NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

First public hearing of the National Commission on Terrorist Attacks Upon the United States

Statement of Glenn A. Fine to the National Commission on Terrorist Attacks Upon the United States
April 1, 2003

Mr. Chairman, Mr. Vice Chairman, and Members of the National Commission:

Thank you for inviting me to appear before the National Commission to discuss the work of the Department of Justice Office of the Inspector General (OIG). Both before and after the September 11 terrorist attacks, the OIG has focused much of its attention on border security and other national security issues in Department of Justice programs and operations.

You have asked me to focus my testimony today on the work of the OIG as it relates to border security issues. My testimony will primarily address these issues, although I will mention

Current News

The Commission has released its final report. [more]

The Chair and Vice Chair have released a statement regarding the Commission's closing. [more]

The Commission closed August 21, 2004. [more]

Commission Members

Thomas H. Kean
Chair

Lee H. Hamilton
Vice Chair

briefly several other OIG reviews that examine other national security issues that are relevant to the National Commission as it conducts its critically important task.

In my testimony, I address three topics. First, I describe the findings of a series of OIG reviews regarding border security and related immigration issues. These reviews examined the operations of the Immigration and Naturalization Service (INS), which had responsibility for immigration and border security issues until March 1, 2003, when its functions were transferred into the new Department of Homeland Security (DHS). Our reviews, both before and after September 11, 2001, highlighted a series of weaknesses in INS programs that affected border security.

Second, I will briefly mention three OIG reviews in the Federal Bureau of Investigation (FBI) that relate to the National Commission's work.

Third, in my conclusion, I will offer several suggestions about issues related to border security that the National Commission may want to examine as it conducts its inquiry in the months ahead.

At the outset of my remarks, however, I want to stress that while the OIG has noted serious deficiencies in INS operations and systems as they relate to border security issues, this should in no way diminish the important work of thousands of INS employees (now DHS employees) over the years. These employees perform diligently, under very difficult circumstances, and their mission is critical to the security of our country. Yet, as this statement will discuss, our reviews of INS programs revealed significant problems that left gaps in the INS's attempts to secure the nation's borders. I will now discuss the findings of several of those reviews.

I. OIG REVIEWS RELATED TO BORDER SECURITY ISSUES

A. The INS's Contacts with Two September 11 Terrorists

In May 2002, the OIG released a 188-page report that examined how the INS mailed forms notifying a Florida flight school that two September 11 terrorists - Mohamed Atta and Marwan Alshehhi - had received approval to change their immigration status from "visitors" to "students" six months after they died committing the terrorist attacks. The mailing of these forms raised questions about the INS's handling of change of status applications. Our review also examined how the two terrorists were admitted into the United States three separate times each in 2000 and 2001. This incident also raised serious concerns about the INS's monitoring and tracking of foreign students in the United States.

With regard to Atta's and Alshehhi's entries into the United States, the evidence did not show that the INS inspectors who admitted them violated INS policies and practices. Atta and Alshehhi each entered the United States three times at separate airports. They had valid passports and visitor visas that were good for multiple entries.

Yet, Atta's and Alshehhi's admissions highlighted that INS inspectors lacked important information when assessing aliens' eligibility for admission into the United States. For example, although both Atta and Alshehhi had completed their flight training by the time they sought to re-enter the country in January 2001, the inspectors who admitted them were not aware of that fact, since the INS did not collect this information about foreign students.

Our review of Atta's and Alshehhi's admissions also illustrated another troubling INS practice.

We were consistently told by INS inspectors at the ports of entry (POEs) we visited that aliens who intended to enter the United States to become full-time students and who lacked the required student visas likely would have been admitted through a waiver process. Although Atta and Alshehhi were not admitted through the waiver process, we found that INS managers, supervisors, and inspectors believed incorrectly that they had broad discretion under the waiver process to admit aliens who lacked the required passports and visas. In fact, the law and INS policy limited the circumstances in which an alien who lacks the proper passport or visa can be admitted with a waiver to "unforeseen emergencies." But the INS's prevailing philosophy in dealing with foreign students at the POEs before September 11 was that students were not a concern or a significant risk worthy of special scrutiny. Therefore, INS inspectors and supervisors would admit students when they appeared at POEs without the proper documentation if they did not appear to have a criminal record or showed no other signs of inadmissibility. Thus, although the INS had clear policies on when such a waiver was appropriate, we found that those policies were not followed or enforced consistently.

Second, we analyzed the INS's adjudication of Atta's and Alshehhi's change of status applications and its notification to the flight school that the applications had been approved. We found that process to be untimely and significantly flawed. The INS took more than 10 months to adjudicate the applications. As a result, Atta's and Alshehhi's applications were not adjudicated until well after they had finished their flight training course at the Florida flight school. In addition, the INS adjudicator who approved their applications did so without adequate information, including the fact that Atta and Alshehhi had left the country two times after filing their applications, which meant they had abandoned their request for a change of status. And even after the INS took 10 months

to approve the applications, the notification forms were not sent to the Florida flight school for an additional 7 months because the INS failed to adequately supervise a contractor who processed the documents.

Atta's and Alshehhi's cases highlighted important weaknesses in the INS's handling of foreign students. Historically, the INS devoted insufficient attention to monitoring foreign students, and its former paper-based tracking system was inefficient, inaccurate, and unreliable. The new Internet-based foreign student tracking system - the Student and Exchange Visitor Information System, or SEVIS - has the potential to dramatically improve the monitoring of foreign students. But we concluded that it would not solve all the problems in the federal government's efforts to monitor foreign students studying in the United States.

We concluded that unless the INS devoted sufficient resources and effort to implementing and using SEVIS effectively, many problems would continue to exist. Among other things, we recommended that the INS ensure that it fully reviews the schools certified to enroll foreign students, make certain that accurate and timely information is entered into SEVIS, provide and enforce clear guidance for INS officers and schools about their responsibilities and the procedures related to foreign students, require that school officials and INS employees are trained properly on these requirements and procedures, and ensure that information in SEVIS about schools and students is used effectively to detect and deter fraud in the system.

B. SEVIS Follow-up Review

In March 2003, the OIG completed a follow-up review to assess the INS's progress in implementing the SEVIS system. We found that the INS had made progress implementing

SEVIS, including requiring previously approved schools to reapply for certification and requiring non-accredited vocational, language, and flight schools to undergo on-site reviews prior to providing them access to SEVIS. However, despite this progress, the OIG report found that SEVIS is not yet fully implemented and that significant deficiencies in its implementation remain. Specifically, this OIG's March 2003 follow-up review found:

- The INS's oversight and training of contractors hired to conduct on-site reviews was inadequate, which resulted in the contractor's checklists being of limited use to INS field adjudicators in determining whether a school was bona fide.
- The INS's review of schools' record keeping and internal controls is insufficient to ensure that schools are complying with SEVIS record keeping requirements or to identify internal control weaknesses that could allow fraud to occur undetected.
- The SEVIS database will not include information on all foreign students until August 1, 2003. The INS required that schools begin using SEVIS for newly enrolled foreign students by January 30, 2003 - a deadline it later extended to February 15, 2003. However, schools have until August 1, 2003, to enter the data for their continuing foreign students into the SEVIS database. Therefore, SEVIS will not include information on all foreign students until August 1, 2003.
- The INS has not established procedures to use SEVIS to identify and refer potential fraud for enforcement action.

The OIG review also concluded that transfer of the INS to the DHS created a significant management challenge for DHS officials. Without close oversight to ensure continuity and a smooth transition, full SEVIS implementation

may be further delayed. We identified eight actions the DHS should take to ensure the transition and effectiveness of the program for monitoring foreign students in the United States.

C. Efforts to Control the Northern Border

Over the last several years, the OIG has conducted a series of reviews on immigration issues that impact border security. For example, we have examined the INS's efforts to prevent illegal immigration across the northern border. Until recently, the INS devoted significant efforts to deterring illegal immigration along the southwest border, but it did not focus such attention on the 4,000 miles of northern border between the United States and Canada.

In February 2000, the OIG issued an inspection report that systematically examined the Border Patrol's operations along the northern border. We found that, as of September 1999, only 4 percent of the national total of 8,364 Border Patrol agents (311 agents) was assigned to northern border sectors. By contrast, the Border Patrol deployed 92 percent of the total (7,706 agents) to its 9 southwest Border Patrol sectors. The remaining 347 agents were assigned to the coastal sectors, headquarters, INS regional offices, and the Border Patrol Academy.

The OIG review reported an increase in illegal activity along the northern border, including an increase in alien and drug smuggling. We concluded that the level of illegal activity clearly exceeded the Border Patrol's capacity to respond. We also found that other factors, such as the detailing of agents from the northern to the southwest border and the lack of detention space to house apprehended aliens, further diluted the Border Patrol's enforcement capabilities along the northern border. We concluded that the number of agents assigned could not adequately patrol the entire length of the northern border. For example, we found that

shifts with no Border Patrol coverage left the northern border unguarded. The Border Patrol realized this risk but, because of the low numbers of agents assigned to northern border sectors, it said it could not cover all shifts 24 hours a day, 7 days a week.

The Border Patrol uses what it calls "force-multipliers," such as cameras, sensors, and other technology, to aid its surveillance of the border and interdiction activities, but we found that northern border sectors did not have adequate amounts of this equipment. For example, at the time of our inspection, one northern border sector had identified 65 smuggling corridors along the more than 300 miles of border within its area of responsibility, but the sector had only 36 sensors with which to monitor these corridors.

Our review recommended that the INS outline the approach the Border Patrol would take to secure the northern border, including determining the minimum number of Border Patrol agents required to address existing gaps in coverage, determining the amount of intelligence resources needed to more accurately assess the level of illegal activity, and identifying and implementing accurate data collection methods to support decisions about personnel and equipment.

In February 2002, we issued a follow-up review that found the INS had made some improvements to enhance border security. However, we found that many Border Patrol stations still were not staffed 24 hours a day, 7 days a week. We concluded that increased staffing and resources for the northern border continued to be a critical priority to help control illegal immigration and enhance national security.

D. Nonimmigrant Overstays

The INS estimates the number of illegal aliens in the United States at 7 to 8 million. Others estimate the number to be even higher. Many of these aliens entered the United States illegally by crossing land borders between the United States and Mexico or Canada. However, the INS believes that approximately 40 to 50 percent of the illegal alien population entered the United States legally as temporary visitors who simply failed to depart when required. These illegal aliens are referred to as "nonimmigrant overstays." More than 90 percent of overstays are tourists or business visitors, but overstays also include students and temporary workers.

The OIG found that the principal INS record-keeping system for tracking nonimmigrant overstays, the Nonimmigrant Information System (NIIS), did not produce reliable data either in the aggregate or on individual aliens. Normally, aliens arriving in the United States at airports fill out an I-94 form and present it to the INS inspector. The immigration inspector collects the arrival portion of the form and returns the departure portion to the passenger. The arrival portion is sent to an INS contractor who inputs the information into NIIS. When the alien leaves the United States, the airlines are supposed to collect the departure portion of the I-94 form and provide it to the INS for entry into NIIS. The data is then matched by NIIS to identify nonimmigrant overstays.

However, our review found that NIIS data was incomplete and unreliable due to missing departure records and errors in processing of the records. NIIS also did not contain departure records for a large number of aliens, most of whom the INS assumed had left the United States. Unrecorded departures result because airlines failed to collect departure forms, aliens departed through land rather than air ports of entry, data entry errors, records were lost through electronic transmission or tape-loading problems, or the NIIS system failed to match arrival and departure records. As a result, the

INS could not identify with reasonable certainty many aliens who remained in the country beyond the period authorized.

E. The INS's Automated I-94 System

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 directed the Department of Justice to develop an automated entry and exit control system that would replace the manual system of collecting I-94 cards from aliens who enter the country. The system was supposed to enable the INS, through on-line searching procedures, to identify lawfully admitted nonimmigrants who remain in the country.

In response to this congressional requirement, the INS introduced a pilot system to automate the processing of air passenger I-94 forms. The automated I-94 system attempted to capture arrival and departure data electronically and upload data to the NIIS system.

In August 2001, the OIG completed an audit of the design and implementation of the automated I-94 system and found that the INS had not properly managed the project. We found that, despite having spent $31.2 million on the system from fiscal year (FY) 1996 to FY 2000, the INS: (1) did not have clear evidence that the system met its intended goals; (2) had won the cooperation of only two airlines; (3) was operating the system at only a few airports; and (4) was in the process of modifying the system. INS officials estimated that an additional $57 million would be needed from FY 2001 through FY 2005 to complete the system. These projections included development, equipment, and operation and maintenance costs.

As a result of our concerns, we made a series of recommendations to help ensure that the INS rigorously analyzed the costs, benefits, risks,

and performance measures of the automated I-94 system before proceeding with further expenditures. Subsequent to our audit, the INS decided that resources should be devoted to developing an entry-exit system required by the USA PATRIOT Act, and it terminated its automated I-94 system. The INS, and now the DHS, is working with other federal agencies to implement another automated entry and exit control system, called the National Security Entry-Exit Registration System (NSEERS).

F. Final Orders of Removal

When aliens enter or remain in this country illegally, the INS has enormous difficulty apprehending and removing them from the United States. For example, we found that even in cases where aliens had been ordered removed, the INS had difficulty ensuring that the aliens actually left the country. As of June 2002, the INS estimated that approximately 355,000 nondetained aliens with final removal orders had failed to leave the country as required.

In 1996, the OIG issued an inspection report that assessed efforts by the INS to ensure that aliens ordered removed from the United States actually leave the country. The OIG found that while the INS removed almost 94 percent of detained aliens with final removal orders, it removed only 11 percent of nondetained aliens with final removal orders.

In a follow-up report issued in February 2003, the OIG found that the INS had not made much progress in this area. Our review found that while the INS removed 92 percent of detained aliens with final removal orders, it removed only 13 percent of nondetained aliens. In addition, we found that the INS failed to take or complete corrective actions in a timely manner that it agreed to implement in response to our 1996 report. Moreover, we found that the INS continued to be ineffective at removing potential

high-risk groups of nondetained aliens:

- The INS removed only 6 percent of nondetained aliens with final orders from countries identified by the U.S. Department of State as sponsors of terrorism (i.e., Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria). In a 15-month period ending in December 2001, 894 of the 2,334 aliens from these countries that were ordered removed were not detained. We examined 470 of these cases and found that the INS removed only 6 percent of the aliens.
- Although the INS cited removing criminal aliens as its top priority, we found that it removed only 35 percent of nondetained aliens with criminal records; and
- The INS removed only 3 percent of the nondetained aliens denied asylum and issued final removal orders. The OIG concluded that the INS's low removal rate for asylum seekers is a cause for concern because this group may include potential terrorists who threaten our national security. The OIG report describes several aliens convicted of terrorist acts in the United States who had requested asylum as part of their efforts to remain in this country.

G. Institutional Removal Program

A September 2002 OIG report assessed the Institutional Removal Program (IRP), an INS program designed to identify deportable criminal aliens incarcerated in federal, state, and local correctional facilities and remove them from the United States upon completion of their sentence. Our review determined that the INS did not manage the IRP process effectively. We found that the INS had not determined the nationwide population of foreign-born inmates, particularly at the county level. Without this information, the INS could not quantify the resources it needs to fully identify and process

all deportable inmates. In addition, we found that at the county jail level IRP interviews of foreign-born inmates to determine deportability were minimal to non-existent. As a result, many potentially deportable foreign-born inmates passed through county jails virtually undetected. We found instances where inmates not identified by the INS as potentially deportable went on to commit additional crimes after being released into the community. Further, our review found that the INS did not always timely process IRP cases. As a result, it has been forced to detain in INS custody criminal aliens released from state and local correctional facilities - after they have served their sentence - until deportation proceedings can be completed.

H. Visa Waiver Program

The Immigration Reform and Control Act of 1986 created the Visa Waiver Pilot Program, which permitted citizens from certain countries to enter the United States as visitors without first obtaining visas. In October 2000, Congress made the Visa Waiver Program (VWP) permanent. Currently, visa requirements are waived for citizens of 28 countries who want to visit the United States for business or pleasure.

In 1999, the OIG examined the INS's efforts to minimize illegal immigration and security threats posed by abuse of the VWP. Because visitors traveling for business or pleasure under the program are not required to obtain visas, they are not screened in any way prior to their arrival at U.S. ports of entry. Instead, VWP visitors present their passports to INS inspectors on arrival. The inspectors observe the applicants, examine their passports, and conduct checks against a computerized lookout system to decide whether to allow them entry into the United States. This review by INS inspectors is the principal means of preventing illegal entry. INS inspectors had, on average, less than one minute to check and decide on each applicant.

Our 1999 review found that INS inspectors did not query all VWP passport numbers against the INS's computerized lookout system. In addition, our review noted that terrorists, criminals, and alien smugglers have attempted to gain entry into the United States through the VWP. INS inspectors told the OIG that terrorists and criminals believed they would receive less scrutiny during the inspection process if they applied under the VWP and consequently would have a greater chance of entering the United States without being intercepted. In addition, several of these terrorists and criminals had criminal records that would have prevented them from obtaining a visa if they were required to apply for one.

In addition, we found that the theft of passports from VWP countries was a serious problem. Because these stolen passports are genuine documents, their fraudulent use is difficult for immigration inspectors to detect. During our review, we tested a sample of 1,067 passports stolen from VWP countries and found that almost 10 percent may have been used to successfully enter the United States.

We also identified problems with the way the INS maintained its lookout system, including its failure to enter information about stolen VWP passports into the lookout database in a timely or accurate manner. As a result, 567 stolen passports in our sample of 1,067 (53 percent) had no lookout record in the INS system. Of the 500 passport numbers that had lookout records, 112 (22 percent) were not entered accurately. This missing or inaccurate information reduced the effectiveness of the lookout system and increased the possibility that inadmissible VWP applicants could enter the United States.

In December 2001, we issued a follow-up report on the VWP program. We found that while the INS had distributed guidance to improve the collection and dissemination of information about missing VWP passports, it did not take

appropriate measures to ensure the guidance was followed at ports of entry. Therefore, the INS did not have a mechanism to provide systematic, consistent, and timely information about missing VWP passports to its immigration inspectors. We concluded that the failure to make this information available to INS immigration inspectors could contribute to the admission into the United States of criminal aliens or terrorists fraudulently using passports from VWP countries. We urged the INS to reissue the guidance and to take aggressive follow-up actions to ensure that inspectors follow the guidance.

I. Passenger Inspections at Airports

1. Primary Inspections

Typically, immigration inspections at air ports of entry (POEs) consist of a primary inspection and, when required, a secondary inspection. These inspections are important to protect the nation from terrorists, persons attempting to enter the country illegally, alien smugglers, and other illegal activities. In FY 2002, the INS inspected almost 70 million air travelers at more than 220 airports designated as POEs around the United States and in foreign countries where travelers are inspected prior to arrival in the United States.

In a review issued in February 2003, we evaluated the INS's procedures for inspecting visitors at air POEs, including critical associated functions relating to analyses of advance passenger information, availability of needed law enforcement information, and inspector training. We found that the capability of INS staff at air POEs to analyze advance passenger information to identify high-risk and inadmissible persons was limited due to the lack of adequate resources. Additionally, the INS's lookout system did not always provide primary inspectors information known to the INS that

could enable them to identify high-risk and inadmissible persons, such as lookouts for stolen passports. We also found that the INS needed to improve its capability to timely disseminate classified intelligence information to air POEs. Without mechanisms to ensure the timely availability of needed law enforcement information, we concluded that the INS increases the risk that persons known to be inadmissible will be allowed to enter the United States.

We also found that primary inspectors were not always querying lookout databases as required, and controls were not sufficient to ensure that all primary inspectors and supervisors could access backup information systems in the event of system outages.

Finally, we found that the INS invested more than $19 million in FY 2002 to provide basic training to approximately 1,000 new inspectors at its Immigration Officer Academy, yet training was not sufficient in 2 important areas - on the use of the computer systems that provide lookouts and other critical information, and on terrorism awareness. We concluded that the fact that approximately 26 percent of all inspectors at air, land, and sea POEs were newly hired in FY 2002 only increased the need to implement an aggressive and complete inspector training program.

2. Security at Airport Facilities

An OIG audit issued in December 2000 found deficiencies in INS inspection facilities at 42 international airports in the United States. We found that airports were vulnerable to illegal entry, escapes, injuries, and the smuggling of aliens and contraband. The OIG recommended that the INS correct the deficiencies and improve the condition of the airport inspection facilities. The OIG recently re-examined this issue because of the severity and number of deficiencies found during the prior audit, the

INS's difficulty in taking effective corrective action, and the increased importance of airport security after September 11, 2001.

In the follow-up review issued in January 2003, we found that the INS took insufficient action to implement the OIG's recommendations from our prior audit. The INS had failed to advise many of the airports and airport authorities of needed improvements or even to notify its own airport staff of the prior audit results. Thus, all 12 airports reviewed in this follow-up audit had repeat deficiencies. In addition, the INS failed to apply sanctions successfully against airlines that did not provide suitable inspection facilities.

In addition to the INS's failure to correct previously identified problems, the OIG review identified new deficiencies, such as secondary inspection areas that did not have adequate camera coverage, interview rooms that did not have a system to videotape interviews, and lack of camera coverage for all gates leading into and out of the airport in-transit lounges. Furthermore, the OIG found ineffective security systems and equipment in the airport inspections area, including inoperable alarms and cameras, and security features that had been turned off, were not monitored, or had not been installed. The OIG concluded that the underlying causes for these deficiencies were rooted in perceptions held by INS officials who did not consider airport security a primary responsibility of the INS.

3. Transit Without Visa Program

The Transit Without Visa Program (TWOV) allows certain nonimmigrants to transit through the United States en route to a destination in another country. Visa requirements are waived for eligible nonimmigrants in TWOV status and the aliens can remain in the United States for up to eight hours awaiting departure on connecting flights to their final destinations. In a 1993

report and a December 2001 follow-up review, we found the INS had not taken adequate measures to improve airlines' supervision of TWOV passengers and could not verify departure of TWOV passengers. We concluded that the TWOV program continued to offer an avenue for aliens to enter the United States illegally.

J. INS Management of Information Technology

One of the key themes in many of our reviews is the importance of information technology systems to provide needed information to the immigration inspectors and agents who enforce the immigration laws. Our reviews of INS programs and their associated information technology systems have revealed significant problems that left gaps in the INS's attempts to secure the nation's borders. Over the past decade, many OIG reviews of INS programs have questioned the reliability of the INS's automated information systems and the accuracy of the data produced by those systems. For example, we found separate automated systems planned for almost every function in the INS, but many of these systems did not "talk" to one another and therefore could not be used to meet other important agency missions.

According to Department of Justice estimates, the INS spent more than $290 million on automated systems in FY 2001 and more than $260 million in FY 2000. However, OIG reviews of the INS's management of its automation initiatives found lengthy delays in completing many of these automation programs, unnecessary cost increases, and significant risk that finished projects failed to meet the agency's needs.

We identified three causes for these problems based on our reviews. First, INS managers did not have adequate knowledge of their automation projects. The INS even had

substantial difficulty providing us with a complete list of all its automation projects. Second, project information needed for effective management and decision-making was not readily available. Third, INS managers did not develop, document, or implement basic management control processes necessary to ensure that projects would be completed on schedule and meet performance and functional requirements. Furthermore, we found that the INS did not implement adequate safeguards to ensure the accuracy of existing data that would be used by systems being developed or re-engineered. As a result, new or existing INS systems could contain inaccurate or unreliable data.

Without adequate information technology systems, the INS cannot perform its mission effectively. As we describe in the next two sections, which discuss the INS's automated fingerprint identification systems, the failure to implement and train employees on information systems can have tragic consequences.

K. Automated Fingerprint Identification System (IDENT)

In 1989, the INS began developing an automated biometric identification system to identify quickly individuals who are apprehended or come into contact with the INS. Biometrics are biological measurements unique to each person, such as fingerprints, hand geometry, facial patterns, retinal patterns, or other characteristics that are used to identify individuals. Fingerprints are the most common biometric used by law enforcement agencies. Historically, without a biometric system the INS had to rely upon the names provided by aliens who were apprehended when checking against its databases or other records. But aliens often used false names or different names during different apprehensions. Also, many have similar names, and spelling errors can result in problems identifying individuals accurately.

After several studies, in 1994 the INS began implementing the Automated Fingerprint Identification System, called IDENT. IDENT was first deployed in the San Diego Border Patrol Sector and subsequently throughout the southwest border. IDENT workstations consist of a personal computer, camera, and a single-fingerprint scanner. During enrollment of individuals into IDENT, INS agents scan an individual's two fingerprints, take the individual's photograph, and enter basic apprehension information about the individual into the automated system. When this information is saved, IDENT matches the fingerprints of the individual against the corresponding fingerprints of all individuals in two central IDENT databases, the lookout database and the recidivist database.

In the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, Congress directed the INS to expand the use of IDENT to "apply to illegal or criminal aliens apprehended Nationwide." INS officials envisioned that most of its programs and operations would benefit from the IDENT system through its quick identification of individuals and its ability to obtain information about them from previous encounters with the INS, including any criminal history.

In 1998, the OIG evaluated the INS's implementation of IDENT and found that the INS was enrolling less than two-thirds of the aliens apprehended along the U.S.-Mexico border into the IDENT system. In addition, the INS was entering the fingerprints in the IDENT lookout database of only 41 percent of the aliens deported and excluded in FY 1996; of these, only 24 percent had accompanying photographs even though the INS relies on photographs to confirm identification. We found virtually no controls in place to ensure the quality of data entered into the IDENT lookout database. As a result, we found duplicate

records and invalid data. We also raised concerns that the INS had not provided sufficient training to its employees on the use of IDENT. These failures hampered the INS's ability to make consistent and effective use of IDENT.

L. The Resendez-Ramirez Case

In March 2000, the OIG issued another report that implicated the IDENT system in tragic circumstances. The OIG examined how the INS handled its encounters with Rafael Resendez-Ramirez (Resendez), a Mexican national accused of committing several murders in the United States. Resendez was known as "the railway killer" because he allegedly traveled around the United States by freight train and committed murders near railroad lines. In early 1999, Texas police obtained a warrant for Resendez's arrest in connection with a brutal murder in Houston, Texas. The police mounted an extensive search to find Resendez and contacted several INS investigators in Houston seeking assistance in the search for him. However, none of those INS investigators placed a lookout notice for Resendez in IDENT. Instead, the INS investigators referred the police to other agencies or databases.

Consequently, when Border Patrol agents apprehended Resendez on June 1, 1999, as he attempted to illegally cross the border into New Mexico, nothing in IDENT alerted them to the fact that Resendez was wanted for murder or had an extensive criminal record. As a result, the Border Patrol followed its standard policy and voluntarily returned Resendez to Mexico. He returned illegally to the United States within days of his release and murdered several more people before surrendering on July 13, 1999.

The OIG review concluded that the failings by the INS employees who did not place a lookout for Resendez in IDENT were indicative of and partly caused by larger failings in the INS's

design and implementation of IDENT. We found that the training that was given to INS employees on IDENT, particularly outside the Border Patrol, was ineffective or non-existent. In the 1998 OIG report, we had noted problems with IDENT training and recommended that the INS develop and implement a strategy for sufficiently training INS personnel using IDENT. Unfortunately, the INS largely rejected this recommendation, claiming that its IDENT training was adequate. We found in the Resendez review that INS program offices, such as Investigations and Intelligence, viewed IDENT as a Border Patrol initiative and were not educated on how IDENT could be useful to their mission.

When we interviewed INS employees in various offices involved with the Resendez case, we found that their knowledge of IDENT was severely lacking. The INS investigators who were contacted by police searching for Resendez did not think of IDENT, even when they were asked to place a lookout in INS databases for Resendez. Although the INS had distributed an IDENT lookout policy, it provided no training on the policy and did little to ensure that the policy was understood or read.

This review found that IDENT still was not linked with FBI databases. The INS's IDENT system, the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and the National Crime Information Center (NCIC) 2000 system were developed separately and along different time lines. Initially, each agency focused on meeting its own requirements and did not pursue integration. As a result, when the FBI finally deployed IAFIS and NCIC 2000 in July 1999, the FBI fingerprint systems were not linked to IDENT.

The Resendez case vividly illustrated the need for integration of the INS and FBI systems and spurred the FBI and the INS to develop an integration plan. In December 2001, we

reviewed the status of efforts to integrate IDENT and IAFIS. The primary finding of our follow-up review, similar to our prior reports' conclusions, was that the Department of Justice had moved slowly toward integrating the two fingerprint systems. We recommended that the Department of Justice continue to seek linkage of the FBI and INS biometric identification systems and continue to use IDENT while this integration is proceeding.

To continue our monitoring of the integration of IDENT and IAFIS, we initiated another follow-up review in December 2002 to assess the progress made over the past year. We expect to complete that review shortly.

II. Other OIG Reviews

The OIG has recently completed or is currently working on several important reviews in the FBI that, while not related directly to the border security issues I have been asked to address, squarely relate to the National Commission's work. I will briefly mention three of these reviews.

A. The FBI's Handling of Intelligence Issues Related to the September 11 Attacks

At the request of FBI Director Mueller, in June 2002 the OIG initiated a review to examine aspects of the FBI's handling of information and intelligence prior to the September 11 terrorist attacks. The investigation is focusing on, among other things, how the FBI handled an electronic communication written by its Phoenix Division in July 2001 regarding Islamic extremists attending civil aviation schools in Arizona (known as the "Phoenix EC"), the FBI's handling of the Moussaoui investigation, and other issues related to the FBI's handling of information or intelligence before September 11 that might relate to the terrorist attacks. The OIG has conducted many interviews of FBI and

Department of Justice employees related to these issues, and we are continuing to move forward with this important investigation. We intend to cooperate fully with the National Commission's review of these subjects.

B. The FBI's Counterterrorism Program

In September 2002, the OIG completed an audit examining several aspects of the FBI's counterterrorism program, including: (1) the FBI's progress toward developing a national-level risk assessment of the terrorist threat to the United States; (2) whether the FBI's strategic planning process provides a sound basis to identify counterterrorism requirements; and (3) the amount of resources dedicated to the FBI's counterterrorism program over the last seven years. Among other findings, the OIG audit determined that the FBI had never performed a formal, comprehensive assessment of the risk of the terrorist threat facing the United States, despite its representation to Congress in 1999 that it would. We concluded that such an assessment would have been useful not only to define the nature, likelihood, and severity of the threat, but also to identify intelligence gaps that needed to be addressed.

The OIG made 14 recommendations to the FBI to improve its management of its counterterrorism program, including recommendations that it prepare an authoritative, national-level threat and risk assessment of terrorism with a predictive and strategic view, including the potential use of weapons of mass destruction; identify the chemical and biological agents most likely to be used in a terrorist attack and fully assess the threat and risk of terrorists' use of all types of weapons of mass destruction; develop criteria for evaluating and prioritizing incoming threat information for analysis, and establish a protocol to guide the distribution of threat information; and establish a time goal and a process for building a corps of professional, trained, and

experienced intelligence analysts for assessing and reporting on threats at both the strategic and tactical levels. The OIG's full 131-page audit report is classified at the "secret" level, but we released publicly an unclassified executive summary of our findings.

C. FBI Information Technology

OIG reviews over the years have identified serious deficiencies in the FBI's information technology systems. In December 2002, the OIG completed an audit of the FBI's management of its information technology projects and found that the FBI has failed to fully implement a series of critical management processes. Specifically, the audit found that the FBI: (1) did not have fully functioning information technology investment boards that are engaged in all phases of IT investment management; (2) had not followed a disciplined process of tracking and overseeing each project's cost and schedule milestones; (3) had failed to document a complete inventory of existing information technology systems and projects, and did not consistently identify the business needs for each information technology project; and (4) did not have a fully established process for selecting new information technology project proposals that considered both existing information technology projects and new projects. FBI officials told the OIG that prior to March 2002, individual FBI divisions determined their information technology needs in a "stovepipe" without knowledge of the business needs and priorities of the FBI as a whole.

The audit found that because the FBI had not fully implemented the critical processes associated with effective information technology investment management, it spent millions of dollars on information technology projects without adequate assurance that these projects would meet their intended goals.

The OIG found that since March 2002, when the FBI began pilot testing a new investment management process, it has made measurable progress towards implementing key practices necessary for an effective management system, especially in the area of selecting new information technology projects. At the beginning of this audit in January 2002, the FBI was executing only 4 of the 38 required "key practices" for building an IT investment foundation. By June 2002, the FBI was executing 14 of the 38 key practices.

III. CONCLUSIONS

Based on the significant body of work conducted by the OIG during the last several years, I believe the National Commission could examine several broad areas relating to border security and immigration issues in more detail.

First, information sharing among all levels of government remains a critical component of any effort to prevent terrorist attacks in the United States. At the federal level, the challenge of sharing information in a timely manner has been heightened with the transfer of immigration and border security responsibilities from the Department of Justice to the newly-created DHS. Without adequate information and intelligence, the ability of front-line employees to screen effectively those who seek to enter the country is limited. In this regard, our reviews have found that the INS's track record of implementing information technology systems is not encouraging.

Second, the country faces a significant challenge in creating an effective immigration screening mechanism while not unduly hindering the free flow of travelers and commerce into this country. We must also consider ways to speed the flow of low-risk, pre-screened border crossers without compromising border security.

Third, the current systems for identifying when aliens enter and leave the country are clearly inadequate and in need of improvement. Implementing an effective tracking system for aliens is a daunting challenge and will require substantial efforts and a large investment of resources. Moreover, we believe the federal government needs to step up its efforts to create an effective enforcement program for identifying and removing aliens, particularly those who pose a threat to this country.

At the same time, we cannot ignore the important immigration benefit-related responsibilities that are a core part of the DHS's immigration functions. The DHS processes approximately 50 types of applications, ranging from applications for employment authorization, to change of status to permanent residence, to asylum and citizenship. Processing the millions of applications in a timely and consistent fashion has been a longstanding challenge for the INS, and now for the DHS. We believe that an enhanced focus on border security must not override these important service-related responsibilities.

Fourth, we encourage the National Commission to focus on the important but often overlooked issue of human capital. To fulfill its mission, the DHS must have a sufficient number of trained immigration staff and supervisors. Historically, we have found this to be a critical challenge for the INS. For example, the INS has had difficulty filling Border Patrol agent positions because of attrition rates among agents, delays in recruitment, and limitations in its training facilities. Like other parts of the federal government, the INS also has suffered from difficulties in attracting and retaining employees in information technology and computer security positions. In addition, past OIG reviews found the INS heavily relied on contractor support for many mission-critical functions such as information systems, records management, immigration service processing, and detention

services, among others. The National Commission may want to examine these and other human capital issues as it conducts its work.

Fifth, the transfer of the INS to the DHS presents enormous management challenges. This transfer will not, in itself, resolve any of the issues I have identified here today. Solutions to border security and immigration issues will continue to require creativity, innovation, and aggressive management oversight. We encourage the National Commission to review this transfer to ensure that the DHS's essential border protection and immigration benefits functions are not negatively affected in the short run.

In sum, I believe that these border security issues identified today present many potential areas for the National Commission to examine and provide recommendations for improvement. Thank you for inviting me to testify about these issues, and I would be pleased to answer any questions.

Glenn A. Fine was confirmed by the United States Senate as the Inspector General of the Department of Justice on December 15, 2000.

Mr. Fine has worked for the Department of Justice Office of the Inspector General (OIG) since January 1995. Initially, he was Special Counsel to the Inspector General. In 1996, he became the Director of the OIG's Special Investigations and Review Unit.

Before joining the OIG, Mr. Fine was an attorney specializing in labor and employment law at a law firm in Washington, D.C. Prior to that, from 1986 to 1989, Mr. Fine served as an Assistant United States Attorney in the Washington, D.C., United States Attorney's Office. In that capacity, he prosecuted more than 35 criminal jury trials, handled numerous grand jury investigations,

and argued cases in the District of Columbia and U.S. Courts of Appeals.

Mr. Fine graduated magna cum laude from Harvard College in 1979 with an A.B. degree in economics. He was a Rhodes Scholar and earned B.A. and M.A. degrees from Oxford University. He received his law degree magna cum laude from Harvard Law School in 1985.