.

<u>Issue</u>: The opportunity for cybercrime increases with the growth of the Internet, and it poses a serious threat to both U.S. national economic and security interests. The Department and its

components, including the FBI, Criminal Division, and U.S. Attorneys, have taken steps to address the varied facets of cybercrime. While the Department has developed several initiatives to combat aspects of this complicated crime, it must continue to respond to this growing challenge.

Action: The FBI continues multiple initiatives to combat cybercrime on the Internet. The Cyber Division has formed a working group with five countries to share knowledge, experience, and best practices to counter the rising threat associated with computer intrusions. The Cyber Division's Internet Crime Complaint Center has received the one millionth complaint related to Internet crime activity, and continues as a vital clearinghouse for cybercrime information for the FBI's state, local, and tribal law enforcement partners. The FBI established the Cyber Initiative and Resource Fusion Unit to maximize the resources of the private sector concerning cutting edge computer hardware and software technology, in addition to its longstanding Public Private Alliance Unit. The FBI's Innocent Images National Initiative, dedicated to combating child pornography, has expanded to include a cadre of foreign law enforcement officers stationed and working alongside a team of Special Agents and IAs. The Cyber Crime Fraud Unit is leading a team of FBI and foreign agencies to combat the proliferation of counterfeit goods, including the purchases of fake products by the U.S. Government, in the Cisco Raider case.

The Criminal Division also plays a key role in the Department's ongoing response to cybercrime. In addition to the efforts outlined by the OIG, the Department is involved in the following:

- A May 2006 Executive Order created the Identity Theft Task Force, chaired by the Attorney General, requiring that it draft a Strategic Plan to improve the federal response to identity theft in the areas of awareness, prevention, detection, and prosecution. The Task Force sent the draft Plan to the President in April 2007. Recommendations targeted key phases in the "life cycle" of an identity theft crime. Broad policy recommendations included: (1) reducing the unnecessary use of Social Security Numbers (SSNs) by federal agencies; (2) establishing national standards for the private sector regarding how to safeguard personal data and notify consumers of significant breaches; (3) educating the public and private sector to deter, detect, and defend against ID theft; and (4) establishing a National ID Theft Law Enforcement Center to coordinate investigation and prosecution of ID thieves. Criminal Division attorneys are working with the Task Force to implement the recommendations in the Strategic Plan.

- Criminal Division attorneys are working to promote the Convention on Cybercrime world-wide, which will strengthen the United States' ongoing international leadership role in cybercrime issues and facilitate rapid international cooperation in cybercrime cases. During this past year, a number of countries, including Mexico, have applied for accession to the treaty with the encouragement of the U.S. government. Also, the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) has taken a leading role in expanding and administering the G8 24/7 Network, now comprising over 50 countries from around the world to respond to cybercrime and cases involving electronic evidence.

- CCIPS, working with EOUSA, continues its efforts to facilitate and support the work of Computer Hacking and Intellectual Property (CHIP) Coordinators in the field. During the past year, CCIPS created the position of National CHIP Program Coordinator and filled that position with an experienced AUSA detailee. Seven new CHIP Units were created, and currently, 25 U.S. Attorney's Offices have operational CHIP Units. For the past 12 years, CCIPS has organized and led an annual training conference for CHIP Coordinators from around the country. In June 2007, CCIPS attorneys and technologists presented and participated in the first ever joint meeting of the CHIP Coordinators and the Government Forum of Incident Response and Security Teams ("GFIRST"), where members of DOJ, DHS, and the DHS U.S. Computer Emergency Response Team (US-CERT) were able to work with hundreds of researchers, security professionals, network operations specialists, and computer security first responders to discuss critical computer security issues.

- CCIPS continues to target and prosecute computer network crime aggressively and bring groundbreaking prosecutions of novel and emerging computer crimes, increasing its computer crime cases by over 25 percent. Working with other sections of the Criminal Division and AUSAs, CCIPS has prosecuted cases that target, among others, "hack, pump, and dump" securities fraud schemes, malicious "botnets," and online data theft.

In June 2006, the Attorney General issued the Progress Report of DOJ's Task Force on Intellectual Property announcing implementation of all 31 of the Task Force's recommendations. Among other accomplishments, the Task Force dismantled two of the largest international software piracy groups operating on the Internet; increased the number of defendants prosecuted for IP offenses by 98 percent from 2004 to 2005; and provided technical assistance and training to over 3,000 prosecutors, judges, and agents from 107 countries. Since the issuance of the Progress Report, Criminal Division attorneys have continued to work on those Task Force recommendations that required ongoing implementation. For instance, in the past year, Criminal Division prosecutors' accomplishments have included, but not been limited to: (1) creating the Intellectual Property Protection Act of 2007 (IPPA), which is a comprehensive legislative package designed to better equip law enforcement with the tools necessary to protect intellectual property rights and deter intellectual property crime (in May 2007, the Attorney General transmitted it to Congress); (2) placing a second Intellectual Property Enforcement Coordinator "IPLEC" in Sofia, Bulgaria, in November 2007 (the first was placed in Bangkok Thailand last year); and (3) increasing by more than 35 percent, in 2007, the number of defendants charged with IP crimes (CCIPS' prosecutions only).

The Internet is providing predators with a new place – cyberspace – to target children for criminal acts. The U.S. Attorneys are leading Project Safe Childhood, a joint effort of federal, state, and local law enforcement, along with community leaders, designed to protect children from online exploitation and abuse. The result has been a 25 percent increase in cases, an increase in the percentage of defendants found guilty, and an increase in the length of defendants' sentences.

Additional resources have been provided to the CHIP units that were established in U.S. Attorney's Offices with significant concentrations of high tech industry. These units include prosecutors and investigators who have received specialized training to enable them to investigate and prosecute computer crimes such as computer intrusion, copyright and trademark violations, and internet fraud. They work closely with the FBI and other agencies to build relationships with the high tech community. As part of this effort, each U.S. Attorney's Office has designated an identity theft coordinator and has increased its focus on identify thieves, resulting in an increase of over 25 percent in identify theft prosecutions.