

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

# THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

DEPARTMENT OF HOMELAND SECURITY

# Semiannual Report to the Congress



OFFICE OF INSPECTOR GENERAL

October 1, 2002 - March 31, 2003



**DEPARTMENT OF HOMELAND SECURITY**  
Office of Inspector General  
Washington, DC 20528

April 30, 2003

The Honorable Tom Ridge  
Secretary  
The Department of Homeland Security  
Washington, DC 20528

Dear Mr. Secretary:

The Inspector General Act of 1978 (Public Law 95-452), as amended (the "Act"), requires the preparation of a Semiannual Report to the Congress summarizing the activities of Offices of Inspector General (OIG). I am pleased to enclose a report for the period March 1, 2003 to March 31, 2003. The Act also mandates that you transmit this report to the appropriate committees of Congress within 30 days of receipt, together with any comments thereon you may wish to make.

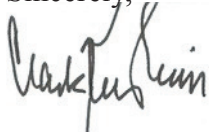
The Department of Homeland Security (DHS), and DHS OIG likewise, came into being on March 1, 2003. Hence, this first semiannual report covers only one month of the standard six month reporting period. However, to provide a more complete picture of the issues facing DHS, I have included brief summaries of the audits, investigations, and inspections completed by the "legacy" agency OIGs during the period October 1, 2002 through February 28, 2003. The legacy agency Inspectors General will issue their own respective reports for this six month period.

During this reporting period, I spent a significant percentage of my time meeting with those OIG and General Accounting Office (GAO) officials who oversaw departments or parts thereof that are now incorporated into DHS. Each of them has detailed the applicable component's top management challenges and other significant issues relating to the economy, efficiency, and/or effectiveness of the components' respective programs and operations. In the Executive Summary of this report is a consolidated list of these management challenges. This list will be used to set DHS OIG's own priorities for audits and inspections or evaluations of DHS programs and operations. In addition, to the extent there are recommendations from legacy OIGs relating to such challenges, we will undertake to track compliance for them.

Another priority for me during the first few weeks of DHS OIG's operations has been demarcating the line between the investigative authority of my own office and that of DHS' various internal affairs offices. The Act assigns to DHS OIG the dominant role in investigating criminal and non-criminal allegations against department employees, contractors, and grantees relative to department programs and operations, and it requires DHS OIG to oversee such investigations as are conducted by internal affairs offices. Accordingly, DHS OIG has signed memoranda of understanding regarding this matter with two of the four relevant DHS components, namely, the Border and Transportation Security directorate and the Bureau of Citizenship and Immigration Services as to the practicalities of how any given allegation should be handled. We are seeking to conclude similar agreements with the United States Secret Service and the United States Coast Guard in the near future. Our aim is to ensure that DHS OIG can carry out its statutory responsibilities, and, in so doing, provide DHS and the Congress with an independent assurance that matters meriting investigation are thoroughly pursued.

I am grateful to you for the support that you have provided me and my office to date. My staff and I are committed to working closely with you and other senior DHS leadership toward the goal of promoting economy, efficiency, and effectiveness in the department's programs and operations.

Sincerely,

A handwritten signature in black ink, appearing to read "Clark Kent Ervin". The signature is written in a cursive style with some loops and flourishes.

Clark Kent Ervin  
Acting Inspector General

Enclosure

# Table of Contents

Executive Summary .....	1
Department of Homeland Security .....	14
Office of Inspector General.....	15
Border and Transportation Security .....	16
Emergency Preparedness and Response .....	32
Information Analysis and Infrastructure Protection.....	32
Science and Technology.....	32
Management.....	32
Coast Guard .....	33
Secret Service.....	34
Bureau of Citizenship and Immigration Services .....	35
Investigations Statistics.....	37
Investigation Narratives .....	39

If you would like to read the entirety of any one of the reports summarized in this document, please go to the respective legacy Office of Inspector General web site:

[www.oig.dot.gov](http://www.oig.dot.gov)  
[www.treas.gov/offices/inspector-general](http://www.treas.gov/offices/inspector-general)  
[www.usdoj.gov/oig](http://www.usdoj.gov/oig)  
[www.fema.gov/ig](http://www.fema.gov/ig)

# Executive Summary

## Major Management Challenges Facing DHS

Over the course of the first few weeks of DHS' existence, I spent a significant percentage of my time meeting with those OIGs and GAO officials who oversaw departments or parts thereof that are now incorporated into DHS. Each of them has detailed the applicable component's top management challenges and other significant issues relating to the effectiveness, efficiency, and/or economy of the components' respective programs and operations. Following, based largely on those inputs, is a consolidated list of management challenges. These challenges will be used in setting DHS OIG's own priorities for audits and inspections or evaluations of DHS programs and operations. In addition, to the extent there are relevant recommendations from "legacy" OIGs relating to such challenges, we will undertake to track compliance for them.

## ESTABLISHING THE DEPARTMENT OF HOMELAND SECURITY

Perhaps the biggest challenge facing DHS is integrating 22 separate components into a single, effective department. Appropriate plans (including workforce plans), goals, objectives and meaningful performance measures must be established as soon as possible to guide that process and track progress.

Complicating the process is the fact that some of the more important components were already undergoing transformation. For example, prior to 9/11, homeland security related matters consumed 14% of the Coast Guard's resources. After 9/11, that percentage rose to 58%. Congress has expressed a concern as to whether, with the transfer of the Coast Guard from the Department of Transportation (DOT) to DHS, its non-homeland security related missions (marine environmental protection, fisheries enforcement, aids to navigation, and illegal drug and migrant interdiction) will be neglected. DHS OIG is required to conduct an annual review of the Coast Guard, with a particularly focus on whether the Coast Guard is meeting such missions.

Further, combining these entities will present opportunities for integrating systems and operations for greater economy and efficiency. For example, DOT OIG recommended that DHS take advantage of the economies of scale that can come from combining the Transportation Security Administration (TSA),

the Immigration and Naturalization Service (INS), and the Customs Service (Customs). Administrative services, such as contracting, budgeting, legal, human resources, and internal affairs, should be consolidated. Likewise, airport space requirements for functions like office space, break rooms, training facilities, and detention cells should be consolidated. Finally, TSA should work with other DHS agencies, the airports, and other federal, state, and local law enforcement agencies before expanding its law enforcement duties (such as the current proposal for extending the federal air marshal program to conducting surveillance and patrolling at airports).

## **CONTRACT AND GRANTS MANAGEMENT**

### **Contract Management**

DHS will be integrating the procurement functions of many constituent programs and component missions, some lacking important management controls. For example, as reported by GAO, Customs has not begun to establish process controls for determining whether acquired software products and services satisfy contract requirements before acceptance, nor to establish related controls for effective and efficient transfer of acquired software products to the support organization responsible for software maintenance. At TSA, where contracts totaled \$8.5 billion at the end of calendar year 2002, the DOT OIG found that procurements were made in an environment where there was no pre-existing infrastructure for overseeing contracts. TSA had to rely extensively on contractors to support its mission, leading to tremendous growth in contract costs. A recent review by TSA of one subcontractor found that, out of \$18 million in expenses, between \$6 million and \$9 million appeared to be attributed to wasteful and abusive spending practices.

Also, some agencies have large, complex, high-cost procurement programs under way that need to be closely managed. For example, Customs' Automated Commercial Environment (ACE) project will cost \$5 billion, and Coast Guard's Deepwater Capability Replacement Project will cost \$17 billion and take two to three decades to complete.

This \$17 billion, multi-year project to upgrade the Coast Guard's fleet of ships, aircraft and communication systems for use far off shore in an integrated package was planned before 9/11, but no changes were made in project requirements after 9/11 and before awarding the contract in June of last year. DOT OIG has argued that post 9/11 changes in the Coast Guard's mission requirements argue for re-evaluating aspects of the project (for example, whether to arm more of its helicopters, whether to add more secure information handling capability, and ensuring that its systems can communicate with other DHS systems). Any such re-evaluation should be done sooner rather than later, especially now that the DHS Act has passed, requiring that consideration be given to accelerating the timetable for Deepwater from 20-25 years to 10. In addition to re-evaluating requirements, the Coast Guard should stabilize and prioritize the requirements, lest Deepwater investments crowd out other needed investments (plugging gaps in Rescue 21, the 911 system for mariners in distress, modernizing aids to navigation, rehabilitating aged buildings, piers, and other shore facilities, and replacing boats used close to shore).

On its \$1 billion IT infrastructure project, TSA did not issue a statement of work detailing its requirements. Instead, it asked vendors to bid based on a "statement of objective" containing no specific requirements. While this approach enabled TSA to select a vendor (Unisys) quickly, it places total reliance on contractors not only to deliver them but also to decide the agency's requirements. As a result, it may be difficult for the agency to evaluate the contractors' performance.

Further, some contracts, regardless of their earlier merits, may no longer be necessary in accomplishing DHS' mission.

### **Grants Management**

Essentially, DHS will absorb five distinct emergency preparedness grant programs: (1) a \$3.5 billion First Responder Program; (2) a \$300 million Assistance to Firefighters Grant Program; (3) a \$300 million Domestic Preparedness Grant Program; (4) a \$500 million Public Health Emergency Preparedness Program; and (5) a \$300 million Emergency Management Preparedness Grant Program. Previous FEMA and Department of Justice



(DOJ) OIG reports have identified significant shortcomings in the pre-award process, cash management, monitoring, and grant closeout processes. Further, each of these programs has redundant or similar features, i.e., emergency planning, training, and equipment purchases and upgrades for emergency management personnel (state and local police, firefighters, and health care workers). Nevertheless, these programs are to be divided between two separate DHS directorates. Preparedness for terrorism will be placed in the Border and Transportation Security directorate, while other preparedness efforts will be located in the Emergency Preparedness and Response directorate. This bifurcation will create additional challenges related to inter-departmental coordination, performance accountability, and fiscal accountability. Furthermore, program managers have yet to develop meaningful performance measures necessary to determine whether the grant programs being absorbed by DHS have actually enhanced state and local capabilities to respond to terrorist attacks and natural disasters.

## **BORDER SECURITY**

The INS has about 9,000 agents along the border with Mexico, augmented by fences and a substantial automated sensor and surveillance infrastructure. On the Canadian border, however, INS is under-resourced in both personnel, with approximately 500 agents, and equipment. GAO has estimated that it will take years before INS can fully implement its border strategy.

**Entry/Exit Tracking:** INS has no effective system to determine whether non-citizens who enter the country subsequently leave it. Many aliens enter under temporary visas and then remain past the expiration date (“visa overstays”). Prior INS efforts tracked only travelers entering and exiting at airports by collecting paper forms, which proved to be an expensive failure. DOJ OIG has found in its reviews that INS lacks project management skills and the information technology (IT) capability to ensure successful acquisition and deployment of such a system.

INS has initiated the National Security Entry-Exit Registration System (NSEERS), a targeted tracking system for male nationals from 25 designated countries that includes photographing, fingerprinting, and location reporting. The

system is intended to enable INS to check the individual against criminal history and immigration record databases, to verify reported location and activities, and to determine whether the alien overstayed his/her visa. The Senate's Fiscal Year 2003 budget markup expressed a concern that INS' claim of success for this program needs to be verified. In addition, the DOJ OIG has received indications that the program is unevenly administered and misapplied by INS personnel who do not fully understand the program's criteria.

**Student Visa Tracking:** INS is developing the Student & Exchange Visitor Information System (SEVIS), a computerized student tracking system designed to tighten INS monitoring of foreign students. DOJ OIG's review expressed concerns over computer difficulties SEVIS has experienced, noted that the accreditation of schools involves only a superficial review with many schools yet to be reviewed, and pointed out that the success of SEVIS depends on schools' willingness to provide data relative to their foreign students.

**Joint INS-FBI Fingerprinting Initiatives:** INS has used a two-print fingerprint scanning and automated search system (IDENT) to identify repeat illegal entries by aliens and to conduct a criminal history check against a limited INS database. The INS and the FBI have been working for several years to integrate IDENT with the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS), which is a ten-print full criminal history check. This integration is critical to identifying illegally entering aliens on lookout lists or with criminal histories, but progress has been slow. DOJ OIG is beginning its fourth review of this project (focusing on the FBI angle); it was also one of the four major INS systems that GAO studied, reporting poor oversight and management.

**High-Technology Equipment:** The Remote Video Inspection System (RVIS) is designed to expedite the clearance of low-risk travelers and to enhance security at remote northern border crossings. RVIS is designed to transmit images of the person, vehicle, documents, and passengers to an inspector located miles away at the main monitoring, 24-hour port of entry. As of September, 2001, only seven sites were capable of operating RVIS equipment. Poor contractor performance and

a lack of strong oversight caused delays in the deployment of RVIS. Since 9/11, Customs has relied primarily on inspectors at these northern border sites.

Treasury OIG completed audits on Customs' use of two other high-tech systems, trace detection equipment and radiation detection systems. With respect to the former, Treasury OIG found that Customs was not effectively or efficiently using the equipment because management did not ensure that the detectors were placed in locations most conducive to their use, failed to maintain them adequately, and failed properly to train inspectors on their use. For radiation detection systems, Customs does not have a documented strategic plan to ensure proper acquisition and deployment of the equipment, and it has not been collecting data on the usage or performance of the equipment. Also, most of the radiation detection equipment currently being used by Customs inspectors is focused on detecting gamma radiation and is unable to detect neutron radiation.

The Advance Passenger Information System (APIS) is a border enforcement tool used by both Customs and INS at our nation's airports to identify and detain high risk travelers on flights bound for the United States. The system is intended to collect biographical information such as name, date of birth, and country of residence from international airline passengers and crewmembers entering the United States at airports around the country. Prior to arrival, these people are matched against law enforcement databases to identify people who should be detained and examined for violation of U.S. law.

Treasury OIG completed an audit report on APIS. The report concluded that the value of APIS is dependent on several factors beyond Customs' control. First, the authenticity of passenger and crew information is dependent on other governments' source documents (passports, visas, etc.), and the integrity of those documents is sometimes questionable. Second, Customs depends on INS to make referrals based on INS' initial screening of arriving passengers and crewmembers. Third, APIS depends on the FBI's National Crime Information Center (NCIC) and Interagency Border Inspection System (IBIS) data to match APIS data for "hits" to occur; however, NCIC and IBIS may require data, like birth dates, that APIS does not always contain.

## **INTERIOR ENFORCEMENT/DETENTION**

INS is thinly positioned to fulfill its non-border enforcement responsibilities. The effectiveness of systems like SEVIS and NSEERS depends on INS' using the information the systems generate to locate and remove aliens who overstay their visas or otherwise violate the terms of their admission. DOJ OIG concluded in a recent study that, on average, INS is deporting only about 13% of all non-detained aliens under final orders of removal. The study also sampled high-risk categories and found that INS had removed only 6% of aliens with final removal orders who came from countries listed as sponsors of terrorism. And, only 35 % of aliens with criminal records and final removal orders were removed. To complicate matters further, INS has other daunting interior enforcement responsibilities that include investigating document fraud and counterfeiting, preventing the illegal employment of undocumented aliens, and attacking sweatshops and smuggling enterprises that exploit undocumented aliens.

On average last fiscal year, the INS had 188,547 aliens in detention facilities each day. In addition to its own facilities, INS houses detainees in state, local, and contractor operated jails, for which INS pays a daily rate to the facility. INS recently obtained clearance to pay a profit to state and local jails with which it does business. The practice is likely to cause a significant increase in its detention costs as other suppliers seek comparable treatment.

State and local correctional institutions also hold many aliens who are removable at the conclusion of their criminal sentence. INS' institutional removal program seeks to identify such persons and to conclude the INS removal process before these aliens are released from state or local prison. If INS does not conclude the removal process before the inmate's release, INS must detain such aliens in an INS facility until removal and absorb the costs of doing so. Avoidable detention costs could reach \$200 million annually, according to DOJ OIG. DOJ OIG also found that INS lacked comprehensive information about deportable aliens, and, as a consequence, many of them can pass through detention facilities undetected. DOJ OIG found instances where inmates not identified by the INS as potentially deportable went on to commit more crimes after being released

into the community, including child molestation, aggravated assault, and cocaine trafficking.

DOJ OIG has also reviewed INS' implementation of its policies for escorting criminal aliens who are being removed from the United States. The report concluded that the INS has placed the traveling public at risk because it does not consistently follow its own escort policy. Some INS field supervisors disregarded provisions of the policy, resulting in the transportation of violent aliens on commercial airlines without escorts.

### **INFORMATION TECHNOLOGY AND SECURITY**

Information technology will be a major management challenge for DHS. Initially, the CIO will need to establish a department-wide IT infrastructure that will enable communications among approximately 180,000 employees. In addition, the CIO will face the challenge of identifying the agency's IT assets, determining what IT assets are needed to meet mission requirements, and consolidating hundreds of systems from transferred agencies. In addition, the CIO, as required by the Federal Information Security Management Act (FISMA), will have a major challenge in developing and implementing an agency-wide information security management program that addresses the risks and vulnerabilities facing the agency's IT systems.

For example, INS has 87 different computer systems that handle sensitive information. INS has not managed IT acquisition or deployment well. DOJ OIG audits have shown that INS has failed to establish cost baselines, conduct life-cycle development planning, and control costs and delivery schedules. INS also has often lacked comprehensive performance measures to ensure that completed projects meet intended goals and uses.

Another example is the Automated Commercial Environment (ACE) project. ACE is intended to enable Customs to release cargo more efficiently by integrating international law enforcement intelligence, commercial intelligence, and data mining results to focus attention on high-risk importers and accounts. Treasury OIG audit reports have concluded, among other things, that Customs did not have

the people and systems in place adequately to manage the development of ACE. Because controls were not being implemented and base line reviews were not being performed, Customs could not identify problems in a timely manner. And, Customs was emphasizing scheduled completion dates at the expense of quality and completeness.

Computer security is a related concern. For example, DOJ OIG found numerous vulnerabilities in two key INS systems that were reviewed pursuant to the Government Information Security Reform Act. Further, Customs has not established effective controls to protect its law enforcement related data against unauthorized modification, loss, or disclosure. Any compromise in the security of the law enforcement data contained in Customs' databases would have a detrimental effect on Customs' ability to perform its law enforcement duties.

## **FINANCIAL MANAGEMENT**

The department quickly must integrate and establish effective controls over the financial systems and operations of the incoming components, each of which brings with it longstanding weaknesses in need of correction. Some components have received unqualified audit opinions on their financial statements; however, they expend tremendous manual efforts and costs to prepare for their financial statements, and weaknesses exist in financial preparation and control. For example, INS has poor databases upon which to calculate accurate fees and to ensure that the fees are spent on the services for which they were paid. INS collects and processes its own fees, but it has been found to have poor cash collection processes at virtually every kind of intake facility. INS has had to halt normal business operations for up to two weeks each year in order to conduct manual counts of millions of applications to calculate its earned revenue figures for its annual financial statement.

In addition, the Customs Service is the second largest revenue producer for the federal government. Total net revenues (duties, excise taxes, user fees, licenses, and other revenue, less refunds, drawbacks and other credits) collected during fiscal year 2002 were \$22.1 billion. Ongoing weaknesses in the design and operation of Customs' controls over trade activities and financial management

and information systems continue to inhibit the effective management of these activities and protection of trade revenue.

Also, Customs has been losing between \$151 and \$432 million per year in uncollected duties related to international mail. Further, Customs had difficulty in collecting outstanding duties already collected by the Postal Service, primarily due to problems in reaching agreement with the Postal Service on the amounts due.

## **TRANSPORTATION SECURITY**

**Gap between security costs and security funding:** DHS has requested \$4.8 billion for aviation security in fiscal year 2004. This is projected against fiscal year 2003 and 2004 passenger security fee revenues of about \$1.7 billion annually and \$300 million annually in contributions from the airlines. DOT OIG has recommended strongly against increasing passenger security fees further, noting that government taxes and fees already constitute 26% of airline ticket costs. DOT OIG also recommended against tapping the airport improvement grants program further, observing that doing so would negatively affect airports' ability to fund needed capacity enhancing projects. The alternative is to tap the general fund, at a time when it is already strained by competing demands throughout the federal government.

**Screeners:** Before 9/11, there were only about 28,000 screeners at the nation's airports. In the last year TSA has hired 62,000. Having augmented the numbers significantly, DOT OIG has recommended that TSA: (1) develop a screener performance measurement system and use it to target training resources to where they are most needed; (2) expand the skills of existing staff and keep them at peak performance levels; (3) determine the proper balance of training between existing and new staff; and (4) "transition" the 45% of screeners who are "temporary" employees into permanent positions or replace them with new employees (who will have additional training needs).

**Checking Bags for Explosives:** TSA's largely successful effort to implement the requirement that all checked bags be screened by explosives detection equipment

by December 31, 2002 has cost \$1.6 billion to date. Remaining to be done is: (1) deploying such equipment to the remaining airports where alternative screening methods are in use today; and (2) integrating explosives detection systems into baggage handling systems at the largest airports (at a cost of more than \$3 billion); and (3) using research and development funds to develop and deploy more effective and economical equipment to address current and future threats and risks.

**Other Transportation Modes:** Appropriately, TSA focused its first year efforts on aviation security. This year more focus should be given to mass transit, rail, and intermodal containers. DHS needs to develop meaningful risk assessments and to target limited resources to the areas of greatest vulnerability. Progress is being made on the container vulnerability issue, but this will require implementation.

DOT's continuing responsibilities for transportation safety and efficiency, including transportation of hazardous materials (HAZMAT) will overlap with DHS responsibilities for transportation security, requiring close coordination between the two departments and between the departments and industry. As a start, DHS and DOT should finalize a Memorandum of Agreement outlining their respective security roles and responsibilities.

## **PORT SECURITY**

While Customs has taken positive steps to address the terrorist threat, additional steps are needed. Specifically, Treasury OIG found that vessel containers were not properly secured from the time of entry into port until the time of release by Customs. Physical security at the port and terminals was lax. Customs did not maintain adequate control over targeted containers being delivered for examination. The time between targeting and examination was unduly long. Certain Customs identified security upgrades were not being adequately implemented. Examinations performed were not in accordance with established guidelines, and the results were not always properly recorded in Customs databases. Customs targeting units were either understaffed, poorly trained, and/or given many collateral duties that diverted focus from targeting.



Treasury OIG took note of new Customs initiatives in the area of port security, including CSI, C-TPAT, and ATS, suggesting that further OIG evaluative work in each area is advisable. CSI (Container Security Initiative) is a partnership with other governments to target and inspect high-risk vessel containers in foreign ports before those containers are shipped to the United States. C-TPAT (Customs Trade Partnership Against Terrorism) is a joint government-business initiative designed to build cooperative relationships that strengthen overall supply chain and border security. Businesses ensure the integrity of their security practices and communicate their security guidelines to their business partners, thereby taking an active role in the war against terrorism. In return, Customs provides specific “benefits,” such as a reduced number of inspections. Another initiative is to improve ATS, the Automated Targeting System, by revising rules and rule weights to enhance capabilities for identifying cargo that might conceal weapons of mass destruction and other instruments of terrorism.

Treasury OIG has found that Customs management controls are not sufficient to mitigate the significant safety, smuggling, and terrorism risks associated with the importation of hazardous materials. Customs’ ability to examine HAZMAT cargo is limited due to the inherent danger in handling these materials and the lack of training on the part of personnel. HAZMAT teams are not actively making internal risk assessments concerning dangerous cargo, visiting importers’ premises, and providing advice on obtaining samples. Furthermore, both headquarters and port personnel have an aging Automated Commercial System (ACS) that does not provide the information necessary best to allocate HAZMAT resources or to determine which port or what type of HAZMAT shipments may be at highest risk for smuggling drugs or becoming instruments of terrorism.

Since 9/11, Customs has expanded the use of high-tech equipment to search for radioactive materials, explosives, chemicals, and biological materials. These pieces of equipment – which includes various vehicle and rail x-ray systems, radiation detection systems, trace detection systems, video systems, and the like – permit Customs officials to inspect cargo and conveyances for contraband without having to perform the costly and time consuming process of unloading cargo or drilling through or dismantling conveyances.

Treasury OIG has been unable to determine whether use of the equipment is meeting Customs' goals. Customs had not developed performance measures or otherwise evaluated the effectiveness of the equipment. Moreover, Customs needed to do a better job of monitoring equipment utilization; the limited data available indicated that equipment was being underutilized. In addition, Treasury OIG found that Customs needed better to track and account for equipment and better plan deployment to avoid installation problems.

## **INTERNATIONAL MAIL**

Each year a huge volume of international mail transported by foreign postal administrators - approximately 160 million letters and parcels - enters the United States at 14 international mail branches (IMB). These IMBs are dispersed throughout the country, but are often co-located with international airports, seaports, and land ports. All international mail is subject to Customs examination, and IMBs are staffed with Customs inspectors, mail specialists, and mail technicians - a total staff of 164 at the 14 locations - who inspect the mail for both contraband and duties owed. Customs uses automated screening equipment, such as x-ray and radiation detection devices and dogs, to assist inspectors in examining the mail.

Treasury OIG audits have found both enforcement and revenue problems. IMBs lacked controls for ensuring that all mail was delivered to Customs for inspection. In some locations, mail bypassed Customs before being delivered to addressees, and in other cases mail was not being adequately safeguarded. Customs needs to take action to ensure that all mail is delivered to IMBs for inspection. Customs also needs to ensure adequate inspector resources and screening equipment is in place adequately to assess potential threats.

# Department of Homeland Security

The creation of DHS is the most significant transformation of the U.S. government since 1947, when President Truman merged the various branches of the armed forces into the Department of Defense better to coordinate the nation's defense against military threats.

DHS represents a similar consolidation, both in style and substance. In the aftermath of the terrorist attacks against America on September 11th, 2001, President Bush determined that 22 disparate domestic agencies needed to be coordinated into one department to protect the nation against threats to the homeland.

The new department's first priority is to protect the nation against further terrorist attacks. Component agencies will analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of our nation to future emergencies.

Besides providing a better coordinated defense of the homeland, DHS is also dedicated to protecting the rights of American citizens and enhancing public services, such as natural disaster assistance and citizenship services, by dedicating offices to these important missions.

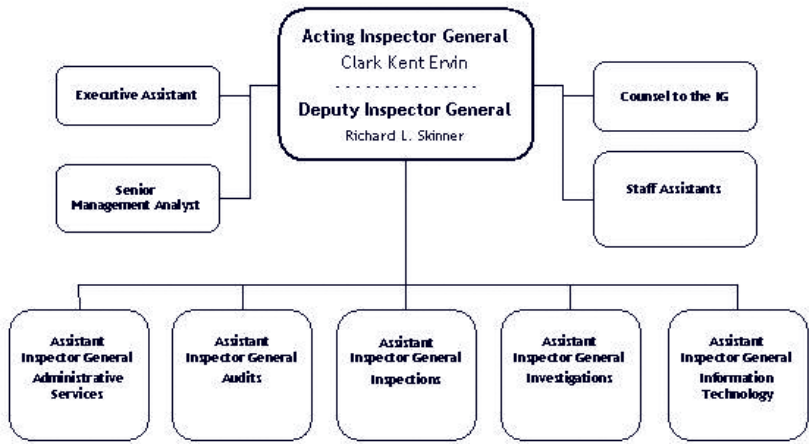
The 22 agencies have been reconfigured into the following nine divisions: Border & Transportation Security, Emergency Preparedness & Response, Information Analysis & Infrastructure Protection, Science & Technology, Management, Coast Guard, Secret Service, Citizenship & Immigration Services, State & Local Government Coordination, and Private Sector Liaison.

# Office of Inspector General

Congress enacted the Inspector General Act of 1978, as amended, to promote integrity and efficiency in government. The Homeland Security Act of 2002, as amended (the Act), established an Office of Inspector General in the Department of Homeland Security. The Inspector General is appointed by the President and subject to Senate confirmation.

The Inspector General is responsible for conducting and supervising audits, investigations, and inspections relating to the programs and operations of the department. The OIG is to examine, evaluate and, where necessary, critique these programs and operations, recommending ways for the department to carry out its responsibilities in the most effective, efficient, and economical manner possible. The Act also assigns to DHS OIG the dominant role in investigating criminal and non-criminal allegations against department employees, contractors, and grantees relative to department programs and operations, and it requires DHS OIG to oversee such investigations as are conducted by internal affairs offices.

On March 1, 2003, DHS OIG acquired personnel and assets from OIGs that had exercised oversight authority over agencies or parts thereof that were merged into DHS. All 200 FEMA OIG full-time equivalent employees (FTEs), 195 Treasury Department OIG FTEs, 45 Transportation Department OIG FTEs, 15 Justice OIG FTEs, and 2 FTEs each from the General Services Administration and Agriculture Departments OIGs were transferred to DHS. Of the total number of 459, 186 are located in Washington, D.C., and 273 are located in 21 field offices throughout the country. DHS OIG's budget for the balance of fiscal year 2003 is \$45 million; we are requesting a budget of \$80 million for fiscal year 2004. A copy of the DHS OIG organization chart with additional detail is attached.



# Border and Transportation Security

## **INS Reemployment of Annuitants**

Normally, federal annuitants rehired by the federal government must have their salary offset by an amount equal to the annuity they receive from the government. In 1996, the Office of Personnel Management (OPM) granted the INS emergency authority to rehire federal annuitants, waive the offset, and pay annuitants their full salary. The Department of Justice (DOJ) OIG audited the INS' rehiring of annuitants in response to a request by the Chairmen of the House Judiciary Committee and the Subcommittee on Immigration, Border Security, and Claims. The DOJ OIG found that the INS did not accurately track the number of federal annuitants it rehired, lacked sufficient accounting controls to confirm the compensation paid to them, had not documented its rationale for hiring each annuitant, and had not developed an effective plan to reduce its dependence on rehired annuitants. Based on records it obtained from the National Finance Center, the DOJ OIG reported that the INS employed 379 annuitants and paid them approximately \$49 million in salary (including overtime) in FY 1996 through FY 2002. Of those 379 annuitants, 294 received waivers and salary compensation totaling \$39.5 million. *The full report, 03-16, was issued by the DOJ OIG, in February 2003.*

## **Quality Control Reviews of TSA's Audited 2002 Financial Statements**

DOT OIG publicly released its quality control review of the audit of TSA's FY 2002 financial statements. The audit was completed by KPMG LLP, Washington, DC. KPMG gave TSA an "unqualified" opinion on its financial statements. The TSA audit report cited five "material internal control weaknesses," one "reportable internal-control condition," and one "material noncompliance" with accounting laws and regulations. KPMG made 18 recommendations to TSA for corrective actions. DOT OIG agreed with the recommendations and found KPMG's audit work complied with applicable government accounting standards. DOT OIG asked TSA to specify its actions and estimated completion dates. *The full report, QC-2003-OIG, was issued by the DOT OIG on January 27, 2003.*

### **IG Testifies Regarding TSA's Aviation Security Costs Before Senate Commerce Aviation Subcommittee**

The DOT Inspector General testified before the Senate Commerce, Science, and Transportation Aviation Subcommittee regarding TSA's aviation security costs. In the last 14 months TSA has made noteworthy accomplishments without any pre-existing infrastructure for overseeing contracts or managing human resources. However, controlling costs must be a priority. The DOT Inspector General testified that TSA will need at least \$3 billion to integrate explosives detection into baggage handling systems at the largest airports, and the need to deploy more effective equipment to meet threats will be ongoing. He urged caution before adding more air travel fees or taxes, saying the most likely option for meeting TSA's financial requirements above existing revenues was to continue using the General Fund to pay a large portion of security costs. *The full report, CC-2003-066, was issued by the DOT OIG, February 5, 2003.*

### **TSA's Progress in Implementing the Aviation and Transportation Security Act**

DOT OIG issued its review of TSA's progress in implementing provisions of Sections 106 and 138 of the Aviation and Transportation Security Act, as requested by Representative James L. Oberstar, Ranking Minority Member of the House Transportation and Infrastructure Committee. Section 106 requires all individuals, goods, property, vehicles, and other equipment to be screened before entering a secure area of an airport in the U.S. Section 138 requires an employment investigation, including a criminal history check, on anyone who has regular escorted access to aircraft or a secure area of an airport. DOT OIG found TSA is taking steps to implement the two sections. This report contains sensitive security information and will not be publicly released.<sup>1</sup> *The full report was completed by the DOT OIG, February 27, 2003.*

<sup>1</sup> The number of any report denoted as containing sensitive security information is not disclosed.

## **TSA's Oversight of Security Screener Contracts**

DOT OIG's audit of TSA's oversight of its security screener contracts found that, based on their hourly rates, six of 13 large contractors charged TSA about \$305 million more for passenger screening services than they previously charged air carriers for similar work. TSA deployed a federal workforce to screen passengers at all airports but has not yet negotiated final contracts with 18 of 74 contractors as of February 26, 2003, including 11 large contractors. TSA is withholding more than \$90 million in payments to contractors that had significantly increased their rates to TSA, pending completion of an audit by the Defense Contract Audit Agency, and it reported contract management as a "material internal control weakness." *The full report, FI-2003-025, was issued by the DOT OIG on February 28, 2003.*

## **Review of TSA's Screener Security Program**

DOT OIG audited TSA's hiring and training of aviation screeners. TSA has made great strides in hiring and training passenger and checked baggage screeners at the nation's commercial airports, but it needs to take additional actions to build a "world class" security workforce. TSA has already moved to correct several weaknesses, but there are four areas where it still needs to take action. TSA agreed to take corrective action and concurred with most of the OIG's findings and recommendations. This report contains sensitive security information and will not be publicly released. *The full report was completed by the DOT OIG on February 28, 2003.*

## **Review of Proposed Aviation Security Technologies**

DOT OIG issued the results of its review of proposed technologies to improve aviation security, a study requested by Representative Martin Sabo. DOT OIG reviewed technologies for their potential to improve aviation security in the airport, aircraft, checked baggage, screening checkpoint, and cargo and mail. DOT OIG recommended actions to foster the development and deployment of aviation security technologies in the near, intermediate, and long term. This



report contains sensitive security information and will not be publicly released.  
*The full report was completed by the DOT OIG on February 28, 2003.*

### **Review of Security at Aircraft Repair Stations**

As part of DOT OIG's larger audit of air carriers' use of aircraft repair stations, they reviewed security controls at these stations. The audit disclosed security vulnerabilities at repair stations located at commercial and general aviation airports and off airport property. DOT OIG recommended that TSA conduct risk based security assessments as a first step in determining the actions needed to address repair station security. This report contains sensitive security information and will not be publicly released. *The full report was completed by the DOT OIG on February 28, 2003.*

## **Customs' Advance Passenger Information System (APIS) Is A Valuable Enforcement Tool But Relies On Factors Outside Its Control**

APIS provides airport inspectors from both the INS and Customs with biographical information on airline passengers and crewmembers from foreign countries. While initially a voluntary program under a November 2001 law, all carriers are now required to provide this information. Customs is responsible for ensuring that air carriers comply with APIS requirements and Customs is authorized to issue penalties to airlines that do not comply.

APIS identifies individuals to intercept and examine. INS and Customs personnel intercept targeted passengers or crew for examination. Treasury OIG found concerns with the system that hindered Customs' enforcement efforts. Treasury OIG also noted that penalties for non-compliance were administered inconsistently. Treasury OIG recommended that Customs take a more uniform approach to enforcing compliance with APIS requirements. To enhance enforcement efforts, Treasury recommended that INS and Customs monitor the usefulness of APIS as an enforcement tool. Treasury OIG recommended that Customs work with DOJ and Treasury to eliminate any possible weaknesses in the program. Customs has taken appropriate action to address these recommendations. On March 1, 2003, APIS became the responsibility of DHS. *The full report, OIG-03-059, was issued by the Treasury OIG.*

## **The Customs National HAZMAT Program Needs To Be Strengthened**

This audit was the third and final report in a series of audits on the United States Customs Service (Customs) hazardous materials (HAZMAT) Program. The objective of this series of audits was to determine whether Customs had sufficient processes in place to ensure the safe and legal transport and inspection of cargo containing hazardous materials. The Department of the Treasury OIG's first report (OIG-02-123 dated September 30, 2002) provided recommendations for a better HAZMAT program at the Port of Brownsville. Its second report (OIG-03-049 dated January 22, 2003) provided recommendations to strengthen the program at the Port of Houston.

A hazardous material is a substance or material that has been determined by the Secretary of Transportation to be capable of posing an unreasonable risk to health, safety and property. Customs developed the HAZMAT Handbook to provide safe, uniform, and environmentally sound procedures for processing this type of cargo, and to ensure compliance with all statutes and regulations pertaining to hazardous materials.

The audit found that Customs management controls are not sufficient; HAZMAT training records were not adequately documented and maintained; and Emergency Action Plans at port facilities were missing or needed to improve required Occupational Safety and Health Administration (OSHA) elements.

Treasury OIG made five recommendations to correct the deficiencies in the HAZMAT program. Customs concurred with the five recommendations and agreed to take corrective action, including having the HAZMAT Headquarters Administrator and HAZMAT personnel take a more active role in the HAZMAT program activities at the ports and revising the HAZMAT Handbook. *The third and final report of this series, OIG-03-065, was issued by the Treasury OIG, on March 17, 2003.*

### **Utilization of Trace Detection Equipment**

Trace detection technology makes use of the minute amounts of vapors given off and the microscopic particles left behind when narcotics and explosives contraband are packaged and handled. This technology provides Customs with the capability to screen and search in a non-intrusive manner for the trace quantities of narcotics and explosives on people, baggage, cargo, vehicles, containers, tickets and identification cards. Prior to the attacks of September 11, 2001, trace detection technology was used by Customs with an emphasis on narcotics interdiction.

Trace detection equipment was delivered to the field as part of the initial deployment of non-intrusive inspection equipment in the late 1990s, per the Customs' Five-Year Technology Plan. The objective was to add this technology to the ports' arsenal of tools, providing a "layered defense" against smuggling.

Treasury OIG's review of trace detection equipment concluded that Customs is not using trace detection equipment in the most efficient and effective manner. This was caused by: (1) a lack of management direction to ensure that the detectors were placed in locations most conducive to their use; (2) a lack of required maintenance necessary to produce reliable readings; and (3) inspectors' operating detectors without adequate training.

Treasury OIG recommended that Customs: (1) re-deploy the equipment to the most optimum sites within locations; (2) ensure that inspectors are adequately trained; and (3) ensure that trace detection equipment is utilized, and its usage and maintenance recorded.

Responsibility for trace detection equipment transferred with Customs to DHS. *The full report, OIG-03-068, was issued by the Treasury OIG, March 24, 2003.*

### **Enforcement of Export Controls**

This review was conducted in partnership with the OIGs at the Departments of Commerce, Defense, State, and the Central Intelligence Agency. The overall objective was to evaluate the adequacy and effectiveness of Treasury's export enforcement activities concerning the transfer of militarily sensitive technology to countries of concern, including its efforts to: (1) prevent the illegal export of dual use items and munitions; and (2) investigate and assist in the prosecution of export control violators.

Treasury OIG found that Customs has devoted limited resources to export enforcement. OIG identified numerous factors that impaired Customs' ability to enforce export controls effectively, some of which were beyond Customs' control. They also found that, though Customs implemented certain corrective steps to address recommendations made in a 1999 OIG audit report, problems remained. Therefore, Treasury OIG believes that corrective actions taken were not always effective in correcting the deficiencies cited in the prior report.

Treasury OIG also found that a Treasury bureau, the Office of Foreign Assets Control (OFAC), could benefit from better coordination with the State Department

and Customs. In addition, OIG found that the State Department did not always timely process OFAC referrals. OIG also maintained that Customs needs to keep OFAC apprised of the status of referred cases. OIG made 11 recommendations to improve the effectiveness of Treasury's enforcement of export controls. *The full report, OIG-03-069, was issued by the Treasury OIG, March 25, 2003.*

### **Examination of International Mail for Contraband and Revenue**

All international mail arriving for delivery in the United States and U.S. Virgin Islands is subject to Customs inspection and release. Inspection is performed at Customs International Mail Branches (IMB). The 14 IMBs are located at, or close to, United States Postal Service (USPS) facilities. Mail is examined to prevent contraband or other illegal articles from entering the U.S. and to collect revenue on dutiable items.

Customs screens the mail using visual inspection, x-ray equipment, x-ray equipment with mounted radiation detectors, personal radiation detectors, isotope identifiers, and detector dogs.

Treasury OIG found, however, that Customs cannot guarantee that all mail arriving in the U.S. is properly transported, secured, and presented to the IMBs for examination. Many IMBs have not established adequate techniques to monitor the mail prior to its presentation to Customs. Specifically, a number of the IMBs have not properly identified the vulnerabilities in the mail transportation process and worked with USPS to secure the mail during transport.

The need to examine parcels properly is also important for identifying dutiable parcels in the mail, since Customs continues to lose significant amounts of revenue. Customs often relies on values on mail declarations, which Customs found during its mail revenue survey are not always accurate. The results of Customs mail revenue survey for Fiscal Year (FY) 2001 showed that Customs continues to lose an estimated \$184 million a year based on values stated on the mail declarations, and \$494 million per year based on examination of the contents of the parcels.

Some IMBs have developed new targeting strategies using the results of the survey to detect dutiable parcels, and others are continuing to use their current methods. Because of the lack of resources, the IMBs are at a disadvantage in identifying revenue in the mail.

To correct the problems above, OIG recommended that Customs: (1) examine the transportation route of all international mail and work with Postal Service to ensure that mail is properly secured; (2) implement a plan for screening tools and detector dogs to be used at all of the IMBs that addresses the potential threats; and (3) continue to work on a strategy to increase revenue collection from the mail.

Customs concurred with the recommendations and will work with the Postal Service and other customs and postal administrations to improve mail examination procedures. *The full report, OIG-03-072, was issued by the Treasury OIG, March 27, 2003.*

### **Customs Deployment of Radiation Detection Equipment**

Customs has made progress since the terrorist attacks of September 11th in improving detection of radioactive materials that may be smuggled into the U.S. at the ports of entry. Customs has deployed, or is in process of deploying, several different radiation detection devices to the ports of entry. These devices range from personal radiation detectors, which are somewhat limited and not very costly, to more sophisticated, capable, and costly portal radiation detection systems. Customs believes that these systems are complementary, and each is thought to be as valuable in its own right in detecting radioactive materials at the ports.

Treasury OIG believes, however, that Customs' radiation detection capability has been hindered because Customs has not developed a documented strategic plan for the acquisition and deployment of radiation detection equipment. In addition, Customs has not been collecting data on the usage or performance of this equipment in detecting illegally imported radioactive materials.

Customs concurred with Treasury OIG's findings and recommendations and plans to have a draft strategic plan by September 2003. In addition, Customs is currently collecting data on significant detections made with the equipment. Audit follow-up is the responsibility of DHS OIG. *The full report, OIG-03-073, was issued by the Treasury OIG, March 27, 2003.*

### **Improved Management of Customs ACE Business Process Reengineering Needed**

The development of the Automated Commercial Environment (ACE) is a massive and multifaceted effort that is critical to the long-term success of the U.S. Customs Service mission. ACE is planned to be a customer-oriented, account-centric process that provides real time access to internal and external information through a secure global channel for travel and trade. The aim is for the federal government to provide a "single window" for the trade on border cargo regulation to reduce the complexity, redundancy, and burden on the trade. The objective of the audit was to determine whether the Customs commercial processes were appropriately reengineered prior to ACE software development.

Treasury OIG's audit concluded that Customs' efforts to define existing system requirements for its core processes (enforcement, management, import/export, and financial) were sufficient to allow the contractor to begin development of future ways of conducting business. However, they found that improved management of reengineering was needed in three areas. First, there was insufficient detail identified in the development of the different increments to allow e-Customs Partnership (eCP) to manage work and for Customs to measure the quality of contract deliverables. Second, the Customs' Modernization Office (CMO) web portal was not available to all contractor and CMO employees. Third, a multi-agency reengineering effort has not been performed to establish requirements for integrating International Trade Data System functionality into ACE.

In addition, two other issues were brought to management's attention, which were not in the audit scope. First, there were indications that improvements were necessary in the staffing, utilization and management of Customs Subject Matter Experts. Second, there were indications that the aggressive ACE

schedule was affecting the quality of work products. Treasury OIG made three recommendations to improve management of the reengineering of business processes. Customs concurred with OIG's recommendations and has initiated actions to require the contractor to prepare and maintain an Integrated Allocation Matrix; to provide Customs and contractor employees with a functional CMO Web Portal; and Customs has initiated actions to gather system requirements from other agencies participating in ACE. *The full report, OIG-03-058, was issued by the Treasury OIG, February 13, 2003.*

### **U.S. Customs Railcar Inspection Program at Port Huron, MI, Needs Further Improvement**

In response to a prior OIG audit, Customs agreed to implement changes to its rail interdiction activities along the northern border. Treasury OIG's review of the current rail inspection program in Port Huron, Michigan showed that corrective actions were implemented. However, the railcar inspection program at this major port of entry was not adequately targeting or inspecting high-risk shipments.

Customs' long-range plans are to increase significantly inspections through the use of non-intrusive inspection equipment. However, this equipment is not scheduled for deployment in Port Huron until June 2004. Interim measures need to be taken to reduce the risk of contraband entering the country through this port.

To address these issues, Treasury OIG made seven recommendations. Customs agreed with these recommendations and established target dates for completing corrective actions. Audit follow-up is the responsibility of DHS OIG. *The full report, OIG-03-071, was issued by the Treasury OIG, March 26, 2003.*

### **The INS' Primary Inspections at Air Ports of Entry**

Most arriving international passengers at air ports of entry (POE) are examined by INS inspectors at a primary inspection station. During a primary inspection, the INS inspector conducts a brief interview, examines travel and identity documentation, and checks the traveler against lookout databases. The goal of the primary inspection is to admit legitimate travelers into the United States quickly



and refer high-risk travelers and inadmissible aliens to a secondary inspection for a more detailed review.

The DOJ OIG that found the INS needs to improve its operational capability to perform passenger analyses prior to flight arrival. Additionally, the DOJ OIG found that INS' lookout system does not always provide primary inspectors with critical information known to the INS. For example, in October 2002, the INS had a backlog of more than 1,800 reports of lost or stolen passports that had not been entered in the databases used by the inspectors. The DOJ OIG also found that some passengers who were referred for secondary inspection left the airport without appearing and, further, that such incidents were not entered in the lookout systems.

The DOJ OIG also found that primary inspectors did not always query lookout databases as required and identified training deficiencies and an inexperienced inspections workforce as contributing causes. The DOJ OIG made 26 recommendations for changes to the INS operation. *The full report, 03-15, was issued by the DOJ OIG in February 2003.*

### **Follow-Up Audit of the INS' Airport Inspection Facilities**

In December 2000, the DOJ OIG found deficiencies in INS inspection facilities at 42 international airports in the United States. Airports were vulnerable to illegal entry, escapes, injuries, and the smuggling of aliens and contraband. In a follow-up audit, the DOJ OIG found that, at the 12 airports it examined, the INS took insufficient action to implement the recommendations from the prior audit. The INS failed to advise many of the airports and airport authorities of needed improvements, failed to apply sanctions against airlines that did not provide suitable inspection facilities, and did not develop a program to review and improve airport inspection facilities. All airports reviewed in this follow-up audit had repeat deficiencies. For example, some airports did not have intercoms between access control points and the command center, emergency exits with both local and central alarms, or hold rooms that could be unlocked easily during an emergency. In addition, the DOJ OIG found inspection areas that lacked adequate camera coverage, inoperable alarms, and security features that had been turned

off, were not monitored, or had not been installed. *The full report, 03-15, was issued by the Department of Justice OIG in January 2003.*

### **The Norfolk Ship Jumping Incident**

The DOJ OIG examined the actions of INS employees in connection with a “ship jumping” incident. When a Russian cargo ship docked in Norfolk, Virginia, four of the 27 crewmen failed to return to the ship prior to its departure on March 18, 2002. The four deserters, referred to as “ship jumpers,” were from Pakistan. Generally, each crewmember is required to have an individual visa, and a waiver of this requirement was subject to a tightened authorization process that the INS had promulgated in November 2001. In the Norfolk incident, however, the waiver was granted by a subordinate official who was no longer authorized to do so.

The DOJ OIG found that the Norfolk immigration inspectors had not been informed of the INS policy change, primarily due to inaction by the INS Washington District Office and, to a lesser extent, the INS Norfolk Office. The DOJ OIG concluded that the Norfolk incident highlighted a longstanding problem in the INS that its Office of Internal Audit had documented two years earlier – that INS policies and changes in policy are not distributed to INS field offices and employees in a uniform or effective way. *The full special report was issued by the Department of Justice OIG in December 2002.*

### **Protecting The Public: Security, Inspection, and Targeting of Vessel Containers at the Ports of New York and Newark Can Be Improved**

The concern that weapons of mass destruction and other contraband or implements of terrorism can enter our country through our seaports has been the subject of much discussion and action by various federal agencies, national media sources, and congressional committees. Millions of vessel containers enter this country every year at the nation’s seaports carrying legitimate cargo. However, it is recognized that due to their sheer numbers and the effort that must be expended to inspect these containers, they are highly vulnerable to exploitation by terrorists. The Treasury OIG recently issued a report focused on our enforcement efforts at the combined Ports of New York and Newark. The objective of the audit was

to determine whether Customs targets, secures, and inspects vessel containers to prevent the smuggling of implements of terrorism, drugs, and other contraband in an effective manner.

The Port of New York/Newark is the largest port complex on the east coast and it processed approximately 800,000 inbound containers between April 2001 and March 2002. To manage the mission during this period, the number of inspectors assigned to Contraband Enforcement Team (CET) ranged between 63 and 71, with approximately seven inspectors assigned to the Advanced Targeting Unit, whose responsibility is to target high-risk cargo for examination. The primary mission of the CET is to target and inspect high-risk cargo and conveyances for implements of terrorism and narcotics.

Treasury OIG determined that Customs management had not implemented oversight procedures to ensure that the security of vessel containers and certain aspects of physical security over the containers would be improved. OIG also reported that the inspection process for vessel containers could be improved in the areas of non-intrusive inspection, timeliness, and examination data recording and reporting. Finally, OIG discussed certain concerns related to the targeting efforts and potential areas for improvement. OIG made nine recommendations with which Customs concurred. Customs port management initiated immediate corrective actions to improve conditions at the port. This report was one of a series of reports initiated by the Treasury OIG last year. *The full report, OIG-03-066, was issued by the Treasury OIG, March 20, 2003.*

## **Follow-up Review on the Status of SEVIS Implementation**

This review assessed the INS' progress in implementing the Student and Exchange Visitor Information System (SEVIS) since issuance of the DOJ OIG's May 2002 report, *The Immigration and Naturalization Service's Contacts With Two September 11 Terrorists: A Review of the INS' Admissions of Mohamed Atta and Marwan Alshehhi, its Processing of their Change of Status Applications, and its Efforts to Track Foreign Students in the United States*. The DOJ OIG found that the INS has made progress in implementing SEVIS to track foreign students. However, the reviewers found continued problems with the INS' certification of schools to accept foreign students, training of contractors and INS personnel, oversight of contractors conducting school site visits, oversight of schools' compliance with SEVIS requirements, procedures for identifying and referring potential instances of student or school fraud, and resource levels for investigating potential fraud. The DOJ OIG concluded that the INS had not fully implemented SEVIS by January 1, 2003, the congressionally mandated deadline. *The full report, I-2003-003, was issued by the DOJ OIG in March 2003.*

## **The INS' Removal of Aliens Issued Final Orders**

The DOJ OIG conducted a review to follow up on a 1996 report that assessed the INS' effectiveness in removing aliens with final orders. It found that the INS remains successful at removing detained aliens, but is unsuccessful at removing non-detained aliens. Detained aliens are currently removed at a rate of 92 percent, while non-detained aliens are currently removed at a rate of 13 percent. These removal rates are similar to those found in 1996. Further, the DOJ OIG examined the removal rate of several high-risk subgroups of non-detained aliens under final orders of removal. The INS removed 35 percent of aliens with criminal records, six percent of aliens from countries identified by the State Department as sponsors of terrorism, and three percent of aliens denied asylum. The DOJ OIG concluded that the INS was unsuccessful at removing non-detained aliens, and that it had failed to implement the corrective actions recommended in the OIG's 1996 report. *The full report, I-2003-004, was issued by the DOJ OIG in February 2003.*

## Emergency Preparedness and Response

- **Benson County, North Dakota**

The county received an award of \$1.49 million from the North Dakota Division of Emergency Management for damages caused by flooding and ground saturation. The county's claim included questioned costs of \$111,844, consisting of uncompleted projects and uncompleted scopes of work. The OIG recommended that the Regional Director disallow the questioned costs. *The report, DD-01-03, was issued by the Department of Homeland Security OIG on March 28, 2003.*

The Federal Emergency Management Agency issued its final Semiannual Report reflecting the period October 1, 2002 – February 28, 2003.

## Information Analysis and Infrastructure Protection

- There was no legacy OIG work relevant to this directorate.

## Science and Technology

- There was no legacy OIG work relevant to this directorate.

## Management

- There was no legacy OIG work relevant to this directorate.

# Coast Guard

## **Coast Guard's Actuarial Estimates for Retired Pay and Medical Benefits**

DOT OIG released a study conducted by the Hay Group, which concluded that the Coast Guard properly reported \$29 billion in military retirement liabilities as of September 30, 2002. The study also reported that the liabilities and annual actuarial activity of the Coast Guard's military retirement system were reasonable and reliable as of September 30, 2001, thereby satisfying the principal objective of the study. FY 2001 data were used because they were the most recent year for which data was available. The study is part of DOT OIG audit of the DOT FY 2002 Consolidated Financial Statements. *The full report was issued by the DOT OIG, January 22, 2003. (Report number was not available at the time of distribution.)*

## **Computer Security and Controls of U.S. Coast Guard's Aircraft Repair and Supply Center**

DOT OIG publicly released its audit report on computer security and controls at the U.S. Coast Guard's Aircraft Repair and Supply Center in Elizabeth City, NC. DOT OIG found the center needs to: (1) establish a disaster recovery and business continuity plan; (2) strengthen security governing access to its computer systems and the physical complex; (3) strengthen its process for controlling changes to production systems; and (4) enhance security administration, including background checks on key personnel. DOT OIG identified five priority actions the Coast Guard should take and asked the Coast Guard to provide its action plan and estimated dates for resolving the action items to the DHS OIG. The audit was conducted by PricewaterhouseCoopers LLP. *The full report, FI-2003-022, issued by the DOT OIG, February 25, 2003.*

# Secret Service

## **Controls Over Secret Service's Law Enforcement Data Need Improvement**

The use of law enforcement data is vital to the missions of several Treasury bureaus, including the Secret Service, now a part of the Department of Homeland Security. The Secret Service had not established adequate controls to ensure the security and integrity of its law enforcement data. For example, the Secret Service did not: (1) certify and accredit business applications used to access law enforcement data; (2) implement access control software parameters; (3) properly restrict access to law enforcement data; and (4) perform a comprehensive analysis of audit trail activity.

In addition, the Secret Service did not document its continuity of operations process for law enforcement data. Consistent with prior findings, weaknesses associated with the Secret Service's ability to establish and formalize a change management process still existed, particularly for changes made to law enforcement databases.

Treasury OIG recommended that the Director of the Secret Service ensure that individual security plans, risk assessments, and system certifications and accreditations are completed for two business applications used to access law enforcement database information; access control software settings be revised; and user access to law enforcement data be controlled. Treasury OIG also recommended that the Secret Service develop a policy and standard operating procedures for operating system and database audit trails; correct a problem that prohibits the generation of database activity logs; and revise the procedure for reporting computer security incidents and vulnerabilities. Finally, Treasury OIG noted that printed material should be properly safeguarded, and the Continuity of Operations Plan be documented, tested, and a copy be stored off-site. Management agreed with the recommendations. *The full report, OIG-03-002, was issued by the Treasury OIG, October 2, 2002.*

# Bureau of Citizenship and Immigration Service

## **The INS' Premium Processing Program**

The Premium Processing Program was established in June 2001 to allow certain employment based immigration applications to be processed expeditiously for an additional payment of \$1,000. Although the immediate goal of Premium Processing is to expedite premium petitions, the long-term objective is to reduce or eliminate backlogs in the INS' total adjudications workload. The DOJ OIG's audit concluded that the Premium Processing program has lengthened the time required to adjudicate routine applications and petitions and that the backlog of routine petitions at INS service centers has increased steadily, reaching 3.2 million in September 2002.

The DOJ OIG also found that, though the INS mandated checks against the Interagency Border Inspection System (IBIS) database on all petition types starting on January 28, 2002, the service centers did not comply promptly. As a result, 11,830 Premium Processing petitions were adjudicated without IBIS checks between January 28, 2002, and March 18, 2002. (An IBIS check is a search of criminal history and national security lookout databases.) Finally, the DOJ OIG reported that the INS lacks reliable data about the Premium Processing workload and the resources it requires. *The full report, 03-24, was issued by the DOJ OIG in February 2003.*

## **The INS' Ability to Provide Alien Information to the Social Security Administration**

The DOJ OIG assessed whether the INS timely posts information about aliens in the INS databases that it shares with the Social Security Administration (SSA). The SSA uses the databases to issue Social Security numbers to aliens. The OIG examined two systems used by the INS to provide the SSA with aliens' immigration status: (1) Immigrant Visa DataShare (DataShare); and (2) the Nonimmigrant Information System (NIIS).

The INS estimated that the entire process of uploading nonimmigrant information into NIIS and making it available to the SSA should take approximately 11 to 13 workdays. The DOJ OIG endorsed the INS' estimate as reasonable. The OIG



also concluded that the INS is prepared to implement the enumeration phase of the DataShare process and provide the SSA immigrant status using DataShare. *The full report, I-2003-001, was issued by the DOJ OIG in November 2002.*

# Investigation Statistics

The following information is a summary of the investigative activity performed by the legacy Offices of Investigations. Investigative activity that is not relevant to DHS is not included.

## **Department of Homeland Security, Office of Investigations**

*(Legacy Agency FEMA Statistics)<sup>2</sup>*

**March 1, 2003 – March 31, 2003**

Funds Recovered (Investigative Recoveries)	\$18,300
Fines and Restitutions	\$4,031,573
Administrative Cost Savings and Recoveries	\$0
Investigative Cases Opened	28
Investigative Cases Closed	27
Arrests	13
Indictments	19
Convictions	19
Personnel Actions	2
Complaints Received	347
Hotline Complaints Received	169
Complaints Referred (to program or other agencies)	8

<sup>2</sup> The complete investigative statistics for this six month reporting period for FEMA OIG are contained in the final FEMA OIG report referenced earlier.

**Transportation Security Administration and U.S. Coast Guard Semiannual Statistics.** These statistics reflect work of the DOT Office of Inspector General for the reporting period October 1, 2002 through February 28, 2003. The Coast Guard statistics involved cases of contract and grant fraud and employee integrity. The TSA statistics are from airport security sweeps conducted by DOT OIG and other federal and local officials, including the FBI, SSA OIG, INS, Customs Service, local law enforcement, and airport law enforcement officials.

Indictments	228 (224 TSA, 4 CG)
Convictions	220 (214 TSA, 6 CG)
Jail (Months)	298 (286 TSA, 12 CG)
Probation (Months)	1206 (1122 TSA, 84 CG)
Recoveries	\$56,541 (\$8,535 TSA, \$48,006 CG)
Referred for Prosecution	289 (264 TSA, 25 CG)
Accepted	288 (264 TSA, 24 CG)
Declined	1 (1 CG)
Pending	1 (1 CG)

**Treasury OIG Statistics  
March 1, 2003 – March 31, 2003**

OIG Activity	Number / \$ Amount
Reports Issued & Oversight Reviews (Investigations)	10
Monetary Benefits (Investigations)	
a) Fines/Restitutions	0
b) Recoveries	0

(We were not able to obtain Treasury OIG's investigation statistics for the rest of this period.)

# Investigation Narratives

## **Department of Homeland Security, Office of Investigations**

*(Legacy Agency FEMA)*

### **FEMA Program Fraud**

A DHS OIG investigation determined that the owner of a company that provided bomb detection dogs in support of the World Trade Center investigation overcharged for services and defrauded the Federal Emergency Management Agency of the Emergency Preparedness and Response directorate of \$11,000 in disaster assistance funds. A joint investigation by the Treasury Inspector General for Tax Administration, the Federal Reserve Office of Inspector General, and the State Department Office of Inspector General determined that the subject also committed similar contractual violations at those respective agencies, totaling approximately \$700,000 in fraud losses. On March 13, 2003, the individual was indicted in U.S. District Court on 26 counts of 18 USC 1343 (wire fraud) and two counts of 18 USC 287 (false claims). The subject was arrested pursuant to a federal arrest warrant and will stand trial on May 14, 2003.

### **Department of Transportation**

The following material reflects the work of the Department of Transportation Office of Inspector General between October 1, 2002 and February 28, 2003.

#### **7 Arrested in Security Sweep at Detroit Metropolitan Airport**

In October 2002, arrest warrants were issued for seven people charged with making false statements or misusing a social security number in order to obtain employment at the Detroit Metropolitan Airport. OIG special agents participated in the arrests. OIG participated in the arrest of 618 people and the indictment of 781 people (including those arrested) in 22 operations at 27 airports since September 11, 2001.

#### **Airport Sweep Update**

In October 2002, two former checkpoint security screeners at Logan International Airport, Boston, MA, pleaded guilty in U.S. District Court in Boston to falsifying

their applications for an airport security badge. An illegal foreign national pleaded guilty to falsifying his eligibility to work in the United States. Separately, another foreign national also pleaded guilty to making false statements on a security badge application about his work eligibility, as well as using a fictitious alien registration card and a social security number that was not his. Both men were scheduled for sentencing in January 2003.

### **Former Security Guard Sentenced for Misusing DOT ID**

A foreign national was fined \$2,500 and placed on six years probation by a U.S. District Court judge in Concord, NH in October 2002, after pleading guilty to misusing official identification. A former contract security guard at Volpe National Transportation Systems Center in Cambridge, MA, he failed to surrender his Transportation Department identification when he resigned in 1999. During a routine traffic stop in May 2002, he displayed the ID and a constable's badge to Portsmouth, NH police and falsely identified himself as a Transportation Department law enforcement officer. The Volpe Center is implementing measures to prevent similar incidents. The case was investigated by the OIG with assistance from local police.

### **Airport Sweep Update**

A former baggage handler at Miami International Airport (MIA) was sentenced in U.S. District Court in Miami to a \$1,000 fine, two months in prison, three years' supervised release, and 750 hours of community service. He was convicted in October 2002 by a federal jury in Miami for using a fraudulent social security number. He and 16 other employees were charged in September, 2002 with various federal crimes involving their access to secure areas of MIA. The investigation was conducted by OIG, Customs Service, SSA, and INS.

A checkpoint security screener was sentenced in October 2002 in U.S. District Court in Boston, MA to 14 days time served in jail and one year's probation after pleading guilty to falsifying his application for a security badge at Logan International Airport in Boston. He was charged with lying about his alien registration status and altering an alien registration card. He had been living and

working illegally in the U.S. since 1998. He is one of 20 charged in a security sweep at Logan.

### **Twenty-Nine People Arrested in Philadelphia Airport Sweep**

In November of 2002, the indictments of 29 current or former workers at Philadelphia International Airport were made public and 13 people arrested in the latest investigation of security at the nation's airports. Of those indicted, 17 people employed in various positions at the airport, such as ramp agents, baggage handler, maintenance, food service and skycaps, were charged with failure to disclose prior convictions. One of these 17 defendants had in his possession at the time of his arrest two firearms that had been stolen from two law enforcement officers' luggage checked at the Philadelphia International Airport. After his arrest, he was additionally charged with possession of firearms by a convicted felon. In addition, 12 food service employees were charged with false use of a Social Security number.

### **21 Newark Airport Employees Charged, 11 Arrested in Latest Sweep**

In November 2002, eleven workers at Newark (NJ) Liberty International Airport were arrested and 10 others were being sought in the latest airport security sweep. All 21 were charged with using false identification to get jobs at the airport that gave them access to high-security areas. The employees, all of whom worked for private contractors in cleaning and security jobs, had access to restricted areas around aircraft and in and around baggage handling facilities. The defendants were charged with Social Security fraud, document fraud, or making false statements on their application for a security badge. The investigation was conducted by OIG, the FBI, INS, SSA OIG, Customs Service, U.S. Marshals, police with the Port Authority of New York and New Jersey, and local law enforcement.

### **127 Charged at JFK and LaGuardia Airports**

In November 2002, federal authorities arrested or obtained warrants for the arrests of a total of 127 current or former employees at John F. Kennedy International

Airport and LaGuardia Airport in New York City in an airport security sweep. Indictments ranged from using false social security numbers and providing false information on their immigration status to failing to disclose criminal histories on their applications for airport security badges. The defendants held a variety of jobs, including passenger service agent, ramp and cargo agents, janitorial workers, and utility and maintenance workers. The operation was conducted by OIG, the FBI, INS, U.S. Customs Service, SSA OIG, the Secret Service, and local authorities.

### **60 Arrested at Dallas/Fort Worth International Airport**

In November 2002, 60 employees at Dallas/Fort Worth International Airport were arrested for using bogus social security numbers to gain employment giving them access to secure and restricted areas of the airport. A total of 99 defendants were charged by criminal complaints. Those arrested included baggage handlers, ramp workers, cargo agents, and food service and custodial workers. The investigation was conducted by DOT OIG, the FBI, INS, Social Security Administration OIG, U.S. Marshals Service, the Texas Rangers, and the airport's Department of Public Safety.

### **Connecticut Airport Checkpoint Screener Arrested for Concealing Criminal History**

In December 2002, a security checkpoint screener at Bradley International Airport in Windsor Locks, CT, was arrested for concealing his criminal record on his employment application with the TSA. He had three previous arrests and four convictions, including sexual assault, "threatening," and breach of peace. The investigation was conducted jointly by OIG and the SSA OIG, with assistance from TSA.

### **Airport Sweep Update**

In January 2003, a former checkpoint security screener at Boston's Logan International Airport was sentenced in U.S. District Court in Boston for making false statements and using a false Social Security number and alien registration

card on his application for a security badge. He was sentenced to three years probation and is subject to deportation. This prosecution is one of 20 resulting from a joint airport security sweep by DOT OIG, SSA OIG, and INS.

A former passenger services agent at Miami International Airport pleaded guilty in January in U. S. District Court in Miami to providing a false Social Security number on an application for a security badge. She and seven other airport workers were arrested in September 2002 for various federal crimes involving their access to secure and sterile areas of the airport. To date, seven defendants have been convicted. The remaining defendants are to be tried in the near future.

#### **Ten Contract Workers Arrested for Concealing Disqualifying Backgrounds**

Ten contract employees in Stratford, CT, were arrested in January 2003 for lying about their criminal history, identity, or immigration status on their background applications. Because the company is a federal contractor with access to classified information, its employees must complete background applications. The employees worked for one of four contractors that provide a variety of services, including maintenance. Each had an electronic “key” card giving them access to the facility. The company manufactures and supplies replacement parts for the Coast Guard’s H.60 *Jayhawk* helicopter, used in search and rescue operations and offshore law enforcement and drug interdiction. This ongoing investigation was conducted by OIG and the Defense Criminal Investigative Service, with assistance from the SSA OIG, and INS.

#### **Flight School Owner Jailed for Four Years for Wide-Ranging Fraud**

In January 2003, the owner and president of a flight school, was sentenced in U.S. District Court, Central Islip, NY, to 44 months in jail and \$26,056 in restitution. In July 2002, a foreign national pleaded guilty to representing himself falsely as a certified flight instructor for instrument training and a U.S. citizen on Federal Aviation Administration (FAA) forms. He also pleaded guilty to wire fraud relating to an insurance claim for a plane that crashed prior to being insured and to access device fraud for unauthorized use of credit card account numbers to



obtain aircraft equipment, aviation fuel, and computer products. The case was investigated by OIG and the FBI with assistance from FAA.

### **15 Employees Arrested in Austin-Bergstrom International Airport Security Sweep**

An airport security sweep at Austin-Bergstrom International Airport in Texas resulted in the arrests of 15 employees in January 2003, on federal charges of misuse of a Social Security number and making false statements and providing false immigration information on airport security badge applications. Six other workers were arrested on state charges of tampering with a government record in connection with their airport security badge applications. This was a multiagency operation involving OIG, the FBI, Treasury OIG for Tax Administration, U.S. Postal Inspection Service, the Customs Service, the Secret Service, the Austin Airport Police, and the Austin Police Department.

### **Foreign National Sentenced for Falsifying Airman's Medical Applications**

A student enrolled in a pilot training program at a flight school, was sentenced in U.S. District Court in January 2003, in Orlando, FL, to two years probation and fined \$400 for falsely claiming U.S. citizenship and failing to disclose a past DUI charge on three airman's medical applications. He was taken into INS custody and is being detained pending the results of a deportation proceeding.

### **Fifth Defendant in Airport Baggage Theft Case Pleads Guilty**

In February 2003, an agent contracted to load and unload passengers' luggage and belongings, pleaded guilty in U.S. District Court in Miami to using his airport security badge to steal items from the luggage of passengers at Miami International Airport. He was one of six defendants arrested by OIG, Customs Service, and the Miami-Dade Police Department on December 11, 2002. Five defendants have pleaded guilty, and the remaining defendant was scheduled for trial February 24.

### **Airport Worker Pleads Guilty to Airport Security Badge Fraud**

In February 2003, an employee at the Long Island MacArthur Airport in New York pleaded guilty in U.S. District Court in Central Islip, NY, for failure to disclose a felony conviction for robbery on his application for a security badge. As the employee, he performed and certified the required background checks of other employees. This case was investigated by OIG, with TSA's assistance.

### **Airport Security Sweep Update**

Following up on the January security sweep at the Austin-Bergstrom International Airport in Texas, 19 former airport employees were sentenced on February 20 in U.S. District Court or Travis County (state) Court in Austin to time served and deported. After pleading guilty to federal charges of providing false statements to FAA or to state charges of tampering with government documents, all were placed on unsupervised probation, which means re-entry into the United States can be considered a violation of probation. During the sweep, 53 people were charged with allegedly falsifying information on their airport security badge applications. Of these, 29 are fugitives and five have pleaded not guilty and await trials. OIG conducted this investigation with the FBI, INS, SSA OIG, Treasury OIG for Tax Administration, and state and local authorities.

A carpenter for a private corporation doing renovation work at the Miami International Airport pleaded guilty in February 2003 in U.S. District Court in Miami, to making false statements on her application for an airport security badge by using a false Social Security number. She is the ninth defendant to plead guilty among 17 former employees netted during a September 2002 security sweep. A sentencing date has not been scheduled. This investigation was conducted by OIG, the Customs Service, SSA OIG and INS.

### **Sixth Defendant in Airport Baggage Theft Case Pleads Guilty**

In February 2003, the last of six defendants charged with conspiracy to use his airport security badge to steal items from the luggage of British Airways passengers pleaded guilty in U.S. District Court in Miami. The defendants were

employees of an airport contractor that loaded and unloaded luggage for British Airways at Miami International Airport. He is scheduled for sentencing on April 30. The other five defendants will be sentenced on April 11. OIG conducted the investigation with the Miami-Dade Police Department, the Customs Service, and British Airways.

### **Airport Security Sweep Update**

In February 2003, a cargo handler at Philadelphia International Airport, was sentenced in U.S. District Court in Philadelphia after pleading guilty to lying about a felony conviction on his security badge application. He was sentenced to 24 months' probation. He is the 15th defendant to plead guilty of 29 former workers netted during a November 2002 security sweep at the airport. The investigation was conducted by OIGs from DOT, the Department of Labor, the SSA, the FBI, the Customs Service, and INS.

### **Department Of Justice**

As of October 1, 2002, the DOJ OIG had 172 cases in an open status and had opened an additional 79 investigations through March 1, 2003. The criminal investigations cover a wide range of offenses, including INS document fraud, bribery of a public official, alien and drug smuggling, and theft of government funds. The administrative investigations include serious allegations of misconduct, including allegations against high-level employees. Following are some of the cases investigated during this reporting period.

### **Sham Marriage Scheme Exposed**

An INS adjudications officer assigned to the Miami District Office and a civilian were arrested in connection with the arrangement of sham marriages for the purpose of obtaining resident alien cards. An investigation by the DOJ OIG Miami field office led to a criminal complaint alleging that the civilian paid \$3,000 to the adjudications officer and \$3,000 to the sham spouse to perpetuate the scheme. Subsequently, the adjudications officer would approve the applications for adjustment of status to legal permanent resident and then

stamp the respective passports and I-94 forms (Record of Arrival and Departure) to reflect legal permanent residency when, in fact, the persons were not legal permanent residents. Judicial proceedings continue.

### **Theft Of Government Funds**

An INS information officer assigned to the INS' Newark District Office was arrested and pleaded guilty to criminal information charging him with theft of government funds. A joint investigation by the New York field office and the U.S. Attorney's Office for the District of New Jersey identified 49 immigration cases in which the information officer stole money orders worth more than \$15,000 sent by aliens to pay immigration application fees. Sentencing is pending.

### **Contract Employees Destroy INS Documents**

Two INS contract employees were arrested on charges of willfully destroying documents that had been filed with the INS. The contract employees were assigned to the INS Service Center in Laguna Niguel, California, and were responsible for processing incoming INS mail. One served as the assistant manager in charge of the file room and the other was the file room's senior supervisor. A joint investigation by the Los Angeles field office and the INS developed evidence that in January 2002 the assistant manager ordered the senior supervisor and other file room supervisors to shred approximately 90,000 unprocessed file room documents. By late March 2002, the backlog was eliminated; however, the assistant manager instructed the senior supervisor and other employees to continue shredding incoming unprocessed documents to prevent any further backlog. The types of documents shredded include U.S. and foreign passports, birth and marriage certificates, and INS applications and notices. Judicial proceedings are pending.

### **Employment Authorization Document Scheme**

An INS supervisory immigration inspector, an immigration consultant, and five civilian co-conspirators were arrested pursuant to a criminal complaint and immigration warrants in the Southern District of California for conspiracy to

commit fraud; manufacture and misuse of visas, permits, and other documents; and reentry after deportation. A joint investigation by the El Centro Area Office, INS, FBI, USAO, and Department of State developed information that the immigration consultant and co-conspirators obtained employment authorization documents for their clients by submitting false information and other fraudulent documents with their applications. The investigation disclosed that the supervisory immigration inspector, who is assigned to the Calexico, California, port of entry, assisted the immigration consultant by falsely submitting cancellation of removal documents for aliens who were not eligible to receive them. Aliens paid from \$3,000 to \$14,000 for these services. Judicial proceedings continue.

### **Special Report On Travel Voucher Abuse**

On January 8, 2003, the DOJ OIG released a special report on travel voucher abuse by INS Border Patrol agents detailed to assist “Operation Safeguard,” an extensive border enforcement initiative, in Tucson, Arizona. The investigation found that some Border Patrol agents falsified the amount of rent they paid and accepted amenities or cash rebates from lodging providers without reducing their claims for reimbursement. Further, the OIG found that supervisory Border Patrol agents improperly rented rooms to subordinate agents and in some cases provided the agents with falsely inflated receipts. The DOJ OIG report made several recommendations to the INS for reducing the abuse of travel reimbursements in connection with long-term details.

### **Treasury, Customs and Secret Service**

#### **Deli Owner Indicted on Bank Fraud-Update**

On July 19, 2002, as a result of a joint investigation by the Office of Investigations, the Department of Labor and the United States Secret Service, a Philadelphia, PA, deli owner was indicted on one count of bank fraud involving forged U.S. Treasury checks, totaling \$140,053, from the Philadelphia Financial Management Center. On January 15, 2003, the deli owner entered a plea of

guilty to conversion of government property, and aiding and abetting. Sentencing was scheduled for April 15, 2003.

### **U.S. Customs Officials Identified Mislabeled Korean Auto Parts**

An investigation conducted by the Office of Investigations focused on the detection and interception of a shipment of mislabeled auto parts being shipped from a Canadian contractor to a U.S. contractor. It was determined that the Canadian contractor had re-labeled parts manufactured in Korea to indicate Canadian origin, and that the U.S. contractor underpaid approximately \$4,708 in duties. As a result of the investigation, the U.S. contractor subsequently paid the additional duties in the amount of \$4,708.

### **Three U.S. Customs Senior Managers Disciplined For Failing To Follow U.S. Customs' Policy**

An Office of Investigations investigation disclosed that a Group Supervisor, a Resident Agent in Charge, and the Special Agent in Charge of the Office of Investigations, the Customs Service, failed to notify the Customs Office of Internal Affairs, as required by Customs' policy, that four OIG Special Agents traveled in government owned vehicles to a restaurant/bar to consume alcoholic beverages after completing a surveillance operation. As previously reported, three of the agents admitted to driving their government vehicles and storing their government issued firearms in the trunk of the government vehicle after consuming alcoholic beverages, in violation of Customs' policy. The fourth agent, who was a passenger, also admitted to consuming alcoholic beverages.

The Group Supervisor was suspended without pay for ten days, the Resident Agent in Charge resigned in advance of proposed disciplinary action, and the Special Agent in Charge was suspended without pay for 15 days.

### **Additional Information and Copies**

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at [www.dhs.gov](http://www.dhs.gov).

### **OIG Hotline**

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.