Office of the Inspector General
United States Department of Justice

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice

before the

House Appropriations Committee
Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies

concerning

Oversight of the Federal Bureau of Investigation

September 14, 2006

Mr. Chairman, Congressman Mollohan, and Members of the Subcommittee:

Thank you for inviting me to testify about the Office of the Inspector General's (OIG) oversight work related to the Federal Bureau of Investigation (FBI). As the FBI continues its transformation after the September 11 terrorist attacks, the OIG continues to devote extensive resources to examining FBI programs and operations. We have conducted many reviews in critical areas, including the FBI's efforts to upgrade its information technology (IT) systems; its allocation of investigative resources; its counterespionage and internal security challenges; and its management of the FBI laboratory. In addition, we review allegations of misconduct and civil rights and civil liberties abuses involving FBI and Department of Justice employees.

In this written statement, I will summarize several of the FBI reviews that the OIG has completed since September 2005, when I last testified before this Subcommittee. In addition, I will describe several important ongoing OIG reviews. A significant part of my testimony will focus on the FBI's Sentinel program, a multi-year project to upgrade the FBI's IT systems. At the request of this Subcommittee, Director Mueller, and others, the OIG is continuing to conduct a series of reviews of the Sentinel program and to monitor its progress.

Before discussing Sentinel and our other reviews, I first want to acknowledge the cooperation we have received from the FBI in the OIG's varied and extensive oversight. To conduct our reviews and investigations, the OIG regularly seeks detailed information from the FBI about its operations and programs. We generally have received good cooperation from the FBI regarding our need for this information. When there are problems and questions, FBI senior managers normally are available to address our concerns and give us the information we need. In particular, Director Mueller has made clear his expectation that the FBI cooperate fully with the OIG. We appreciate that support.

We recognize that many of our reports are critical of aspects of FBI programs and operations. In reaching these conclusions, we keep in mind the FBI's difficult job and the importance of its mission. The purpose of our reviews and our criticisms is to help the FBI and the Department of Justice improve their operations. We have found that the FBI, by and large, understands our role and considers our recommendations in the constructive light in which they are made.

I will now discuss the OIG's oversight of the Sentinel project, an area I know this Subcommittee is closely monitoring.

I. SENTINEL

The OIG has continued to review the FBI's efforts to upgrade its information technology systems. In particular, we are examining the FBI's Sentinel program, a project to replace its antiquated Automated Case Support (ACS) system with a modern case management system.

Sentinel is the successor to the Virtual Case File (VCF) project, which the FBI ended unsuccessfully in 2005 after expending 3 years of effort and $170 million. Audits by the OIG found that the VCF project failed for a variety of reasons, including poorly defined and slowly evolving design requirements, weak information technology investment management practices, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on information technology projects, unrealistic scheduling of tasks, and inadequate resolution of issues that warned of problems in project development.

In March 2005, the FBI scrapped development of the VCF and focused its efforts on Sentinel, a planned $425 million, 45-month project intended to move the FBI away from paper-based records to an electronic case management system that will process, store, and manage FBI case information to allow it to more effectively perform its investigative and intelligence operations and share information.

In March 2006, the OIG released the first in a series of audit reports that will examine the progress of the Sentinel project. The March report discussed the FBI's pre-acquisition planning for the project, including the approach, design, cost, funding sources, time frame, contracting vehicle, and oversight structure. In that report, the OIG concluded that the FBI had developed information technology planning processes that, if implemented as designed, can help the FBI successfully complete Sentinel. In particular, the OIG found that the FBI has made improvements in its ability to plan and manage a major IT project by establishing Information Technology Investment Management processes, developing a more mature Enterprise Architecture, and establishing a Program Management Office dedicated to the Sentinel project.

However, our March report highlighted several concerns about the Sentinel project that we believed the FBI needed to address: the (1) ability to track and control Sentinel's costs, (2) lack of an established Earned Value Management process to guide the Sentinel upgrade, (3) ability to reprogram funds to complete the second phase of the project without jeopardizing the FBI's other mission-critical operations, (4) efforts to ensure that Sentinel will allow the sharing of information between the FBI and other intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (5) incomplete staffing of the Sentinel Project

Management Office, and (6) lack of complete documentation required by the FBI's information technology investment management processes.

The OIG's second audit of Sentinel – which is nearing completion – is examining the FBI's contracting for the project, including whether the FBI is establishing the necessary work requirements and baselines. In addition, the current audit examines the FBI's progress in resolving the concerns highlighted in our first review.

In March 2006, the FBI awarded Lockheed Martin Systems a $57 million task order for Phase 1 of Sentinel, with options for an additional $248 million for three additional phases and the operation and maintenance of the system.

In addition to this cost baseline, the FBI has developed an overall schedule for the Sentinel project and is establishing specific baselines for each of its four phases. Over the next 4 years, Lockheed Martin will be responsible for designing, developing, integrating, testing, deploying, operating, and maintaining Sentinel, which primarily will be based on commercial-off-the-shelf software. Lockheed Martin is performing this work under a cost-plus-award-fee arrangement, similar to the contract used during the Trilogy project. However, we are finding that the FBI is providing much greater control and oversight for Sentinel compared to the weak project management practices evident in the Trilogy project.

Although our current audit is not complete, our preliminary findings indicate that the FBI has made progress toward resolving most of our initial concerns about planning for the Sentinel project. However, some concerns, such as the full staffing of the Sentinel Program Management Office (PMO), have not yet been fully addressed. Moreover, our current audit has identified additional issues that we believe the FBI must resolve in order to avoid serious problems as the Sentinel project continues through its first phase of development and enters its more challenging and higher-risk second phase in early 2007. These issues include uncertainty over risk mitigation, contingency planning, and total project costs.

Cost Tracking and Controls: The OIG's prior reviews of the Trilogy project, as well as audit work by the Government Accountability Office, found that the FBI lacked an effective, reliable system to track and validate the Trilogy project's costs. Our March 2006 report also noted that while the FBI stated that it was evaluating a tool to track Sentinel project costs, potential weaknesses in cost control remained a project risk for Sentinel.

In our current audit work, we found that the FBI has established a baseline budget and schedule to allow it to track the costs and progress of the Sentinel project. The FBI and Lockheed Martin also have implemented Earned

Value Management (EVM) systems, in accord with Office of Management and Budget requirements, to track and validate Sentinel project costs throughout the life of the project. The FBI's EVM system relies on cost data provided through the FBI's Budgetary Evaluation and Analysis Reporting System, which extracts purchase order information from the FBI's Financial Management System and generates reports on funds requested, amounts approved and spent, and obligations that have not yet entered the FBI's overall Financial Management System.

The FBI is using the EVM system to help manage project risks by providing an early warning of unexpected costs and problems that could delay Sentinel's completion. We are also monitoring the FBI's EVM reporting to identify any unexplained growth in overall project costs or any schedule delays.

In addition to the cost-reporting systems, the FBI has established other controls to help ensure that Sentinel expenditures are authorized in advance and that items are verified when delivered and validated when invoiced. For example, the FBI has developed a system of overlapping responsibilities for oversight of Sentinel's costs that include: accounting, auditing, and budget monitoring by the FBI's Finance Division; detailed tracking of Sentinel's costs by the Office of the Chief Information Officer's IT Financial Management Unit; tracking and controlling program and development costs and developing policies and procedures for processing invoices, requisitioning and procuring equipment, reviewing contractor time charges, and resolving discrepancies by the Sentinel PMO Business Management Unit.

We believe that the tracking systems and controls the FBI has implemented since the Subcommittee's last oversight hearing provide greater assurance that the FBI will be better able to monitor and control project costs for Sentinel than was the case under Trilogy.

Funding for the Sentinel Project: Our March 2006 report noted concerns about the FBI's ability to reprogram significant funds to complete the second phase of the project without jeopardizing its other mission-critical operations. Our current audit found that the FBI faces uncertainty over the source of the approximately $150 million the FBI says it needs in fiscal year (FY) 2007 funds to continue the Sentinel project. The President's FY 2007 budget request included $100 million for Sentinel, and the FBI would need an additional $50 million to bridge the gap between the requested funds and its FY 2007 requirements for Sentinel. The FBI expects to be able to rely on some amount of unused FY 2006 funds, including management reserves, but the specific amount and source of funds that will be required to bridge any funding gaps remain unclear. The FBI's Chief Information Officer (CIO) recently told us that an FY 2007 appropriation of less than $100 million would be cause for

concern and could result in an unanticipated level of reprogramming of FBI resources to fund the Sentinel project.

As we reported in March 2006 and as various FBI managers stated to us, a second significant reprogramming of FBI funds could erode the FBI's mission capability in counterterrorism, cyber crime, and other important operational areas. Therefore, until the funding issues are addressed, we remain concerned about the impact that reprogramming significant amounts of non-IT funds to support Sentinel would have on other critical FBI priorities.

With respect to overall project costs, the FBI reported to us that it stands by its estimates that the total cost of Sentinel will be $425 million, with $305 million to cover work by Lockheed Martin on a variety of task orders and an additional $120 million to cover other costs, such as the FBI's Program Management Office staffing, contractor support, and contingency reserves. Training costs are now built into the Lockheed Martin portion of the estimate, which was a concern we noted in our March 2006 report when the FBI had not yet developed a complete cost estimate for its training plans.

We are examining the FBI's cost estimates in our ongoing audit and have some concerns about the scope of the costs contained in the estimate. For example, it is unclear whether the cost estimate accurately includes operations and maintenance costs. We found that some portions of one of the FBI's estimates provide costs for 2 years, while other portions include costs for 3 years.

In addition, our current work also has identified costs associated with Sentinel that have been categorized by the FBI as separate projects and therefore not included as part of Sentinel's overall $425 million cost. For example, the implementation of Sentinel will require changes to the FBI's National Name Check system. In response to a request from a federal, state, or local agency, the National Name Check Program queries FBI records to determine whether the person named in the request has been the subject of an FBI investigation or mentioned in an FBI investigation. The data system used by the Name Check program relies very heavily on the ACS system, which Sentinel is intended to replace. The estimated cost of updating the existing name check system to work with Sentinel is over $10 million. In addition, the FBI has ongoing security and process re-engineering projects that will be affected by Sentinel. If these separate projects were included as Sentinel costs, the $425 million cost estimate could be higher.

The FBI's position is that these separate projects are enterprise-wide projects that will benefit the FBI's overall IT structure, including Sentinel but also many other FBI systems. The CIO and the Sentinel Program Manager contend that the costs of these other independent projects ought not be

considered as Sentinel costs. While we agree that these Sentinel-related projects may not be direct Sentinel costs, in our view Sentinel is mainly driving the need for these projects, even though they may also benefit the FBI's overall IT systems.

Moreover, variations in the estimates of Sentinel's projected costs demonstrate the difficulty of estimating the cost of such a complex information technology project at its outset. Because of these difficulties, and because the project is in its early stages, we could not validate the FBI's overall estimate of $425 million for Sentinel, and we believe that the ultimate cost could be lower or higher. As the FBI finalizes Sentinel's design and gains experience with actual project costs, we urge it to regularly update its estimate of the overall project costs to keep Congress and the Department informed. In addition, we intend to continue to monitor the costs of the project as it progresses and inform the Congress and the Department of our findings.

Information Sharing: Our March 2006 report expressed concerns that the FBI had not adequately examined Sentinel's ability to share information with computer systems in other Department of Justice components, the Department of Homeland Security, and other intelligence community agencies, and that the FBI had not fully coordinated with these outside agencies. Since our last audit we have found that, consistent with our recommendations, the FBI has focused more attention on external information-sharing needs and has been coordinating with these and other federal entities, including the Drug Enforcement Administration, Immigration and Customs Enforcement, and the Office of the Director of National Intelligence. FBI officials have also stated that Sentinel is being built to meet the standards of the National Information Exchange Model, a joint Department of Justice and Department of Homeland Security standard that has become the government-wide standard for any new law enforcement and intelligence systems being developed. We will continue to monitor the information-sharing capacity of Sentinel as the project proceeds.

Program Management Office (PMO) Staffing: Our current audit work shows that the FBI has made progress in the staffing of the Sentinel PMO since our first report. Of a total planned staff of 78, 63 positions have now been filled. The FBI said it has intentionally delayed filling 10 positions until the second phase of Sentinel and is considering the possibility of reducing the number of positions by 4 because of less overlap in the project phases than initially anticipated. Five other positions remain vacant, although the Program Manager recently told us that candidates have been selected for several of these positions and are in the process of being hired.

We are still concerned that the FBI has not yet hired a property manager for the project, since the FBI lacked adequate control over equipment purchased during the Trilogy project. We also believe that, due to the lack of

sufficient project oversight during Trilogy and the VCF portion of that project, the FBI should complete the staffing of positions currently needed for the PMO and provide enough lead time to process and provide the necessary security clearances for any new hires required to help manage the upcoming phases of the project.

Information Technology Investment Management Processes: Our March 2006 report discussed the progress the FBI had made in establishing sound IT investment management processes through its Life Cycle Management Directive. However, we noted that two key plans required by the directive had not yet been developed pending the completion of the project design: Independent Verification and Validation (IV&V) and the system security plan. The FBI's plan to fully implement the IV&V process was delayed while the Department obtained a contract for Department-wide IV&V services.

We believe the IV&V performed by a contractor or contractors not otherwise associated with the Sentinel project is a critical risk-mitigation approach. The IV&V process requires the testing of the project's software and systems against the design requirements to ensure that the project's performance expectations are being met. The CIO recently told us that the Department has completed its contracting process and that about eight vendors are available to the FBI to perform aspects of IV&V throughout the development of Sentinel.

A system security plan is also critical to help ensure that Sentinel will meet the FBI's security standards and can be certified and accredited for use within the FBI's operating environment. The CIO recently told us that the security plan has now been drafted and is in the approval process.

In accordance with the FBI's Life Cycle Management Directive, the final design for the first phase of the Sentinel project will occur in October 2006. Because Lockheed Martin will be using off-the-shelf components to develop Sentinel, the complication and risk of the project design should be lessened, although configuring all of the components into one seamless system will remain the greater challenge. The FBI has stated that it will conduct future design reviews prior to the initiation of subsequent phases in order to solidify the design and deliverables for each phase.

Project Risks and Mitigation: In addition to software design and security risks, we view the FBI's ability to successfully migrate data from the ACS system to Sentinel as a potentially significant challenge. If the migration were to fail or be seriously delayed, essentially the FBI will be saddled with maintaining its legacy ACS system with all of its flaws. An inability to migrate the ACS data would also result in a Sentinel system that builds its data forward, without the benefit of years of investigative data compiled in the old

system. Further, should ACS cease to be maintainable, that data could effectively be lost. The Sentinel Program Manager told us that the task of "cleaning" and reconciling the ACS data for migration into Sentinel is not technically difficult and the FBI plans to use an available software tool for that purpose. However, he pointed out that it will take a significant amount of work to accomplish.

Another potential risk we are monitoring is the extent to which Sentinel will actually use commercial-off-the-shelf software modules as intended. A high degree of customization of the software could result in increased costs and schedule delays. The Program Manager told us that the components for Sentinel are all off-the-shelf and little or no customization is anticipated. The key task will be configuring Sentinel's various applications – such as the workflow, document management, searching and reporting, and electronic signatures – to all work together. The Program Manager noted that Lockheed Martin has successfully configured similar systems in other major projects.

To its credit, the FBI has created a list of 20 high-risk areas associated with the Sentinel project that warrant active monitoring. While we believe the FBI's establishment of a risk management program is a positive step, we are concerned that contingency plans, and the triggers for activating such plans, currently exist for only three risks – including only one of the top five risks. The Program Manager told us that in some cases it is difficult to develop a contingency plan before a risk becomes an operational issue. He explained that the focus is on preventing problems that would rise to the level of requiring mitigation, and that if a problem occurs a corrective action will be developed. He also told us that many risks are temporary and as a project phase progresses the risk may become moot and is closed. However, we believe there should be a plan in place for high risks that have the potential to result in a significant cost, schedule, or performance deviation from the project baselines.

OIG Conclusions Regarding the Sentinel Project: By establishing stronger IT investment management processes and an array of monitoring and control mechanisms, the FBI has positioned itself to better manage the Sentinel project and avoid the problems that occurred in the Trilogy and VCF projects. However, this does not mean that Sentinel is risk free. While the FBI has corrected or alleviated many of the concerns we raised in March 2006, several areas warrant continued attention to avoid potentially serious problems as the project progresses, such as accurately estimating total project costs, the ability of the FBI to reprogram funds without adversely affecting mission-critical operations, staffing of the Sentinel PMO, and the ability to mitigate project risks and correct problems before they seriously affect project costs or schedule.

Consistent with this Subcommittee's and Director Mueller's requests, the OIG will continue to monitor and periodically issue audit reports throughout the four overlapping phases of the FBI's Sentinel project in an effort to track the FBI's progress and identify any emerging concerns related to Sentinel.

II. OTHER OIG REPORTS EXAMINING FBI ISSUES

The OIG has continued its oversight of other FBI programs and operations since this Subcommittee's FBI oversight hearing last year. In this section of my testimony, I briefly summarize some of the most important of those recent reviews.

1. Seaport Security: The OIG released an audit report in March 2006 that examined the FBI's efforts to protect U.S. seaports from terrorism. The protection of U.S. seaports is a shared responsibility among the U.S. Coast Guard, the U.S. Customs and Border Protection agency, and the FBI. The Coast Guard protects and enforces laws at seaports while the Customs and Border Protection agency enforces import and export laws and inspects cargo at seaports. The FBI, as the lead federal agency for preventing and investigating terrorism, has an overarching role in protecting the nation's seaports, which includes gathering intelligence on maritime threats and maintaining well-prepared tactical capabilities to prevent or respond to maritime-based terrorism.

The OIG review of the FBI's efforts to protect the nation's seaports found that the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks at seaports. For example, the FBI has created a centralized maritime security program at FBI Headquarters and, in addition to its counterterrorist tactical teams, placed enhanced maritime SWAT teams in the FBI field offices closest to 14 of the nation's strategic seaports. Further, most of the FBI's 56 field offices have Maritime Liaison Agents responsible for coordinating with other federal agencies on maritime security.

However, we found that the FBI did not always assign these agents according to the threat and risk of a terrorist attack on a given seaport. For example, an FBI field office with six significant seaports in its territory had only one maritime liaison agent while another FBI field office with no strategic ports in its area had five Maritime Liaison Agents. Furthermore, the OIG review found that the FBI and the Coast Guard had not yet fully resolved issues regarding their overlapping responsibilities, jurisdictions, and capabilities to handle a maritime terrorism incident. An interim Maritime Operational Threat Response (MOTR) plan, which was developed under the National Strategy for Maritime Security and issued in September 2005, establishes protocols for lead and supporting agencies in responding to terrorist threats in the maritime

domain. However, our review found that the interim MOTR did not fully clarify these issues.

This lack of jurisdictional clarity could hinder the FBI's and the Coast Guard's ability to coordinate an effective response to a terrorist threat or incident in the maritime domain. Specifically, our audit report expressed concern about how confusion over authorities would affect the two agencies' ability to establish a clear and effective incident command structure in response to a terrorist attack on a seaport. In our judgment, unless such differences over roles and authorities were resolved, the response to a maritime incident could be confused and potentially disastrous.

The OIG report made 18 recommendations that focus on specific steps that the FBI should take to improve its counterterrorism efforts regarding seaport and maritime activities, including resolving overlapping responsibilities with the Coast Guard through the MOTR plan before a terrorist incident occurs; leading more interagency maritime-related exercises involving likely terrorism scenarios; preparing and using after-action reports after these exercises in order to identify lessons learned; and assessing the threat and risk of maritime terrorism compared to other threats and assigning resources accordingly.

The FBI has implemented three of our recommendations concerning the management of its maritime security program and is working on the improvements needed to implement other recommendations, including our recommendation to resolve potential incident command conflicts that may occur during a maritime response. The FBI also reports that the interim MOTR plan that is used to guide incident response and command has been revised since our report was issued. The FBI expects the revised MOTR plan to be issued this month.

2. Status of IDENT/IAFIS Integration: In July 2006, the OIG issued the latest of its periodic reports monitoring the FBI's progress toward achieving biometric interoperability between the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT). The report, the sixth issued by the OIG, found that the FBI and the DHS are developing the first phase of a three-phase plan to make IDENT fully interoperable with IAFIS by December 2009.

Fully interoperable fingerprint systems would allow law enforcement and immigration officers to more readily identify criminals and known or suspected terrorists trying to enter the United States and those already in the country. However, the FBI and the former Immigration and Naturalization Service, now part of the DHS, developed separate automated fingerprint systems in the early

1990s. The FBI's IAFIS is based on 10 rolled fingerprints, while the DHS's IDENT system uses 2 flat fingerprints. The differing fingerprint collection requirements and preferences of the FBI and the DHS had created an impasse that stalled interoperability efforts. This impasse was resolved in May 2005 when the DHS agreed to use 10 flat fingerprints as its primary standard for its automated fingerprint system.

In July 2006, we reported that that the FBI and the DHS were moving forward toward interoperability and had begun implementing a three-phase plan to make IDENT and IAFIS fully interoperable by December 2009. The FBI since has confirmed that on September 3, 2006, the FBI and the DHS implemented the first phase of the interoperability plan by deploying a link between the two agencies' systems that will allow the exchange of copies of key immigration and law enforcement data.

In the latter two phases of the plan, the agencies intend to expand the amount of immigration and law enforcement data shared and to allow access to that data by federal, state, and local law enforcement agencies. When the interoperability effort is completed, which the FBI and DHS estimated will occur in December 2009, a single request is expected to search all fingerprint records maintained by the FBI and the DHS, and the requestor will receive all associated criminal history and immigration information about a subject.

Until a fully interoperable system is achieved, the FBI has taken interim steps to reduce the risk that criminal aliens or terrorists will enter the United States undetected. As we recommended in our December 2004 report, the FBI has increased the transmission of "Known or Suspected Terrorists" records to the DHS from monthly to daily. In addition, the FBI has improved the overall availability of IAFIS to all users, has increased its capacity for DHS-requested fingerprint searches, and has reduced the response time to DHS requests for checks of aliens' fingerprints.

3. Civil Rights and Civil Liberties – Section 1001 Reports: During the past year, the OIG has completed several reviews that either directly or indirectly examined the impact of FBI activities on civil rights and civil liberties issues.

First, consistent with Section 1001 of the USA PATRIOT Act (Patriot Act), the OIG released to Congress our eighth semiannual report in March 2006 and ninth semiannual report in August 2006 describing the OIG's activities during the prior 6 months related to civil rights and civil liberties complaints.

Both reports summarize investigations and reviews undertaken by the OIG in furtherance of our Section 1001 responsibilities. In addition, the March Section 1001 report described the results of an OIG review of the FBI's

reporting to the President's Intelligence Oversight Board (IOB) of possible intelligence violations. Our report detailed the types and percentages of possible violations reported by the FBI to the IOB in FY 2004 and 2005 and the process used by the FBI to report such violations.

Examples of the possible violations that the FBI reported to the IOB in FYs 2004 and 2005 include FBI agents intercepting communications outside the scope of the order from the Foreign Intelligence Surveillance Act (FISA) Court; FBI agents continuing investigative activities after the authority for the specific activity expired; and third parties providing information that was not requested by an FBI National Security Letter. However, not all violations were attributable solely to FBI conduct. According to the data we reviewed, third parties such as telephone companies were involved in or responsible for the possible violations in approximately one-quarter of the reported matters in both years we examined. The OIG's Section 1001 report also provided detailed information that summarized the percentages of possible violations reported to the IOB, broken down by specific intelligence activity. We intend to continue to review these potential IOB violations and report on our findings in future reports.

4. September 2005 Shooting Incident Involving the FBI and Ojeda Rios: In August 2006, the OIG issued a 171-page report examining the shooting incident involving the FBI and long-time fugitive Filiberto Ojeda Rios, leader of a Puerto Rican pro-independence organization. The FBI Director had requested that the OIG conduct an investigation to determine the facts and circumstances of the Ojeda shooting incident and to make recommendations regarding what actions, if any, the FBI should take in connection with it.

The OIG investigation found that Ojeda opened fire as the FBI approached Ojeda's residence on the afternoon of September 23, 2005, to arrest him on a fugitive warrant. An intense exchange of gunfire ensued, and three FBI agents were shot, with one seriously wounded. A stand-off ensued, and at approximately 6:00 p.m. an FBI agent saw Ojeda through a kitchen window with a gun in his hand. The agent fired three shots at Ojeda, one of which struck him. The FBI did not enter the house until shortly after noon the next day, at which time the agents found Ojeda dead on the floor from a single bullet wound.

The OIG conducted an extensive review of this shooting incident, including interviews of the FBI agents involved, Puerto Rico law enforcement officials, and the Puerto Rico scientists who prepared the forensic reports. We concluded that once Ojeda began firing he posed an imminent danger of death or serious injury to the agents and that the FBI agents did not violate the DOJ Deadly Force Policy by firing at Ojeda, either during the initial gunfire or when the agent saw Ojeda in the window. The report also examined the reasons that

the agents did not enter the residence until more than 18 hours after an agent shot and hit Ojeda. The OIG concluded that the FBI's cautious approach toward entering the residence after Ojeda was shot was motivated by consideration of agent safety, not by any desire to withhold medical treatment from Ojeda or to let him die.

However, the OIG report cited deficiencies in several aspects of the planning and execution of the attempted arrest. For example, the investigation determined that the decision to conduct an emergency daylight assault to arrest Ojeda on September 23 was extremely dangerous and was not the best option available. The OIG concluded that a strategy of surrounding the residence and calling for Ojeda to surrender, with the option of using chemical agents such as tear gas to force Ojeda outside, would have been a safer and more effective strategy. We also found other deficiencies in the FBI's planning and implementation of the operation, including a failure to integrate negotiators into the initial planning.

The OIG report made 10 systemic recommendations intended to improve the planning and conduct of future FBI arrest operations, including assuring the reconsideration of all relevant tactical options when circumstances change and ensuring that negotiators are integrated into tactical planning for operations in which a standoff is a foreseeable contingency.

5. FBI Interviews of Potential Protesters at the 2004 Democratic and Republican National Conventions: In April 2006, the OIG issued a report on the FBI's use of its investigative authorities to conduct interviews of potential protesters in advance of the 2004 Democratic and Republican national political conventions. The OIG initiated this investigation after reports that dozens of people had been interviewed in at least six states, including anti-war demonstrators and political demonstrators and their friends and family members.

The OIG review did not substantiate allegations that the FBI improperly targeted protesters for interviews in an effort to chill the exercise of their First Amendment rights at the conventions. The report concluded that the FBI's interviews of potential convention protesters and other related interviews, together with the FBI's related investigative activities, were conducted for legitimate law enforcement purposes and were based upon a variety of information related to possible bomb threats and other violent criminal activities.

6. Terrorism Screening Center: As discussed in my testimony before this Subcommittee last year, the OIG completed two reviews in 2005 that examined various aspects of the Terrorist Screening Center (TSC), a multi-agency effort to consolidate the federal government's terrorist watch lists and

provide 24-hour, 7-day-a-week responses for screening individuals against the consolidated watch list.

As part of our reviews, the OIG examined the accuracy of the TSC's watchlist database and the TSC process for correcting erroneous entries on the watch list. The OIG concluded that the TSC had not ensured that the information in the database was complete and accurate. For example, the OIG found instances where the consolidated database did not contain names that should have been included on the watch list and found inaccurate or inconsistent information related to persons included in the database.

The OIG's June 2005 report offered 40 recommendations to the TSC to address areas such as database improvements, data accuracy and completeness, call center management, and staffing. Since issuance of that report, we have followed up with the TSC about the progress in responding to our recommendations. The TSC informed us that it has initiated a record-by-record review of the terrorist screening database to help ensure accuracy, completeness, and consistency of the records, focusing first on the records deemed most important. However, according to the TSC, review of the entire database, which contains more than 235,000 records, will take several years.

The OIG continues to monitor this issue and this fall we intend to initiate a follow-up review to assess the TSC's progress in ensuring the accuracy of the TSC databases.

7. The FBI's Handling and Oversight of Counterintelligence Asset Katrina Leung: In May 2006, the OIG issued a report that examined the FBI's handling and oversight of Katrina Leung, one of the FBI's most highly paid counterintelligence assets. Leung and her FBI handler of 18 years, Special Agent James J. Smith, were arrested in April 2003 after an FBI accused Leung of spying for the People's Republic of China against the United States. The FBI's investigation also revealed that Leung and Smith had been involved in an intimate romantic relationship for nearly 20 years. Following the arrests of Smith and Leung, the FBI Director asked the OIG to review any FBI performance and management issues relating to this case.

The OIG review found that Smith had operated Leung with little oversight and that the FBI was aware of serious counterintelligence concerns about Leung that began to surface during the late 1980s but did little to follow up on the warning signals it received. The OIG report concluded that the FBI's inattention to the oversight of Smith and Leung, its willingness to exempt Smith from complying with the rules governing asset handling, and its failure to aggressively question Smith or follow up when red flags arose allowed Leung to deceive the FBI about her activities and permitted Smith to continue his affair with Leung until his retirement in November 2000.

The OIG found that since the discovery of Smith's long-term relationship with Leung, the FBI has taken steps to address deficiencies in its China Program and to improve asset handling and vetting procedures. However, the OIG's report provided 11 recommendations to help address further the systemic issues that enabled Smith and Leung to escape detection and avoid accountability for so long. The OIG recommendations include requiring separate documentation for red flags and other counterintelligence concerns involving assets, requiring alternate case agents to meet with assets on a frequent basis, limiting the time a single agent can handle an asset, and implementing fully the FBI's policy regarding counterintelligence polygraph examinations.

8. FBI's Handling of the Brandon Mayfield Matter: In March 2006, the OIG released a 273-page report that examined the FBI's handling of the Brandon Mayfield case. Mayfield, a Portland, Oregon, attorney, was arrested by the FBI in May 2004 on a material witness warrant after FBI Laboratory examiners concluded that Mayfield's fingerprint matched a fingerprint found on a bag of detonators connected to the March 2004 terrorist attack on commuter trains in Madrid, Spain, which killed almost 200 people and injured more than 1,400 others. However, Mayfield was released 2 weeks later when the Spanish National Police identified an Algerian national as the source of the fingerprint on the bag. The FBI Laboratory subsequently withdrew its fingerprint identification of Mayfield.

We found several factors that caused the FBI's fingerprint misidentification. First, the unusual similarity between Mayfield's fingerprint and the fingerprint found on the bag confused three experienced FBI examiners and a court-appointed expert. However, we also found that FBI examiners committed errors in the examination procedure, and the misidentification could have been prevented through a more rigorous application of several principles of latent fingerprint identification. For example, the examiners allowed their interpretation of the latent fingerprint to be biased by features they saw in Mayfield's known fingerprint, a process known as "circular reasoning." The examiners also overlooked or rationalized several important differences in appearance between the latent print and Mayfield's known fingerprint that should have precluded them from declaring an identification. In addition, the FBI missed an opportunity to catch its error when the Spanish National Police informed the FBI on April 13, 2004, that it had reached a "negative" conclusion with respect to matching the fingerprint on the bag with Mayfield's fingerprints.

Although the OIG determined that Mayfield's religion played no role in the FBI examiners' initial conclusions, we found that by the time the Spanish National Police issued its "negative" conclusion, Laboratory examiners had

become aware of information about Mayfield obtained in the course of the Portland Division's investigation, including the fact that he had acted as an attorney for a convicted terrorist, had contacts with suspected terrorists, and was Muslim. We believe that these factors likely contributed to the examiners' failure to sufficiently reconsider the identification after the Spanish National Police raised legitimate questions about it.

Our report made a series of recommendations to help the FBI address the fingerprint identification issues raised by the Mayfield case. The FBI responded that its Laboratory is planning to adopt new procedures that are consistent with most of our recommendations.

9. The FBI's DNA Laboratory: In May 2006, the OIG issued a report on the FBI's Combined DNA Index System (CODIS), a national DNA-profile matching service containing DNA profiles from crime scenes, convicted offenders, and sources involving missing persons. CODIS allows federal, state, and local crime laboratories to electronically compare over 3 million DNA profiles contributed by DNA laboratories throughout the United States for crime solving and for identification of missing or unidentified persons. While the participating laboratories upload their qualifying forensic profiles into CODIS, the FBI CODIS Unit is responsible for overseeing CODIS operations and ensuring that these activities are conducted appropriately.

We concluded that the FBI has made improvements to several aspects of CODIS operations, has implemented various corrective actions that address previously identified weaknesses, and has received an overall positive evaluation of its administration of CODIS from other federal, state, and local laboratories.

However, we found that the FBI needs to make further improvements to ensure that it properly oversees the CODIS program and participants. Specifically, the FBI has not implemented routine audits of forensic profiles uploaded into CODIS and instead continues to rely on participating laboratories to annually certify that they are in compliance as the primary means of quality control over the data uploaded into the database. We also recommended that the FBI provide training on quality assurance standards, track findings identified in quality assurance audits of state and local participating laboratories, and emphasize providing written rather than verbal guidance to the participating laboratories.

The FBI agreed with most of our recommendations and is in the process of implementing those recommendations.

III. ONGOING OIG REVIEWS IN THE FBI

1. The FBI's Use of Certain Patriot Act Authorities: As required by the *USA Patriot Improvement and Reauthorization Act* of 2005, the OIG is reviewing (1) the FBI's use of National Security Letters to obtain certain categories of records, including telephone toll and transactional records, financial records, and consumer reports; and (2) the FBI's obtaining of business records by applying for ex parte orders issued by the FISA Court pursuant to Section 215 of the Patriot Act.

The Patriot Reauthorization Act directs the OIG to review the extent to which the FBI has used these authorities; any bureaucratic impediments to their use; how effective these authorities have been as investigative tools and in generating intelligence products; how the FBI collects, retains, analyzes, and disseminates information derived from these authorities; whether and how often the FBI provided information derived from these authorities to law enforcement entities for use in criminal proceedings; and whether there has been any improper or illegal use of these authorities.

In this review, the OIG is examining FBI investigative files, interviewing FBI and other DOJ officials, visiting FBI field offices, and analyzing the FBI's use of these authorities in the last several years. According to the Patriot Reauthorization Act, the OIG is required to report the results of its review to Congress by March 2007.

2. Follow-up Review of the FBI's Response to the Robert Hanssen Case: In August 2003, the OIG issued a review of the FBI's performance in detecting, deterring, and investigating the espionage activities of Robert Hanssen, the most damaging spy in FBI history. Our report described long-standing problems with the FBI's internal security efforts that the Hanssen case exposed. Our report made 21 recommendations to the FBI to improve its internal security and its ability to deter and detect espionage in its midst.

The OIG is currently conducting a follow-up review to assess the FBI's progress in implementing the recommendations contained in the OIG report. Our follow-up review is assessing the FBI's response in the following five general areas: 1) improving the FBI's performance in detecting an FBI penetration; 2) improving coordination with the Justice Department; 3) improving source recruitment, security, and handling; 4) improving security; and 5) improving management and administration.

3. FBI Observations of and Reports Regarding Detainee Treatment at Guantanamo Bay and Other Military Facilities: The OIG is examining FBI employees' observations and actions regarding alleged abuse of detainees

at Guantanamo Bay, Abu Ghraib, Afghanistan, and other venues controlled by the U.S. military. The OIG is investigating whether FBI employees participated in any incident of detainee abuse in military facilities at these locations, whether FBI employees witnessed incidents of abuse, how FBI employees reported any observations of abuse, and how those reports were handled. In addition, the OIG is assessing whether the FBI inappropriately retaliated against or took any other inappropriate action against any FBI employee who reported any incident of abuse.

4. The FBI's Investigation of Certain Domestic Advocacy Groups: The OIG recently initiated a review to examine allegations that the FBI targeted domestic advocacy groups for scrutiny based solely upon their exercise of rights guaranteed under the First Amendment of the United States Constitution. The review is examining allegations regarding the FBI's investigation, and the predication for any such investigation, of certain domestic advocacy groups, including the Thomas Merton Center, Greenpeace, and People for the Ethical Treatment of Animals. Our review of the domestic advocacy groups is similar in scope to the OIG's review of the FBI's investigation of potential protesters at the 2004 Democratic and Republican National Conventions.

5. FBI Weapons and Laptops Follow-up. The OIG is conducting a follow-up review of the FBI's controls over its weapons and laptop computers. In a prior OIG audit, issued in 2002, we found that the FBI lacked sufficient internal controls over its inventory of weapons and laptops, as indicated by the FBI's inability to account for 212 missing weapons and 317 missing laptop computers. In that report, we made ten recommendations to help the FBI improve its accountability for this sensitive government property. Our follow-up review is examining the FBI's progress in strengthening its controls over weapons and laptop computers in order to reduce similar losses.

6. Department and FBI Internal Controls over Terrorism Reporting. The Department reports many terrorism-related statistics in its performance plans and statistical reports. The Congress and Department management use these statistics to assess the success of its counterterrorism efforts, to help make operational and funding decisions for Department and FBI counterterrorism activities, and to support the Department's and the FBI's annual budget requests.

Given the importance of these statistics, the OIG initiated an audit to determine if the FBI, the Department's Criminal Division, and the Executive Office for United States Attorneys accurately gather and report terrorism-related statistics. As to the FBI, we are reviewing whether the FBI is accurately reporting statistics in categories such as the number of terrorist convictions,

the number of intelligence reports issued, and the number of terrorism-related threats tracked.

7. FBI Intelligence Analysts. The OIG issued a report in May 2005 examining the FBI's efforts to hire, train, and retain intelligence analysts. Our report concluded that while the FBI had made progress in hiring and training intelligence analysts, the FBI needed to make further improvements in this area. Our review found that the FBI had fallen short of its hiring goals, had not developed a quality training curriculum for new analysts, and was often using its intelligence analysts to perform administrative or non-analytical tasks rather than to perform the analytical tasks for which they were hired. The OIG report made 15 recommendations to help the FBI improve its efforts to hire, train, and retain intelligence analysts. We currently are conducting a follow-up audit to examine the progress made by the FBI in these areas.

IV. CONCLUSION

The FBI has made progress in transforming itself after the September 11 attacks, but it still has substantial work to do. With regard to its Sentinel project, we are finding that the FBI has put in place management systems that, if implemented, will help the success of the project, and the FBI has addressed most of the initial concerns that we found in our prior review of Sentinel. However, the Sentinel project is in its early stages, and the FBI must ensure that it follows its IT investment management processes to keep Sentinel on track and within budget.

In other areas, such as its counterterrorism efforts, the interoperability of fingerprint identification systems, civil rights and civil liberties issues, internal security issues, and the FBI laboratory, the OIG will continue to monitor the FBI's progress. The FBI continues to face significant challenges in these and other critical areas, and the OIG will continue to do our part by performing thorough reviews of FBI programs and operations.