DEPARTMENT OF HOMELAND SECURITY

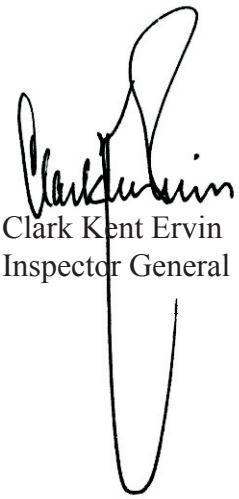
Office of Inspector General

Fiscal Year 2004
Annual Performance Plan

A Message From the Inspector General

I am pleased to present the Fiscal Year (FY) 2004 Annual Performance Plan of the Department of Homeland Security's (DHS) Office of Inspector General (OIG), outlining the projects that we intend to undertake this fiscal year to evaluate the department's programs and operations. Although this is our second such plan, it represents our first plan covering a full twelve-month operating period, because DHS itself and DHS OIG were fully operational for only part of last fiscal year.

In developing this plan, we attempted to address the interests and concerns of DHS senior management officials, the Congress, the Office of Management and Budget (OMB), and OIG itself. We focused on our core mission of conducting independent and objective inspections, audits, and investigations to promote effectiveness, efficiency, and economy in the department's programs and operations, and to prevent and detect fraud, waste, abuse, and mismanagement.



Clark Kent Ervin
Inspector General

Table of Contents

Chapter 1 - OIG Mission and Responsibilities

The Homeland Security Act of 2002 provided for the establishment of an OIG in DHS to ensure independent and objective audits, inspections, and investigations of the operations of DHS.

An Inspector General is appointed by the President, confirmed by the Senate, and reports directly to both the Secretary and the Congress. Barring narrow and exceptional circumstances, the Inspector General may inspect, audit, and investigate anyone in the department or any program or operation of the department that he chooses. Further to assure the Inspector General's independence, the OIG has its own budget, contracting, and personnel authority separate from that of the department. Such authority enhances the OIG's ability to pursue fraud, waste, abuse, and mismanagement aggressively and to provide objective and credible assessments of DHS to the Secretary, the Congress and the American people.

Specifically, the OIG's key legislated responsibilities are to:

1. Conduct audits, inspections, and such other reviews as may be appropriate to prevent and detect fraud, waste, and abuse in department operations, including the department's business transactions with its external partners – its contractors, suppliers, and grant recipients.
2. Investigate potential criminal behavior and serious misconduct by department employees, contractors, and grantees.
3. Keep the Secretary and Congress fully and currently informed about problems and deficiencies in department programs, and monitor the completion of corrective actions that respond to OIG recommendations.
4. Fulfill statutory responsibilities for the annual audits of the department's financial statements and the security of its information technology.
5. Review and make recommendations regarding existing and proposed legislation and regulations regarding department programs and operations.

Chapter 2 - OIG Organizational Structure

The OIG consists of the following components:

Executive Office: The office consists of the Inspector General, the Deputy Inspector General, and support staff. It provides executive leadership to the OIG. This office has seven employee slots.

Office of Counsel to the Inspector General: The Office of Counsel to the Inspector General provides legal advice to the Inspector General; supports audits, inspections, and investigations by ensuring that applicable laws and regulations are followed; is the OIG's designated ethics office; manages the OIG's Freedom of Information Act and Privacy Act responsibilities; and furnishes attorney services for the issuance and enforcement of IG subpoenas, False Claims Act and Civil Money Penalty Act claims, and suspension and debarment actions. The office has ten employee slots.

Office of Audits: The Office of Audits provides in depth and formal reviews of DHS programs and operations. In addition, the Office of Audits overseas the annual audit of the DHS financial statement. It also performs grant reviews. It has eight large field offices and seven smaller offices and a total of 218 employee slots.

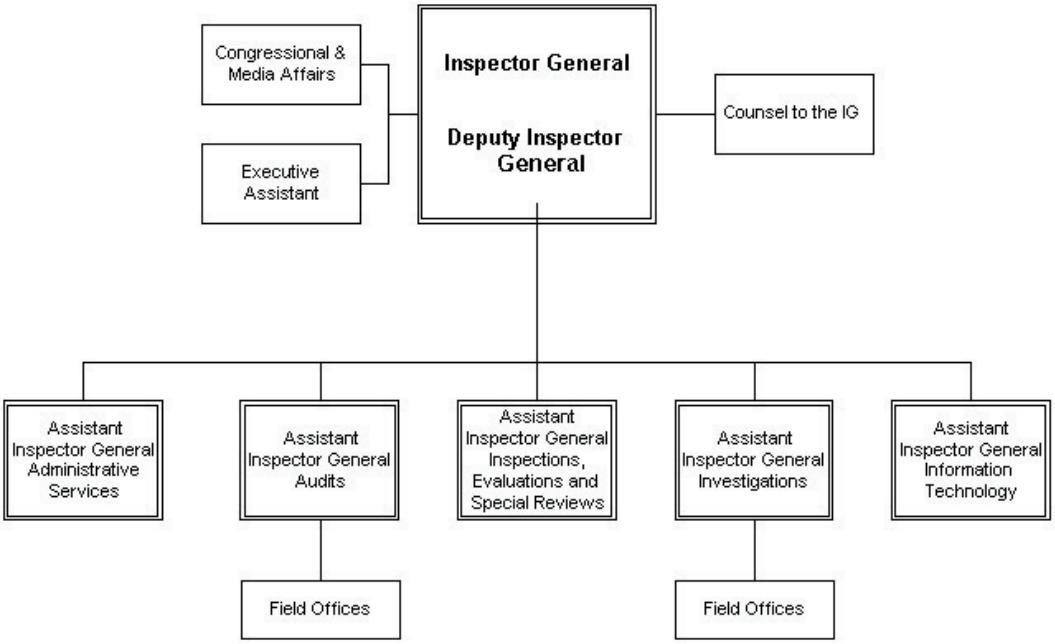
Office of Inspections, Evaluations, and Special Reviews: The Office of Inspections, Evaluations, and Special Reviews complements the work of the office of Audits by providing quick and less structured reviews of those DHS programs and operations that are of pressing interest to department managers, the Congress, or the Inspector General. This office has 24 employee slots.

Office of Information Technology: The Office of Information Technology evaluates DHS's information management, cyber-infrastructure protection, and systems integration activities. The office also assesses DHS' information security program as mandated by the Federal Information Security Management Act. This office has 25 employee slots.

Office of Investigations: The Office of Investigations investigates alleged criminal conduct on the part of department employees, contractors and grantees,

as well as serious allegations of non-criminal misconduct. It also supervises the investigative activity of the department's various internal affairs offices. This office has 141 employee slots.

Office of Administrative Services: The Office of Administrative Services provides critical administrative support functions including: OIG strategic planning; development and implementation of administrative directives; the OIG's information and office automation systems; budget formulation and execution; and oversight of the personnel, procurement, travel and accounting services provided to the OIG, on a reimbursable basis, by the Bureau of Public Debt. The Office also prepares the OIG's Annual Performance Plans and the Semiannual Reports to the Congress. This office has 32 employee slots.



Chapter 3 - Fiscal Year 2004 Planning Approach

The Annual Performance Plan is the OIG's "roadmap" for the inspections and audits it plans to conduct each year to evaluate department programs and operations. In devising the plan, OIG endeavors to assess the department's progress in meeting what we consider to be its major management challenges.

This plan describes more projects than may be completed in FY 04, especially since we anticipate that developments and requests from DHS management and Congress during the year will necessitate our undertaking some projects that we cannot anticipate now. Resource issues too may require us to vary the plan in some way as the year progresses. Finally, the plan contemplates that some jobs listed here will start during FY 04 but will carry over into FY 05.

In establishing priorities, the OIG placed particular emphasis on legislative mandates, such as the Chief Financial Officer's Act and the Federal Information Security Management Act, DHS' strategic objectives, the President's Management Agenda, the Secretary's priorities, Congressional priorities, and the most serious management challenges facing DHS.

DHS' strategic objectives include:

- Prevent terrorism within the United States
  - Intelligence and Warning
  - Border and Transportation Security
  - Domestic Counterterrorism
- Reduce vulnerability of the United States to terrorism
  - Protecting Critical Infrastructure and Key Assets
  - Defending against Catastrophic Threats
- Minimize damage, and assist in the recovery from terrorist attacks that do occur in the United States
  - Emergency Preparedness and Response
- Carry-out Non-Homeland Security Functions

The President's Management Agenda addresses the following:

- Strategic Management of Human Capital

- Competitive Sourcing
- Improve Financial Performance
- Expanded Electronic Government
- Budget and Performance Integration

The OIG identified the following as the most serious management challenges facing DHS:

- Consolidating the department's components
- Border Security
- Transportation Security
- Integration of Information
- Security of Information Technology
- Human Capital Management
- Financial Management
- Contract Management
- Grants Management

In addition, keeping with the priorities of both the Secretary and Congress, the OIG will focus attention on DHS' "non-homeland" missions. Particular attention will be given to the Coast's Guard's "non-homeland" mission, as mandated by the Homeland Security Act, and to disaster response and recovery activities.

These programs and functions are not an all-inclusive inventory of DHS' activities. Rather they represent those activities that are the core of DHS' mission and strategic objectives. By answering certain fundamental questions within each of these program and functional areas, the OIG will determine how well DHS is performing and will be able to recommend ways for improving the efficacy of DHS' programs and operations.

The OIG will strive to have a close, consultative, and collaborative working relationship with the senior management of DHS. That said, the role of the OIG will be one of independence and objectivity, providing, where such criticism is warranted by the facts, constructive criticism of DHS' programs and operations.

Chapter 4 - Allocation of Resources

On October 1, 2003, President Bush signed the first appropriation bill for DHS. The FY 2004 appropriation provides the DHS OIG with total budget authority of $80,318,000 and a total of 457 employee slots. The funding will support the annualized costs of the personnel and obligations transferred in FY 2003, along with increases in payroll and benefit costs.

STANDARD CLASSIFICATION SCHEDULE
Direct Obligations
(Dollars in Thousands)

Object Class	FY 2003 Estimate	FY 2004 Proposed Operating Level	Variance
Personnel compensation:			
Permanent positions	31,625	39,095	7,470
Positions other than permanent	375	237	(138)
Other personnel compensation	2,000	453	(1,547)
Total personnel compensation	**34,000**	**39,785**	**5,785**
Civilian personnel benefits	12,000	10,866	(1,134)
Travel and transportation of persons	6,000	9,450	3,450
Rents, communications and utilities:			
Rental payments to GSA	5,000	5,667	667
Rental payments to others	1,000	-	(1,000)
Other rents, communications and utilities	1,000	1,902	902
Other services:			
Advisory & assistance services			-
Other services	8,000	9,554	1,554
Purchase of goods/services fr Govt. accts	3,000	1,004	(1,996)
Equipment	1,000	1,990	990
Unvouchered		100	100
Total obligations	**71,000**	**80,318**	**9,318**
Unobligated balance available, SOY	-	-	-
Unobligated balance available, EOY	-	-	-
Unobligated balance expiring			-
Total	**71,000**	**80,318**	**9,318**

Chapter 5 - Performance Goals and Measures

In the development of performance measures, the Inspector General Act of 1978, as amended, mandates the reporting of certain statistics and related quantitative data to the Secretary and Congress. To accommodate uncontrollable or unpredictable factors, the OIG's performance goals and measures will be updated annually for maximum effectiveness in meeting the changing needs of DHS, consistent with OIG's statutory responsibilities. In addition to the mandatory requirements, performance measures identified here will serve as a basis to determine the overall effectiveness of our OIG work.

FY 2004

Performance Goals and Indicators

Goal 1. Add value to DHS programs and operations.

1.1 Provide audit and inspection coverage of 75% of DHS' strategic objectives, the President's Management Agenda, and the most serious management challenges facing DHS

1.2 Achieve at least 75% concurrence with recommendations contained in OIG audit and inspection reports

1.3 Complete draft reports for at least 75% of inspections and audits within six months of the project start date (i.e., entrance conference)

Goal 2. Ensure integrity of DHS programs and operations.

2.1 At least 75% of substantiated investigations are accepted for criminal, civil, or administrative action.

2.2 At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.

2.3 Provide audit coverage of $500 million of DHS grant programs.

4.4 Achieve at least 75% concurrence management with recommendations on grant audits.

Goal 3. Deliver quality products and services.

3.1 Establish and implement an internal quality control review program covering all elements of DHS OIG.

3.2 Establish and implement an employee training program for DHS OIG.

3.3 Establish and implement a performance evaluation program for employees of DHS OIG.

4.4 Establish and implement an awards program for DHS OIG.

Chapter 6 - Project Narratives

BORDER AND TRANSPORTATION SECURITY DIRECTORATE

IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE) BUREAU

ICE's Institutional Removal Program

ICE's Institutional Removal Program (IRP): (1) identifies criminal aliens in federal, state, and local correctional facilities that may legally be "removed" or returned to their home countries because they were never entitled to be in this country to begin with or because their prescribed period of admission has expired; (2) ensures that criminal aliens are not released into the community; and (3) removes criminal aliens from the United States after they have completed their sentences. The IRP process ideally begins with the identification of potentially deportable foreign-born inmates as they enter the correctional system, and culminates in a hearing before an immigration judge at a designated hearing site within the federal, state, or local prison system. Upon completion of their sentences, deportable aliens are then released into ICE custody for immediate removal. The IRP is a cooperative effort among ICE, the Executive Office for Immigration Review, and participating federal, state, and local correctional agencies. ICE statistics show that, of the 71,063 criminal aliens the former Immigration and Naturalization Service (INS) removed in FY 2001, 30,002 were removed via the IRP. A Department of Justice (DOJ) OIG report prior to the transfer of immigration functions to DHS found that the INS did not effectively manage the IRP.

OIG will determine whether ICE management has: (1) identified the universe of alien inmates in county, state, and federal prisons; (2) completed the administrative review prior to the end of the alien's sentences; (3) ensured that criminal aliens are deported and repatriated upon completion of their sentences; and (4) has effective practices for dealing with countries refusing to repatriate such deportees. *Office of Audits**

* Italicized is the component of DHS OIG responsible for the applicable project

Prioritization of Aliens to be Detained

At the federal level, "detention" refers to the temporary holding of aliens suspected of violating federal immigration laws or pending immigration hearings and removal proceedings. Detention differs from "incarceration," which is confinement of those convicted of federal crimes who have been sentenced to jail time. There are three main reasons why an illegal alien may be detained - risk of flight, risk to the community, and requirement of law. Aliens are detained per established immigration priorities. For example, the top two priorities are aliens with criminal records, and aliens from the list of countries suspected of harboring and training terrorists. Detention does not by itself imply that a person is facing federal criminal charges. Detainees may be in the removal process, i.e., deportation from the U.S., or in hearings before an administrative law judge to determine whether they are eligible to remain in the United States.

The OIG will determine whether: (1) consistent criteria are used to establish detention priorities; and (2) detention standards have been re-evaluated and updated since September 11, 2001. *Office of Audits*

Air and Marine Operations

Originally established primarily to combat drug smuggling, the Office of Air and Marine Operations (AMO) has taken on an expanded homeland security role since September 11, 2001. AMO's mission is to protect the American people and critical infrastructure by using an integrated and coordinated air and marine force to deter, interdict, and investigate acts of terrorism and smuggling arising from the unlawful movement of people and good across the borders of the United States. The Air and Marine Operations Center (AMOC), under the direction of AMO, is a multi-agency radar, communications, and control center that is linked to a wide array of civilian and military radar sites, aerostats, airborne reconnaissance aircraft and other detection assets which can potentially provide 24-hour, seamless radar surveillance throughout the continental United States, Puerto Rico, the Caribbean, and beyond. This allows AMO to identify, track, and support the interdiction and apprehension of violators attempting to enter United States airspace with illegal drugs or terrorist objectives.

In addition, the National Capital Region Coordination Center (NCRCC), also under AMO's direction, enhances airspace security for the National Capital Region (NCR) through coordination of information exchange among participating agencies as they perform their individual missions to prevent, deter, and interdict air threats. The role of the NCRCC is to provide "AMOC-type" service, manage specifically designated air security systems for the NCR, and deploy air interdiction aircraft.

The OIG will evaluate whether AMO is managing its resources effectively and efficiently to ensure that it is meeting its mission objectives. *Office of Audits*

Certifying Educational Institutions to Reduce the Risk of Terrorism from Foreign Students and Exchange Visitors

The Student and Exchange Visitor Information System (SEVIS) revises and enhances the process by which foreign students and exchange visitors gain admission to the United States. SEVIS increases the ability of ICE to maintain up-to-date information on foreign students and exchange visitors to ensure that they arrive in the U.S., appear and register at the designated school or exchange program, and properly maintain their status during their stay in the U.S., as the law requires. Only those institutions certified to use SEVIS are currently able to sponsor a new foreign student or exchange student.

The USA PATRIOT ACT of 2001 earmarked $36.8 million for implementing SEVIS and the Student and Exchange Visitor program. In addition, almost $3.5 million was collected from SEVIS-certified schools. The foreign students cannot register and begin taking classes at those schools until ICE has approved their applications. The Enhanced Border Security and Visa Entry Reform Act of 2002 requires schools to report within 30 days after the school's registration deadline foreign students, who fail to enroll. As of July 2003, more than 3,500 "no-show" students had been reported to ICE. ICE will use this information to determine whether the "no-show" students have violated the law and/or pose a security risk.

The OIG will determine whether: (1) there are controls in place to ensure that foreign students and exchange visitors are attending certified schools and do

not pose a security threat; and (2) ICE is timely approving applications before students can register and begin taking classes. *Office of Audits*

Visa Security Program in Saudi Arabia

Section 428 (i) of the Homeland Security Act requires DHS to assign staff to Saudi Arabia to review all visa applications before they are issued or denied so as to screen for terrorists. DHS temporarily assigned personnel to perform these duties on September 1, 2003, in the cities of Riyadh and Jeddah. The act also authorized the establishment of Visa Security Offices (VSO) worldwide, and DHS has announced plans to open VSOs in at least six other countries in 2004. Because the planned VSOs will likely be staffed and operated based on DHS' experience in Saudi Arabia, an early evaluation of the Riyadh VSO will be highly useful to DHS decision makers as VSOs begin to become operational worldwide.

The OIG will evaluate the visa application review process at the VSO at the U.S. embassy in Riyadh, Saudi Arabia. This evaluation will also serve as a prototype for future inspections by the DHS OIG at other overseas DHS VSO locations. *Office of Inspections, Evaluations, and Special Reviews*

Security Vulnerabilities of the Visa Waiver Program

The OIG will evaluate the security of the Visa Waiver Program (VWP). Specifically, the review will examine statistical evidence of security weaknesses (or violations) of the VWP, evaluate the safeguards used to identify potential or actual VWP violators, and identify procedures to reduce VWP security vulnerabilities. *Office of Inspections, Evaluations, and Special Reviews*

Federal Air Marshals Service (FAMS) Program

The FAMS program has undergone a rapid expansion in mission and workforce size since September 11, 2001. The OIG will examine the background investigations and training for FAMS officers. It also will review workload requirements and coverage of scheduled flights. Finally, it will examine the

transfer of FAMS from Transportation Security Administration (TSA) to ICE. *Office of Inspections, Evaluations, and Special Reviews*

ICE's Compliance Enforcement Office

BTS has invested substantial resources in strengthening border security by devising new or enhanced database systems to monitor the entry, departure, and activities of non-immigrants in the United States. The principal systems are SEVIS (which tracks foreign students) and US-VISIT (the United States Visitor and Immigrant Status Indication Technology System, a successor system to NSEERS, National Security Entry Exit Registration System, that tracks foreign travelers holding visas). The two systems seek to identify non-immigrants who breach their conditions of entry -- by dropping out of school, overstaying their visa, or other actions. ICE's Compliance Enforcement Office is responsible for following up on "visa overstays" or out-of-status aliens identified by the tracking systems, as well as resulting from other immigration enforcement programs and initiatives. The review will cover resources, enforcement strategies, and performance of the office's efforts to identify, locate, and remove aliens. In doing so, the review will assess the linkages between entry/exit/registration requirements and enforcement efforts when registrants are reported to be delinquent. This review will not assess the separate Institutional Removal Program discussed above. *Office of Inspections, Evaluations, and Special Reviews*

Law Enforcement Support Center (LESC)

The LESC serves as a national enforcement operations center by providing timely immigration status and identity information to local, state, and federal law enforcement agencies on aliens suspected, arrested, or convicted of criminal activity. The LESC operates 24 hours a day, 7 days a week assisting law enforcement agencies with information gathered from 8 databases, the National Crime Information Center, the Interstate Identification Index (III), and other state criminal history indices.

The OIG will evaluate the operations of the LESC. The review will examine the LESC's ability to support state and local law enforcement agencies. The review will include management of the LESC mission, resources, products produced, and performance metrics. *Office of Inspections, Evaluations, and Special Reviews*

CUSTOMS AND BORDER PROTECTION (CBP) BUREAU

US-VISIT

On May 19, 2003, DHS announced the establishment of US-VISIT, an automated system for tracking and controlling the entry and exit of all aliens entering and leaving the country through air, land, and sea ports of entry (POEs). Prior to the creation of DHS in March 2003, the DOJ, in consultation with the Department of State, had been mandated by Congress to establish such an electronic entry-exit system based on pieces of legislation enacted between 1996 and 2002. Pursuant to the Homeland Security Act of 2002, DHS was charged with this task when immigration functions were transferred from DOJ to DHS. This entry-exit system will utilize biometric technologies (i.e., fingerprints and photographs) and machine-readable, tamper-resistant documents to provide authorized personnel from CBP at POEs and other agencies at consular posts abroad with access to integrated alien arrival and departure data in an electronic format (i.e., database).

The OIG will determine whether the US-VISIT Program Management Office is effectively monitoring compliance with contract requirements to ensure that milestones are being met and deliverables are provided as intended, whether controls are in place to ensure that project costs are closely monitored, and whether controls are in place to ensure that modifications are scrutinized to minimize the risk of waste, fraud, abuse, and mismanagement. *Office of Audits*

Entry/Exit Control Issues at Land Ports of Entry

Historically, development of a national entry-exit system has focused on establishing a process for airline passengers at airport POEs. Airport POEs offer

many logistical and control features that facilitate an entry/exit system that may not be duplicated at land POEs.

The OIG will review the developmental efforts to implement an entry/exit system at land ports of entry. The review will examine system operating requirements, integration and operability strategies with other systems, and identification of specific land port of entry requirements. With respect to prospective planning for implementation of US-VISIT, the review will evaluate project objectives and timelines, pilot test results, performance measures, and the project management plan as they relate to land POEs. *Office of Inspections, Evaluations, and Special Reviews*

Secure Electronic Network for Travelers' Rapid Inspection (SENTRI) Program

The SENTRI program was developed to facilitate the flow of traffic at land POEs on the southern border by pre-registering "low-risk" drivers and passengers. SENTRI is also the highest volume "trusted traveler" program in current use and, therefore, is a potential prototype for other such applications. The OIG will evaluate the integrity of the SENTRI program.

This review will examine the processes and procedures to prevent and detect fraud, identify fraudulent applicants, and interdict violators. The review will assess the integrity of the security process of the SENTRI program to ensure that only qualified applicants are enrolled in and remain enrolled in the program. *Office of Inspections, Evaluations, and Special Reviews*

Customs Trade Partnership Against Terrorism (C-TPAT)

C-TPAT was developed to enhance the security of international supply chains and deter international acts of terrorism, as well as facilitate the smooth passage of commerce across United States borders. Under C-TPAT, CBP officials work in partnership with private industry, reviewing supply chain security plans and recommending improvements. In order to participate in this program, businesses must conduct comprehensive self-assessments of security areas, including

procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security. In return, C-TPAT members receive the benefit of a reduced likelihood that containers traveling along their supply chains will be inspected for weapons of mass destruction. As of May 2003, 3,355 companies had signed C-TPAT agreements. CBP is still developing critical aspects of the program intended to ensure that member companies comply with C-TPAT requirements for improving and maintaining supply chain security practices. The FY 2004 Budget Request allocated $12 million for C-TPAT.

The OIG will evaluate whether CBP has implemented adequate management controls over the C-TPAT program to ensure that C-TPAT participants are meeting their program participation requirements and that program objectives are being met. *Office of Audits*

Container Security Initiative (CSI)

Containerized shipping is a critical component of global trade because about 90 percent of the world's trade is transported in cargo containers. Since September 11, 2001, concern has increased that terrorists could smuggle weapons of mass destruction in the seven million containers that arrive annually at U.S. seaports. In response to this concern, CSI was developed in January 2002 to detect and deter acts of container-related terrorism at the earliest point feasible along the supply chain. Through CSI, high-risk maritime cargo containers are identified and examined for weapons of mass destruction at foreign ports before they are shipped to the United Sates. CSI consists of four core elements: (1) establishing security criteria for identifying high-risk containers based on advance information; (2) pre-screening containers at the earliest possible point; (3) using technology to pre-screen high-risk containers quickly; and (4) developing secure and "smart" containers that cannot be tampered within transit. The FY 2004 Budget Request allocated $61 million for CSI. The OIG will conduct a series of audits to evaluate the implementation of CSI and its impact on enhancing port security. *Office of Audits*

Plans to Improve Security at Northern Border Ports, Crossings, and Public Lands

CBP and ICE, along with other law enforcement agencies including the Department of Interior, are responsible for the security and management of over 300 official POEs, as well as unofficial crossings and public land straddled by national parks. Close lines of communication, collaboration, and adequate equipment are needed to ensure security at the border. The potential for illegal activity along the northern border is great because it includes waterways and vast stretches of wilderness with minimal law enforcement presence. In 2001, the Border Patrol estimated that approximately 250,000 undocumented migrants entered the country through parkland, and 80% of drug smuggling now occurs between POEs. Furthermore, vulnerabilities in targeting and inspection programs increase the opportunity for railcars and trucks transporting garbage to be used as means to conceal weapons of mass destruction and other instruments of terrorism. Many of the northern border ports do not have mobile radios to facilitate communication between inspectors, adequate lighting, or camera equipment.

The OIG will conduct a series of audits to assess the vulnerabilities of the northern border that may facilitate terrorist activity. These reviews will include targeting, use of equipment, and inspections to prevent ports, unofficial crossings, public land straddled by national parks, railcars, and trucks carrying garbage from being used to smuggle terrorists and implements of terror into the country. Also, the reviews will evaluate whether Border Patrol resources are coordinated with CBP inspection activities, and roles and responsibilities are clearly defined to ensure that security measures are operating according to the overall security strategy. Also, the OIG will assess DHS' collaborative efforts with the National Park Service and other law enforcement agencies to strengthen security at the northern border. *Office of Audits*

ACE Implementation Process

On August 13, 2001 the U.S. Customs Service awarded e-Customs Partnership a contract to develop the Automated Commercial Environment (ACE). ACE is a 5-year project estimated to cost over $2 billion. Audits performed in the program

management and contracting areas identified problems regarding communications, implementation of management programs, quality of deliverables, and funding. It is important that program processes be tracked and modified to ensure that they provide CBP with the tools needed to manage this massive effort effectively.

The OIG will conduct several audits to determine whether: (1) the Process Improvement Program is implemented, operational, and providing necessary changes to support CBP's growth and objectives effectively; and (2) funds requested through expenditure plans are used as intended, and that negotiated amounts paid are in agreement with requirements delivered. Also, the OIG will assess the deployment of ACE with regard to planning, user training, security and systems operations, and system performance. *Office of Audits*

CBP's Efforts to Reorganize Its Inspection Workforce

CBP unifies legacy U.S. Customs Service (Customs), INS, Animal and Plant Health Inspection Service (APHIS) inspectors, and the Border Patrol to stand guard at the nation's land borders, seaports, and international airports. Their work had been divided up based on their respective missions – INS inspectors monitor people, Customs monitors cargo, and APHIS monitors animals and plants, which could be carrying destructive foreign pests. Formerly, each individual inspection unit had its own structure, computer systems, procedures, lingo, and culture. However, now all have to perform in unison to accomplish the mission of DHS.

CBP is crafting a plan to reshape the inspection workforce based on the "One Face at the Border," initiative. This initiative is designed to unify the border inspection process under one CBP officer who is cross-trained to address all three highly important inspection needs. The CBP officer will carry out all of the functions previously performed by inspectors from Customs, INS, and APHIS. The current CBP, legacy INS, and APHIS inspectors will be converted to the new CBP officer positions in the spring of 2004, and will begin cross-training in all aspects of the new position.

The OIG will determine whether CBP: (1) has established and implemented a plan to allocate resources and utilize best practices to manage its new inspection

workforce; and (2) has taken measures to ensure that adequate cross-training is provided, systems are integrated, and communications technology has been aligned to support homeland security requirements better. *Office of Audits*

CBP's Ability to Detect Uranium at Ports of Entry

The OIG is conducting a review of CBP's ability to detect uranium at POEs at the request of the House Energy and Commerce Committee. Specifically, we are following up on two ABC News stories regarding reporters' being successful in smuggling depleted uranium into the U.S. via commercial shipping containers. The first incident involved depleted uranium smuggled into the U.S. from Istanbul, Turkey through the Port of New York. The second incident involved depleted uranium, smuggled into the U.S. from Jakarta, Indonesia through the Port of Los Angeles. On both occasions CBP officials said that the interdiction system functioned properly because the container was targeted as a "high risk" shipment and inspected. Nonetheless, despite being targeted and inspected, CBP inspectors failed to detect the package containing the depleted uranium.

The OIG will assess the CBP inspection protocols and detection equipment related to the shipments to identify the vulnerabilities that allowed the depleted uranium to go undetected. Also, the OIG will assess whether the material would have been detected had it been weapons-grade uranium or other nuclear materials. *Office of Audits*

Detecting Weapons of Mass Destruction with High Technology Equipment

High technology equipment used to detect weapons of mass destruction can include mobile truck x-ray units, fixed-site truck x-ray systems, vehicle and cargo inspection systems, mobile x-ray vans, personal radiation detectors, itemisers, isotope identifiers and portal detection systems. Treasury OIG conducted a number of audits in this area that identified several weaknesses. These include a lack of equipment utilization monitoring, ineffective inventory control procedures, and inadequate logistical planning when deploying the larger pieces of equipment. Additionally, legacy Customs had not developed a strategic plan for acquiring, deploying, or assessing certain equipment items.

The OIG will determine whether CBP has addressed the previous concerns and developed a strategic plan to coordinate, monitor, and account for the high technology equipment that is an integral part of the enforcement inspection process. *Office of Audits*

Use of Recognition and Remote Assessment Technology

The OIG will assess the CBP's testing and introduction of recognition and remote assessment technology. The review will examine the use of the technology at POEs and the potential expansion to otherwise unguarded areas of the border. These technologies are viewed as "force multipliers" and potentially significant assets to guard the nation's borders in remote areas. The review will cover identification of operational requirements, identification of appropriate technology, development and fielding strategies, development of project objectives and timelines, pilot test results, performance measures, and the project management plan. *Office of Inspections, Evaluations, and Special Reviews*

Review of Access Controls over DHS Financial Systems

The General Accounting Office's (GAO) Federal Information System Controls Audit Manual defines "access controls" as controls that should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include logical controls such as security software programs designed to prevent or detect unauthorized access to sensitive files. Access controls are critical to review to ensure that there is adequate reliance on the data generated and processed within the financial systems. The audit will determine whether logical and physical access to DHS' financial systems have been protected against unauthorized modification, disclosure, loss, or impairment. *Office of Information Technology*

FEDERAL LAW ENFORCEMENT TRAINING CENTER

Challenges Facing the Federal Law Enforcement Training Center (FLETC)

Since its inception in the early 1970s, FLETC, now a component of DHS, has played a vital role in training personnel from federal, state, local, and foreign law enforcement agencies. FLETC is responsible for providing basic, advanced, specialized, and refresher training for law enforcement officers from 75 federal law enforcement agencies, with the exception of the Federal Bureau of Investigation and the Drug Enforcement Agency.

FLETC's role since September 11, 2001, has increased significantly. In fiscal year 2003, according to the FLETC officials, 65% of its projected training workload will come from nine agencies transferred to DHS. The sudden influx of large numbers of law enforcement personnel to FLETC, coupled with the post September 11 environment, has raised concerns about whether FLETC can meet the training demand challenges and provide quality and timely training. A GAO report, issued on July 24, 2003, recommended that DHS improve FLETC's capability planning, periodically assess the condition of training facilities and infrastructure, and improve the acquisition process for an automated scheduling system.

The OIG will: (1) determine whether FLETC will be able to meet the continued demand to provide effective and timely training to DHS and other federal, state and local law enforcement agencies; and (2) evaluate FLETC plans to meet the long-term demand and future cost associated with resource requirements, such as instructors, facilities and equipment. *Office of Audits*

TRANSPORTATION SECURITY ADMINISTRATION

Access to Secure Areas at Airports

Controlling access to secure airport areas where only authorized airport employees and contractors are allowed is paramount to ensuring the safety of

the flying public. Individuals with unescorted access to secure areas of the airport are required to have undergone a fingerprint-based criminal history record check. This area of security is the primary responsibility of the airport authority and its tenants. Ensuring that access to secure areas of the airport is adequately safeguarded will minimize the opportunity for terrorism. As an added security measure, major airports have added the requirement that only passengers with boarding passes be allowed entry to the security checkpoints. During our penetration testing of the civil aviation security screening function, we identified access vulnerabilities, which allowed us to gain access to the security checkpoints and consequently the sterile area of most of the airports tested. Also, TSA has developed and implemented, on a pilot basis, the Transportation Worker Identification Program (TWIP). TWIP is intended to enhance access security by establishing a system-wide common credential used across all transportation modes for personnel eligible for unescorted physical access to secure areas of the national transportation system. The OIG will conduct penetration tests to evaluate the airline industry's compliance with federal aviation security requirements that adequate security procedures be established and implemented to allow only authorized personnel and equipment access to secure airport areas. *Office of Audits*

Assessment of Domestic Air Cargo Security

TSA is responsible for ensuring that cargo transported domestically by air carriers and indirect air carriers is free from weapons of mass destruction and other deadly implements. TSA relies on air carriers and indirect air carriers to implement security programs that include requirements for limited pre-screening of shippers and limited inspection of cargo. In 2002, there were approximately 3,200 indirect air carriers and approximately 226 domestic and foreign air carriers, 2,789 of which had approved security programs at U.S. airports. TSA is responsible for oversight of the air carriers' and indirect air carriers' compliance with cargo security requirements, which includes comprehensive assessments of the various security practices employed by air carriers and indirect air carriers. Transportation OIG issued a report on the TSA's cargo security program. The report concluded that TSA had failed to develop and implement an oversight system that effectively monitors and adequately ensures compliance with air cargo

security program requirements. The OIG will evaluate TSA's efforts to assess the air cargo security programs of both air carriers and indirect air carriers, and its ability to monitor the air transportation security programs. *Office of Audits*

Effectiveness of ETD versus EDS in Detecting Explosives

Since January 1997, the Federal Aviation Administration (FAA) has been steadily deploying advanced security technologies to airports nationwide to improve the screening of passengers' checked baggage. Among these technologies are the Explosive Detection Systems (EDS) and the Explosive Trace Detection (ETD) machines. After September 11, 2001, there was a radical acceleration in the deployment schedule of advanced security technologies, especially the deployment of EDS to screen all checked baggage. The enactment of the Aviation and Transportation Security Act (ATSA) on November 19, 2001, mandated 100% screening of checked baggage using EDS. EDS utilizes CT-Scan technology to detect certain kinds of explosives based on measurements of density, whereas ETD technology detects residues of explosive materials by examining surface samples taken from key areas of passengers' carry-on and checked baggage. Successful detection of explosives by the ETD is dependent upon proper sampling techniques by the screener. The OIG will assess the pros and cons associated with using EDS and ETD as the primary tool for screening checked baggage. *Office of Audits*

Arming Pilots Against Terrorism Act (APATA)

The Arming Pilots Against Terrorism Act was enacted as part of the Homeland Security Act of 2002. It requires TSA to establish a program to select, train, deputize, equip, and supervise volunteer pilots for the purpose of defending flight decks against acts of criminal violence and air piracy. At present, the Federal Flight Deck Officer program is open only to pilots of passenger aircrafts. To participate in the program, pilots must meet numerous criteria. Training must be completed in its entirety and re-qualification is required every two years. Allowing pilots to carry guns in the flight deck has been a longstanding source of controversy.

The OIG will: (1) determine how pilots are selected and screened for the program; (2) evaluate the training received by the pilots; and (3) determine whether training is provided in a timely manner. *Office of Audits*

Security for all Modes of Transportation

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. Yet, since its inception, the agency has been mainly concerned with aviation. TSA is in the process of working on a national security plan that will address all modes of transportation. TSA is also in the process of drafting memoranda of understanding with other transportation related agencies to determine how they will coordinate work in the future. This collaboration is important given that safety and security aspects of transportation have been split, leaving safety with the Department of Transportation and moving security to TSA. In its 2004 budget of $4.8 billion, $4.5 billion is earmarked for aviation security and $85 million is earmarked for non-aviation transportation modes like rail, highway, mass transit, cruise lines, and ferries.

The OIG will assess TSA's efforts to ensure that all modes of transportation provide reasonable security measures to protect against terrorist activity. Specifically, we will determine whether TSA has conducted a threat assessment to include all modes of transportation, developed an implementation plan, and distributed funds accordingly. *Office of Audits*

Known Shipper Program

Under TSA's Known Shipper Program, only cargo from approved shippers and forwarders is allowed on passenger aircraft. If the cargo is from an unapproved ("unknown") shipper or forwarder, it must be diverted to an all cargo aircraft or another form of transport. On average, TSA annually receives approximately 18,000 requests from air carriers to ship cargo, of which an average of 6,000 are unknown shippers. Based on TSA's data base of approved shippers and forwarders, carriers are advised whether the cargo can be accepted. There is an estimated 12.5 million tons of air cargo transported per year, 2.8 million tons of which are on passenger planes.

The OIG will assess TSA's known shipper program processes and procedures to determine whether practices are adequate to minimize the risk that weapons of mass destruction and other deadly contraband can be transported on passenger aircraft. *Office of Audits*

TSA's Efforts To Improve Screener Performance

The events of September 11, 2001, encouraged Congress to create the ATSA. The law was designed to enhance security of the nation's aviation system. ATSA mandated that TSA hire and train thousands of screeners for the nation's 429 commercial airports by November 19, 2002. The plan to federalize the screener workforce has been plagued with difficulties since its inception. TSA has made efforts to correct several past weaknesses regarding screener performance; however, improvements are still necessary to ensure that the flying public is as well protected from terrorist activity as reasonably possible. A recent DHS OIG undercover audit of screener procedures revealed that several problems still plague screener performance. This review will determine the types of improvements that have been made to enhance the performance of federal aviation security screeners and assess those improvements.

The OIG will: (1) evaluate TSA's policies, procedures, and practices to ensure air carrier passengers and their carry-on and checked baggage are adequately screened; and (2) TSA's Screener Standard Operating Procedures and training material reflect the most effective practices and technologies for improving screener performance. *Office of Audits*

Federal Air Marshal Service

At the request of members of the House Select Committee on Homeland Security, the OIG is conducting a review of allegations that the TSA is conducting investigations to ferret out and discipline FAMS for talking to the Congress, the press, or the public about cross-country and international flights. The OIG will assess the validity of the allegations. *Office of Audits*

Authorities and Responsibilities of Federal Security Directors (FSD)

The FSDs are a significant federal presence at airports with a responsibility for air transportation security that often depends upon the cooperation of other aviation and law enforcement participants. The OIG will examine the authorities, explicit and implicit, of FSDs to manage security operations at U.S. airports. The review will seek to determine the strengths and weaknesses of the FSD program and the obstacles to making program improvements. *Office of Inspections, Evaluations, and Special Reviews*

Training and Testing Process for Baggage Screeners

The OIG will continue to explore issues developed in an earlier inspection of alleged irregularities in the baggage screener testing program. We conducted that review in response to a request from Senator Charles E. Schumer. During that review, we identified problems with the testing plan used to certify baggage screeners at the conclusion of the classroom segment of training. This review will evaluate whether actions planned by TSA to update, modify, and improve the training of checked baggage screeners have been completed and have resulted in an enhanced training program. The review will examine the current training curriculum, manuals, testing tools, and operating procedures with particular regard for the on-the-job training that is said to supplement the classroom portion. *Office of Inspections, Evaluations, and Special Reviews*

Procedures to Prevent Passenger Baggage Theft

Since the federal government now assumes responsibility for screened baggage, it is also responsible to ensure that that baggage and contents are secure from theft. The OIG will examine the process used by TSA to prevent and investigate thefts of passenger baggage (or contents) after TSA has taken control of the baggage. The review will also examine the processes TSA uses to resolve passenger claims. *Office of Inspections, Evaluations, and Special Reviews*

Seaport Security Grants Programs

TSA will disburse $170 million and the Office of Domestic Preparedness (ODP) will disburse $75 million for port security improvements. The OIG will examine the management and coordination between TSA's Port Security Grant Program and the ODP port security grant program administered as part of the Urban Areas Security Initiative. The review will focus on decision criteria used in awarding grants, including vulnerability assessments. The review also will assess efforts by TSA and ODP to ensure that funds are used appropriately and effectively to enhance port security. Finally, the review will explore the role of the Information Analysis and Infrastructure Protection directorate relative to seaport security enhancements as part of its infrastructure protection program. *Office of Inspections, Evaluations, and Special Reviews*

Unisys Contract

In August 2002, Unisys Corporation was awarded an unprecedented, multi-year task order to build an advanced information technology infrastructure for TSA. Under the management services contract, Unisys is to provide information technology and telecommunications services, including hardware and software services, help desk, network/security operations, and business process re-engineering services for TSA. This performance based task order has an initial period of three years and can be renewed by the government for two additional two-year periods. It is estimated that the contract's cost may now be in excess of $1 billion.

The OIG will assess TSA's oversight of the Unisys contract, especially in light of TSA's exemption from the Federal Acquisition Regulation. The OIG will also review the process surrounding contract award and compare this with best practices in federal procurement. *Office of Audits*

Collection of Air Passenger User Fees

CBP is responsible for collecting user fees from air passengers arriving in the U.S. The fees are designed to pay for the costs of inspection services provided by CBP,

which now includes legacy INS and APHIS inspection processes. In addition, TSA is also required to impose a fee on airline passengers. This fee is designed to pay for the costs of providing specific civil aviation security services, including screening personnel and federal air marshals. Between Fiscal Year 1998 and 2002, the former U. S. Customs Service collected $1.1 billion from the airlines. Now that CBP's inspection workforce has expanded to legacy INS and APHIS inspection services, it is important that CBP ensure that revenues collected are accounted for and are adequate to cover the costs of services provided. Similarly, TSA should ensure that the revenues collected are accounted for and are adequate to cover the costs of services for which it is required to collect a fee.

The OIG will determine whether: (1) air passenger user fees are properly accounted for; and (2) revenues collected are adequate to recover the service costs as authorized. *Office of Audits*

OFFICE OF DOMESTIC PREPAREDNESS

State First Responder Grants

State and local governments received first responder grants of approximately $3.2 billion in FY 2003 from the ODP. Approximately $3.3 billion will be provided in FY 2004, plus $750,000 that will go directly to high-threat urban areas. The states are responsible for ensuring that first responders get the benefit of the funds, but each state determines its own methodology for allocating the funds. Some buy equipment and distribute it, while others distribute the funds and allow local governments to do the purchasing. Some states use a regional allocation process, while others distribute to counties or cities. A key to the effective use of the funds is the states' ability to allocate the funds expeditiously based on a strategic plan that prioritizes needs.

The OIG will audit individual states to determine how, and how well, they evaluate threat, vulnerability, capability, and needs; prioritize requirements; determine an allocation methodology; and measure the effectiveness of the

program. The OIG will also attempt to verify that states and local jurisdictions comply with grant requirements. *Office of Audits*

Effectiveness of SHSAS in Data Collection

To assist the states in conducting their threat, risk, and needs assessments, and developing a three-year strategy, the Office of Justice Programs (OJP) developed an on-line data collection tool in 1999 called the "State Homeland Security Assessment and Strategy" (SHSAS). ODP updated the SHSAS for FY 2003. It will continue to serve as a planning tool for state and local jurisdictions, but will also be useful to ODP in allocating federal resources for homeland security and establishing preparedness standards. The OIG will assess the effectiveness of the SHSAS and evaluate its use by ODP. *Office of Audits*

DHS Office of State and Local Coordination and the Office of Domestic Preparedness

ODP is the principal component of the department responsible for preparing the country to respond to acts of terrorism. In carrying out its mission, ODP provides training, funds for the purchase of equipment, support for the planning and executions of exercises, technical assistance, and other support to assist states and local jurisdictions to prevent, plan for, and respond to acts of terrorism. The Office of State and Local Coordination is responsible for addressing many of the homeland security concerns of state and local government officials and business leaders. The Office, housed in the Office of the Secretary, will coordinate with the private sector and with state and local governments to ensure adequate planning, equipment, training, and exercises. It also coordinates and consolidates federal systems of communications and the distribution of warnings and security information.

The OIG will examine the operation of two DHS organizations with overlapping or complementary responsibilities to provide enhanced emergency response capabilities to federal, state, and local governments. The review will cover communication and interoperability between the two organizations, coordination

of efforts, and the differences and similarities of the services they provide. *Office of Inspections, Evaluations, and Special Reviews*

EMERGENCY PREPAREDNESS AND RESPONSE (EP&R) DIRECTORATE

Strategic National Stockpile

EP&R will be receiving a major increase in funding in FY2004 for the Strategic National Stockpile. It will receive about $900 million to purchase critically needed vaccines or medication for bio-defense and $400 million to maintain the stockpile to be able to respond to a national bio-terrorist attack.

The OIG will: (1) assess the effectiveness of the stockpile's transition to DHS; (2) assess DHS preparedness to purchase vaccines and medications; and (3) evaluate the adequacy of DHS' management of the stockpile. *Office of Audits*

Urban Search and Rescue Response System Preparedness

The National Urban Search and Rescue Response System was created to provide specialized lifesaving assistance during major disasters or emergencies. Currently there are 28 task forces in 19 states. In 1997, the Federal Emergency Management Agency (FEMA) OIG audited components of the program and identified deficiencies.

The OIG will conduct a broader scope evaluation to determine whether the task forces are maintaining their readiness, whether DHS provided adequate funding, whether the funding was used for its intended purposes, whether previous management control and eligibility criteria deficiencies have been corrected, and to identify the impact of uncorrected deficiencies. *Office of Audits*

The National Response Plan

The Federal Response Plan has been the government's blueprint for responding to major disasters. It defines the roles of FEMA and other response organizations. It is replaced by the National Response Plan, which is currently being developed. The National Response Plan will expand the Federal Response Plan to include

terrorism and incorporate an incident command structure. The OIG will evaluate the proposed changes. *Office of Audits*

Disaster Grants

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, (Stafford Act) governs disasters declared by the President of the United States. Title 44 of the Code of Federal Regulations provides further guidance and requirements for administering disaster relief grants awarded by FEMA.

The OIG will perform audits of grantees and sub-grantees, focusing on large grants with suspected problems, and areas that are of concern to Congress and FEMA. We will determine whether grantees and sub-grantees accounted for and expended FEMA funds according to federal regulations. These audits will focus primarily on public assistance grants, but may include hazard mitigation grants, and assistance to individuals and households. *Office of Audits*

Effectiveness of Intergovernmental Communications and Information Sharing in Responding to Critical Infrastructure Failures

The denial of electrical service for an extended period of time can cause a dangerous ripple effect of death and destruction across virtually all of the nation's civic and economic sectors. As highlighted by the August 14, 2003, blackouts in the northeastern United States and Canada, as well as widespread outages as a result of Hurricane Isabel the following month, massive regional power failures may be a goal of our terrorist enemies, raising concerns about the vulnerability of U.S. power supplies to enemy attack. There is concern, too, as to whether federal, state, and local governments are effectively communicating and sharing information to deter, or ensure rapid and effective response to, potential attacks on such critical energy sector operations. The OIG will determine the effectiveness of federal, state, and local government communication and information sharing to deter and/or ensure rapid response to potential attacks on critical sector operations, such as power supply and distribution. *Office of Information Technology*

MANAGEMENT DIRECTORATE

Human Capital Management and Planning

The Homeland Security Act gave DHS special authorization to design a human capital management system that fit its unique mission. Currently, DHS employees are covered by their predecessor agencies' human capital policies and procedures. Numerous articles have cited the inefficiencies and inequities of having two persons in the same department doing approximately the same job for different pay and promotion potential. In addition to developing options for pay and classification, performance management, labor relations, discipline and employee appeals, DHS must also consider the President's outsourcing initiative. The Administration has established goals for competitively sourcing commercial activities, and DHS should be assessing its roles and functions to determine what activities may benefit from outsourcing and what activities should be considered inherently governmental.

The OIG will assess DHS' progress toward establishing its own unique human capital management system and determine what steps DHS is taking to ensure that all concerns from Congress, the Administration, and DHS management are adequately addressed. We will also examine DHS' efforts to identify outsourcing opportunities. *Office of Audits*

Compliance with Improper Payment and Recovery Acts

Under the Improper Payments Information Act of 2002, agencies are required to review annually all programs and activities to identify those that may be susceptible to significant erroneous payments. Where the risk is significant, agencies are to estimate erroneous payments and report them to the President and Congress, including corrective actions. "Significant risk" is defined as annual erroneous payments exceeding both 2.5 percent of program payments and $10 million. Reporting is to begin in FY 2004.

Also beginning in FY 2004, agencies must submit to OMB a report on their recovery audit programs. Section 831 of the *Defense Authorization Act for Fiscal*

Year 2002 (31 USC §§3561-3567) requires agencies that enter into contracts with a total value in excess of $500 million in a fiscal year to carry out a cost-effective program for identifying errors made in paying contractors and for recovering erroneous payments. The program must include the use of recovery audits. The OIG will determine DHS' compliance with these two laws and the degree to which it is prepared to meet the 2004 reporting requirements. *Office of Audits*

Credit Card Program Monitoring

The federal government spends billions of dollars each year through its travel card and purchase card programs. Congressional testimony and OIG and GAO reports show that some federal agencies do not have adequate controls over their purchase programs. Prior to March 1, 2003, organizations that are now in DHS were previously operating under legacy organizations, with varying degrees of internal controls relative to their credit card programs. DHS has seized the opportunity to put together a model program, and has asked for our active involvement. The DHS credit card programs will include regular sampling of all purchase card and travel card transactions by the OIG. Irregularities and improprieties will be reported for criminal investigation and/or management resolution as appropriate. *Office of Audits*

DHS' FY 2004 Financial Statements

The *Accountability of Tax Dollars Act of 2002* requires that an annual financial statement audit be performed at DHS. The purpose of this annual financial statement audit is to determine whether: (1) DHS' FY 2004 financial statements are fairly presented and free of material errors; (2) DHS' internal controls related to financial reporting are adequate; and (3) DHS complies with certain laws and regulations, including the Federal Financial Management Improvement Act. *Office of Audits*

Oversight of Contracted Information Technology-Related Testing Performed as Part of the Department's Fiscal Years 2003 and 2004 Audited Financial Statements

Financial statement audits performed under the Chief Financial Officers Act of 1990 are intended to play a central role in: (1) providing more reliable and useful financial information to decision makers; and (2) improving the adequacy of internal controls and underlying financial management systems. Computer related controls are a significant factor in achieving these goals and in the auditor's understanding of the entity's internal control structure. Computer related controls should be considered during all phases of the audit.

The OIG will determine whether contracted auditors performed sufficient testing to evaluate the department's general and application controls over critical financial systems and data to reduce the risk of loss due to errors, fraud, and other illegal acts and disasters, and effectively to protect its information infrastructure from security threats or other incidents that cause the systems to be inoperable. *Office of Information Technology*

Financial Controls Over the National Flood Insurance Program (NFIP)

The NFIP administers over 90% of its flood insurance policies through private insurance companies called "Write Your Own" companies, with the remaining policies administered by a direct NFIP contractor. Another contractor performs overall statistical and accounting activities for the program.

The purpose of this audit is to test controls over financial, underwriting, and claims activities at these insurance companies and contractors. This audit supports the financial statement audit and is performed because of the government's extensive reliance on private companies and contractors to conduct its flood insurance business. *Office of Audits*

Drug Control Accounting

The Office of National Drug Control Policy (ONDCP) Circular, titled *Drug Control Accounting*, provides the policies and procedures to be used by National Drug Control Program (NDCP) agencies in conducting a detailed accounting and authentication of all funds expended on NDCP activities. The circular designated ICE, CBP, and the Coast Guard as "NDCP agencies".

The OIG will express an opinion about the reliability of specific assertions made in the Detailed Accounting Submission Report that DHS components must provide to the ONDCP. *Office of Audits*

DHS' Information Security Program for Fiscal Year 2004

In response to the increasing threat to information systems and the highly networked nature of the federal computing environment, the Congress, in conjunction with the OMB, requires an annual review and reporting of agencies' compliance with the requirements of the Federal Information Security Management Act (FISMA). Further, in response to Congressman Jim Turner's request, OIG will include in its FISMA evaluation an analysis of the department's ability to conduct security assessments of the many systems used by its contractors.

The OIG will evaluate whether DHS' information security program and practices are adequate. Also, we will determine what progress DHS has made in resolving weaknesses cited in the prior year's review. *Office of Information Technology*

Wireless Security at DHS

The challenge of managing an invisible network made up of wireless computing, applications, and devices is one of the nation's top five security threats for 2004. Wireless technologies can provide productivity improvements for mobile DHS employees, but at the same time, they can expose government information systems to security vulnerabilities. In the last five years, there has been a dramatic

evolution in wireless technologies, standards, and implementation practices, and these changes have affected the security of wireless devices.

The OIG will determine whether DHS has developed adequate policies, established oversight procedures, and implemented adequate security measures to ensure that wireless devices and networkings are secure. *Office of Information Technology*

Chief Information Officer Governance Structure

The Chief Information Officer (CIO) is responsible for consolidating and maintaining the Information Technology (IT) infrastructure, products, and services necessary to support the operations and mission activities of the department. To fulfill the requirements of the Clinger-Cohen Act, the CIO must be a valued member of the senior executive team and serve as a bridge among senior executives, line management, and technical professionals. Possessing the resources, authorities, and accountabilities needed to establish strategic IT directions and a department-wide management structure for meeting current and future technology needs are just as important. The CIO's strategic IT responsibilities include IT business and architectural planning; investment management; policy formulation; systems acquisition, operations, and maintenance; and contract management.

The OIG will determine the effectiveness of the CIO's reporting relationships, resources, authorities, management structure, and functions for managing the department's strategic IT directions. *Office of Information Technology*

Enterprise Architecture Development

An enterprise architecture establishes the roadmap to achieve an agency's mission through optimal performance of its core business processes within an efficient information technology environment. Simply stated, enterprise architectures are blueprints for systematically and completely defining an organization's current or desired environment. Enterprise architectures are essential for evolving information systems and developing new systems that optimize their mission

value. The OIG will evaluate whether DHS and its bureaus have aligned their strategic plans and individual business priorities within an appropriate enterprise architecture framework. *Office of Information Technology*

Review of Disaster Recovery Cost/Benefit Analysis

The primary objective of a disaster recovery capability is to be able to restore mission critical systems as of a certain point in time (e.g., to their state one hour before the disaster) and within a pre-established time period. There are various methods that may be employed to provide this disaster recovery capability, including an in-house (e.g., a remote location), a reciprocal agreement with another DHS entity, or through a commercial vendor. The decision to build an internal recovery capability, to provide a reciprocal capability with another entity, or to outsource must include an analysis of the: (1) relative total cost of ownership; and (2) return on investment. The OIG will determine whether cost/benefit analyses for using commercial recovery facilities: (1) considers department-wide (in-house) facility use alternatives; (2) includes all the resources needed to recover critical applications and realistic out year costs; and (3) uses vendors that can actually provide the necessary recovery services. *Office of Information Technology*

Network Consolidation

Perhaps the foremost and most costly IT challenge the department faces is integrating and consolidating its communications infrastructure, creating the equivalent of one network from the various Wide Area Networks and Local Area Networks in the unclassified environment. The department is looking to major telecommunications carriers to play an integral part in determining priorities and the most effective approach to building the unified network. The OIG will evaluate the effectiveness of DHS' plans and project management structure for consolidating its telecommunications infrastructure. *Office of Information Technology*

Remote Access Security

Connecting laptops and home computers to public networks and downloading sensitive information is one of the top five security threats for 2003. Many organizations, including government ones, have a work-at-home policy to allow employees to access computer systems and data remotely. An employee can gain "remote access" or connect to an organization's network using a public system, such as the Internet or the telephone system, by using a dial-up modem. Unfortunately, networks that allow remote access are targets for hackers. This risk needs to be recognized and every possible step taken to minimize it. The OIG will determine whether DHS has implemented adequate and effective security procedures and authentication systems for gaining remote access to its computer systems. *Office of Information Technology*

Effectiveness of DHS Management of Unclassified Sensitive Personal Information

The loss or compromise of sensitive personal information entrusted to DHS or its contractors can have serious consequences. DHS needs to ensure that systems protecting unclassified, but sensitive, personal information are implemented and maintained with the proper security controls in place. The OIG will determine whether DHS' unclassified but sensitive personal information systems adhere to federal requirements and guidelines and provide for the necessary level of security/protection. *Office of Information Technology*

DHS' Intelligence (SCI) Information Systems

Addressing and controlling potential threats identified during the risk management process is key to protecting DHS' Sensitive Compartmented Information (SCI) systems adequately, which are critical to supporting DHS' mission. The OIG will determine whether DHS' SCI systems adhere to federal requirements and guidelines, and whether the desired level of security protection has been established. *Office of Information Technology*

DHS' Classified Information Systems

The loss or compromise of classified information entrusted to DHS or its contractors can have serious consequences for national security. The cornerstone of a solid classified information system security program is the risk management process, which agencies should use to evaluate the perceived value of classified information and assess the consequences of loss of confidentiality, integrity, and availability, as well as the cost of protective countermeasures. The OIG will determine whether DHS' classified information systems adhere to federal requirements and guidelines and provide for the necessary level of security/ protection. *Office of Information Technology*

DHS' Mainframe Computer Operations

DHS relies on mainframe computers to process information in support of its mission. To ensure mainframe operations are protected, DHS should have a risk management approach, one that identifies all threats and vulnerabilities, determines the greatest risks, and evaluates which risks to accept and which risks to mitigate. The OIG will determine whether DHS has implemented an effective risk assessment and management process to protect its mainframe computers and the department's ability to perform its missions. *Office of Information Technology*

Contractor Access to Sensitive Data

DHS and its components use contractors extensively in their computer operations. As part of their job tasks/assignments, contractor personnel are given direct access to data files, application programs, and computer facilities. Therefore, it is important that contractor access to computer operations (both logical, including dial-up access, and physical) and sensitive data be reviewed to ensure that only authorized users have access and that these users are part of the current contract. The OIG will evaluate effectiveness of DHS' procedures for controlling contractor access to sensitive data and computer operations. *Office of Information Technology*

Network Operating Systems Configuration Management

The software manufacturers that produce and distribute network operating systems regularly update them. These system updates are distributed under annual software maintenance plan subscriptions and are also often available for download from the operating system manufacturer's Internet site. A key issue is the complete and timely installation of the network operating system updates on the agency's servers and workstations.

The OIG will review LAN operating systems configuration management to determine whether: (1) the most current version/subversion is installed; (2) the latest service packs are installed; and (3) relevant hot fixes are installed. *Office of Information Technology*

Production Database Systems Configuration Management

Software manufacturers that produce and distribute database management systems (DBMS) for both the server and workstation components regularly update them. These system software updates are distributed under annual software maintenance plan subscriptions, and are often available for download from the system software manufacturer's Internet site. A key issue is the complete and timely installation of the DBMS updates on the agency's hosts and workstations.

The OIG will determine whether: (1) the most current client and server version/subversion is installed; (2) DBMS compatibility is certified by the application systems software vendor; and (3) the most current client and server DBMS utilities version/subversion is installed. *Office of Information Technology*

INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (IAIP) DIRECTORATE

Terrorist Watch List Consolidation

The events of September 11, 2001, underscore the need for standardization and consolidation of terrorist watch lists better to ensure homeland security. Currently, nine federal agencies use at least a dozen different watch lists, developed in response to their individual legal, cultural, and systems environments and disparate missions. The multiple lists in multiple locations confuse officials who may not know which list at which agency to use in order to list or search for names of suspected terrorists. An effective and consolidated terrorist watch list system will be essential in denying visas to suspected terrorists, detaining and deporting questionable individuals, and finding and arresting suspected international criminals.

The OIG will evaluate challenges and results to date from DHS' efforts to standardize and consolidate the various agencies' terrorist watch lists. We will also assess DHS' role in the Central Intelligence Agency-led Terrorist Threat Integration Center and the newly established FBI-led Terrorist Screening Center. *Office of Information Technology*

Effectiveness of IAIP's Mission and Use of IT

In response to a request from Congressman Jim Turner, the IT office will review the effectiveness of IAIP's use of IT in support of its mission. Significant investment in and use of advanced technologies will be critical to accomplishing the mission and objectives of IAIP. The directorate merges under one roof the capability to identify and assess current and future threats against the homeland, map those threats against our vulnerabilities, issue timely warnings, and take preventive and protective action. Activities necessary to fulfill these responsibilities include: (1) fusing and analyzing information from multiple federal, intelligence, law enforcement, and public sources; (2) conducting threat analysis and warnings; (3) coordinating and consolidating communications with state and local public safety agencies and the private sector; (4) conveying

actionable intelligence and other threat information and, as necessary, (5) making public alerts. The OIG will determine the effectiveness of IAIP's plans and approaches to using IT to assess, guard against, and respond to threats to homeland security. *Office of Information Technology*

DHS Efforts to Secure Cyberspace

One of the nation's top five security threats for 2003 is computer systems' becoming new cyber terrorism targets. The consequences of an attack on DHS' cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, delaying the notification of emergency services, damaging our economy, and putting public safety at risk. The OIG will determine how effectively DHS is assessing the nation's vulnerability to a major cyber terrorist attack, and identify the steps that are being taken to mitigate this threat. *Office of Information Technology*

Homeland Security Operations Center (HSOC)

The OIG will evaluate how the HSOC collects and analyzes information, and produces and disseminates a final analytical threat product. The review will focus on how the HSOC ensures that it receives all of the information it requires, how it manages its analytical operation, and how it ensures that its products meet the needs of its customers. It will also assess the HSOC's process to identify information requirements and prioritize its work efforts. *Office of Inspections, Evaluations, and Special Reviews*

Infrastructure Threat Assessment

The OIG will assess the process used by the IAIP to identify critical national assets, assess threats against those assets, identify threat vulnerability mitigation requirements, and prioritize the threat assessment/mitigation effort. *Office of Inspections, Evaluations, and Special Reviews*

SCIENCE AND TECHNOLOGY DIRECTORATE (S&T)

Plum Island Animal Disease Center

The Plum Island Animal Disease Center is responsible for research and diagnosis to protect the nation's animal industries and exports from catastrophic economic losses caused by foreign animal disease agents accidentally or deliberately introduced into the U.S. In the U.S., certain highly infectious foreign animal diseases, such as foot-and-mouth disease, can be studied only at Plum Island. The S&T directorate was recently assigned oversight responsibility for Plum Island. That responsibility formerly resided within the U.S. Department of Agriculture. The S&T directorate has asked the OIG to assist them by proactively monitoring the development and implementation of their oversight program. *Office of Audits*

Homeland Security Advanced Research Projects Agency's (HSARPA) Funding of Projects

The review will evaluate the process HSARPA uses to identify, prioritize, and fund research projects relevant to detection, prevention, and recovery from homeland security threats, particularly acts of terrorism. It will also examine how the HSARPA monitors the progress made by funded projects. *Office of Inspections, Evaluations, and Special Reviews*

S&T Roles, Responsibilities, and Operations

The OIG will survey the roles, responsibilities, and operations of S&T. The review will summarize the tasks and resources assigned to the S&T offices, the entity's relationship with other DHS components, other federal, state, and local agencies, and the national laboratories. The survey will report on present and prospective programs with a view toward providing baseline information for use by the OIG and for the development of future audits and inspections. *Office of Inspections, Evaluations, and Special Reviews*

BioWatch Program Evaluation

The DHS OIG will work in partnership with the Environmental Protection Agency's Office of Inspector General (EPA OIG) to evaluate the design and implementation of the BioWatch program. The BioWatch program is an expanded use of EPA's air quality sensor network to detect biological agents in select areas. In addition to adding more monitoring stations, the DHS Science and Technology Directorate plans to modernize the sensor network by automating sample analysis and data collection and upgrading sensors. The review will determine whether the BioWatch Program is accomplishing the department's bio-surveillance initiative goals, and whether the BioWatch modernization plans address the program's deficiencies. *Office of Audits*

UNITED STATES COAST GUARD

Mission Performance

The Coast Guard responded to the September 11, 2001, attacks by redirecting 59 percent of its resources to domestic maritime security. The redeployment, however, came at the expense of other important but non-security-related missions. For example, mission hours devoted to core missions such as drug interdiction dropped from 21 percent to 11 percent. Other core mission areas such as living marine resources, marine safety, alien migrant interdiction, aids to navigation and law enforcement, were also hard hit. Despite increased funding for FY 2003, the Coast Guard has not restored operating hours devoted to non-homeland security-related missions to pre-September 11th levels.

This audit is required by Section 888 of the Homeland Security Act of 2002. The law requires OIG annually to assess the Coast Guard's performance of all its missions, with particular emphasis on non-homeland security missions. *Office of Audits*

Helicopter Utilization

In May 2003, the Secretary announced that the Coast Guard's Helicopter Interdiction Squadron (HITRON) would be used for counter-terrorism missions. HITRON was established in 1999 to interdict "go fast" boats transporting drugs to the United States. HITRON, located in Jacksonville, FL, currently consists of eight helicopters. The OIG will review the Coast Guard's aircraft deployment plans and its ability to perform the counter-terrorism and drug interdiction missions, crew training, and use of force doctrine. *Office of Audits*

Law Enforcement Training

Since the September 11, 2001 terrorist attacks, the Coast Guard has reallocated resources to support port, waterways, and coastal security operations, with an emphasis on security and law enforcement operations. New and expanded law enforcement operations and activities include boarding teams and Sea Marshals

established to search vessels for weapons and terrorists. Additionally, the Coast Guard created maritime safety and security teams (MSSTs) for quick deployment when and where necessary. In its FY 2004 budget estimate, the Coast Guard requests funding for further expansion of Sea Marshals and MSSTs, as well as, adding two new Port Security Units.

With these new initiatives comes the need for training and development, not only for these specialized units, but also for the hundreds of general, multi-mission operational units at stations and on cutters around the country that now spend a large part of their time on security and law enforcement patrol. Moreover, with these new initiatives and concepts of operation, the Coast Guard is subject to the likely use of deadly force – a marked change from traditional law enforcement operations.

The OIG will evaluate the adequacy of the training programs supporting these new and expanded law enforcement and security operations. *Office of Audits*

Marine Safety Mission

This audit will complement the mission performance audit required by the Homeland Security Act and address Maritime Transportation Security Act implementation. The extent of marine safety activities is not captured by vessel or aircraft operating hours since the mission is performed primarily by shore based Coast Guard personnel. This audit will review this mission in-depth to determine its adequacy and effectiveness since September 11, 2001.

Coast Guard Marine Safety Offices are tasked with ensuring vessel safety and security. Historically these offices inspected vessels to ensure compliance with safety regulations, such as working and accessible lifeboats and flotation devices. The Coast Guard would implement recent regulatory changes focused on security concerns largely by redirecting or tasking personnel from the Marine Safety Offices. For example, the Maritime Transportation Security Act of 2002 has a number of provisions that call for concerted and extensive action by the Coast Guard to meet a December 31, 2004, deadline for implementation. These actions include reviewing and approving about 18,000 security plans called for by the

act and new rulemakings. The OIG will evaluate the Coast Guard's ability to accomplish these tasks in light of the operational burdens already placed on Coast Guard since September 11, 2001, and the need to fulfill its marine safety mission responsibilities. *Office of Audits*

High Interest Vessels

The Coast Guard is responsible for detecting, identifying, tracking, boarding, inspecting, and escorting high interest vessels that may pose a substantial risk to U.S. ports due to the composition of a vessel's crew, passengers and/or cargo. More than 8,000 vessels make 51,000 port visits each year. The Coast Guard has instituted strict reporting requirements for all vessels arriving/departing U.S. seaports. It also has developed a sophisticated decision-making system for targeting high interest vessels, cargoes, and crews. Responding to high interest vessels requires a substantial commitment of personnel, equipment, and funding. The OIG will evaluate to what extent the Coast Guard is able to detect, identify, board, and inspect all high interest vessels before they enter a U.S. port. The OIG will also determine whether: (1) the program has the right number of personnel with the required expertise and equipment to conduct thorough inspections of these vessels, cargoes, and crews; (2) measures are in place to deal with vessels that, as a result of the inspection, continue to pose a potential security threat, and (3) what impact these activities have on Coast Guard's ability to perform other missions. *Office of Audits*

Deepwater

In June 2002, the Coast Guard awarded the Deepwater Project contract with an estimated cost of $17 billion. The project is intended to replace or modernize by 2022 all assets used in missions that generally occur more than 50 miles offshore including approximately 190 cutters, 100 aircraft, and assorted sensors and communications systems. Since the events of September 11th and Coast Guard's expanded role in homeland security, additional project requirements have been identified. In addition, the Homeland Security Act required the Coast Guard to determine whether the project could be accelerated for completion within 10

years. Both the requirements changes and project acceleration would result in increased annual funding needs for the project.

The OIG will determine whether: (1) the Coast Guard's FY 2004 budget request for Deepwater was based on a reliable cost estimate and a reasonable assessment of needs; (2) the financial and management controls over Deepwater were adequate to ensure the effective use of funds and monitoring of progress; and (3) the large amount of capital funding dedicated to Deepwater affected Coast Guard's other capital needs, such as shore facilities and aids to navigation. *Office of Audits*

Integrated Deepwater System (IDS) Program

The OIG will evaluate the effectiveness of Deepwater information technology systems acquisition and development activities to provide the Coast Guard with a significantly improved ability to detect, identify, and respond appropriately to maritime challenges. *Office of Information Technology*

U.S. SECRET SERVICE

Management and Coordination of Credit Card Fraud/Identity Theft Cases

Financial industry sources estimate that losses associated with credit card fraud are in the billions of dollars annually. The Secret Service is the primary federal agency tasked with investigating access device fraud and its related activities under Title 18, United States Code, and Section 1029. Although it is commonly called the "credit card statute," this law also applies to other crimes involving access device numbers including debit cards, automated teller machine (ATM) cards, computer passwords, personal identification numbers used to activate ATMs, credit card or debit card account numbers, long distance access codes, and the computer chips in cellular phones that assign billing. During fiscal year 1996, the Secret Service opened 2,467 cases, closed 2,963 cases, and arrested 2,429 people for access device fraud. Industry sources estimate that losses associated with credit card fraud are in the billions of dollars annually.

The OIG will review the management of this program by the Secret Service, and the effectiveness of their coordination with other federal, state, and local law enforcement entities, as well as with financial industry sources in the private sector. *Office of Audits*

CITIZENSHIP AND IMMIGRATION SERVICES (CIS)

Progress to Eliminate Immigration Benefit Application Processing Backlogs

The OIG will examine the CIS' short-term plans to reduce immigration application backlogs and its long-range plans to prevent backlogs from occurring in the future. The review will include identification of the size and nature of the application backlog problem, the resources required to eliminate and prevent backlogs, workload planning, performance measures, management oversight, and long-term initiatives to introduce new procedures or technology to prevent application backlogs. *Office of Inspections, Evaluations, and Special Reviews*

MULTI-COMPONENT REVIEWS

Procedures for Controlling Seized Cash and Property

The review will evaluate the procedures used by DHS law enforcement components to seize and dispose of cash, narcotics, and other property acquired during law enforcement operations. The review will cover seizure, owner notification, inventory control, maintenance and security procedures while the property is in DHS custody, and final disposition of the property. *Office of Inspections, Evaluations, and Special Reviews*

Status of DHS Efforts to Address Its Management Challenges

Combining 22 federal agency components into one agency presents perhaps the greatest challenge facing DHS and offers opportunities for integrating systems and operations for greater effectiveness, economy, and efficiency. The department has initiated a number of efforts, with varying degrees of success, to combine and integrate its functions into a more effective and efficient operation. This review will identify those efforts and their timetable for completion, as well as assess the department's progress in addressing other major management challenges. The OIG will use its multidisciplinary resources to review and report on the results of these efforts. *Office of Audits*

DHS Management and Oversight of Major Procurements

DHS has several multi-billion dollar procurements that are critical to meeting the DHS mission. The OIG will audit DHS' management and oversight of the largest and most critical procurements to determine whether contract managers are effectively monitoring compliance with contract requirements to ensure that milestones are being met and deliverables are provided as intended. The audit will also determine whether controls are in place to ensure that: (1) project costs are closely monitored, and (2) modifications are scrutinized to minimize the risk of waste, fraud, abuse, and mismanagement. The OIG will also review the process surrounding the various contract awards and compare them with best practices in federal procurement. *Office of Audits*

Appendix A - OIG Headquarters and Field Office Contacts

OIG Headquarters Senior Management Team

Department of Homeland Security
Attn: Office of Inspector General
245 Murray Drive, Bldg 410
Washington, D.C. 20528

Telephone Number (202) 254-4100
Fax Number (202) 254-4285
Website Address www.dhs.gov

Clark Kent Ervin……. Inspector General
Richard L. Skinner…….. Deputy Inspector General
Richard N. Reback …… Counsel to the Inspector General
Richard Berman…….. Assistant Inspector General/ Audit
Elizabeth Redman……. Assistant Inspector General/ Investigations
Robert Ashbaugh……. Assistant Inspector General/ Inspections, Evaluations and Special Reviews
Frank Deffer……. Assistant Inspector General/ Information Technology
Ed Cincinnati……. Assistant Inspector General/ Administrative Services
Tamara Faulkner……. Congressional Liaison and Media Affairs
Jennifer Price…….. Executive Assistant to the Inspector General

Location of Audit Field Offices

Atlanta, GA
3003 Chamblee-Tucker Rd., Suite 374
Atlanta, GA 30341
(770) 220 -5228 / Fax: (770) 220-5259

Boston, MA
408 Atlantic Avenue, Room 330
Captain J.F. Williams Federal Building
Boston, MA 02110
(617) 223-8600 / Fax: (617)-223-8651

Chicago, IL
55 W. Monroe Street, Suite 1010
Chicago, IL 60603
(312) 886-6300 / Fax: (312)-886-6308

Denton, TX
3900 Karina Street, Suite 224
Denton, TX 76208
(940) 891-8900 / Fax: (940) 891-8948

El Segundo, CA
222 N. Sepulveda Blvd, Suite 1680
El Segundo, CA 90245
(310) 665-7300 / Fax: (310)-665-7302

Houston, TX
5850 San Felipe Road, Suite 300
Houston, TX 77057
(713) 706-4611 / Fax: (713)-706-4625

Indianapolis, IN
5915 Lakeside Boulevard
Indianapolis, IN 46278
(317) 298-1596 / Fax: 317-298-1597

Kansas City, MO
901 Locust, Room 470
Kansas City, MO 64106
(816) 329-3880 / Fax: (816) 329-3888

Marlton, NJ
5002D Greentree Executive Campus,
Route#73 and Lincoln Drive
Marlton, NJ, 08053

Miami, FL
3401 SW 160th Ave, Suite 401
Miramar, FL 33027
(954) 602-1980 / Fax: (954)-602-1033

Oakland, CA
1111 Broadway, Suite 1200
Oakland, CA 94607-4052
(510) 627-7007 / Fax: (510) 627-7017

St. Thomas, VI
Nisky Center Suite 210
St Thomas, VI 00802
(340) 774-0190 / Fax: (340) 774-0191

San Juan, PR
New San Juan Office Building
159 Chardón Avenue, 5th Floor
Hato Rey, Puerto Rico 00918
(787) 296-3531 / Fax: (787) 296-3652
Mailing Address: P.O. Box 70105
San Juan, PR 00936

Location of Investigative Field Offices

Atlanta, GA
3003 Chamblee-Tucker Rd
Suite 301
Atlanta, GA 30341
(770) 220-5290 / Fax: (770) 220-5288

Chicago, IL
55 W. Monroe Street, Suite 1010
Chicago, IL 60603
(312) 886-2800/ Fax: (312)-886-2804

Dallas, TX
3900 Karina Street, Suite 228
Denton, TX 76208
(940) 891-8930 / Fax: (940) 891-8959

El Centro, CA
321 South Waterman Avenue
Room #108
El Centro, CA 92243
(760) 335-3549 / Fax: (760) 335-3534

El Paso, TX
Federal Office Building
4050 Rio Bravo Suite 200
El Paso, TX 79902
(915) 534-6133 / Fax: (915) 534-6146

Houston, TX
5850 San Felipe Road, Suite 300
Houston, TX 77057
(713) 706-4611 / Fax: (713)-706-4625

Los Angeles, CA
222 N. Sepulveda Blvd, Suite 1640
El Segundo, CA 90245
(310) 665-7320 / Fax:(310)-665-7309

McAllen, TX
Bentsen Tower
1701 W. Business Highway 83, Rm.510
McAllen, TX 78501
(956) 618-8151 / Fax: (956) 618-8145

Miami, FL
3401 SW 160th Ave, Suite 401
Miramar, FL 33027
(954) 602-1980/Fax: (954) 602-1033

New York, NY
10 Exchange Plaza, Suite 804
Jersey City, NJ 07302

Philadelphia, PA
5002B Greentree Exec. Campus,
Route# 73 and Lincoln Drive
Marlton, NJ, 08053
(856) 968-6600 / Fax: (856)-968-6610

San Francisco, CA
1301 Clay St, Suite 420N
Oakland, CA 94612-5217
(510) 637-4311 / Fax: (510) 637-4327

St. Thomas, VI
Office 550 Veterans Drive,
Room 207A
St. Thomas, USVI 00802
(340) 777-1792 / Fax: (340) 777-1803

San Diego, CA
701 B Street, Room #560
San Diego, CA 92101
(619) 557-5970 / Fax: (619) 557-6518

San Juan, PR
New San Juan Office Building
159 Chardón Avenue, 5th Floor
Hato Rey, Puerto Rico 00918
(787) 296-3531 / Fax: (787) 296-3652
Mailing Address: P.O. Box 70105
San Juan, PR 00936

Tucson, AZ
Federal Office Building
10 East Broadway Suite 105
Tucson, AZ 85701
(520) 670-5243 / Fax: (520) 670-5246

Appendix B - Acronyms

ACE	Automated Commercial Environment
ACS	Automated Commercial System
AMO	Office of Air and Marine Operations
AMOC	Air and Marine Operations Center
APATA	Arming Pilots Against Terrorism Act
APHIS	Animal and Plant Health Inspection Service
ATM	Automated Teller Machine
ATSA	Aviation and Transportation Security Act
CBP	Customs and Border Protection
CIO	Chief Information Officer
CIS	Citizenship and Immigration Services
CSI	Container Security Initiative
C-TPAT	Customs Trade Partnership Against Terrorism
DBMS	Distribute Database Management Systems
DHS	Department of Homeland Security
DOJ	Department of Justice
EDS	Explosive Detection Systems
EOIR	Executive Office for Immigration Review
EPA	Environmental Protection Agency
EP & R	Emergency Preparedness and Response
ETD	Explosive Trace Detection
FAA	Federal Aviation Administration
FAM	Federal Air Marshals
FAMS	Federal Air Marshal Service
FAR	Federal Acquisition Regulation
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FSD	Federal Security Directors
FTE	Full Time Equivalent
GAO	General Accounting Office
HAS	Homeland Security Act
HITRON	Helicopter Interdiction Squadron
HSARPA	Homeland Security Advanced Research Projects Agency
HSOC	Homeland Security Operations Center
IAIP	Information Analysis and Infrastructure Protection
ICE	Immigration and Customs Enforcement
IDS	Integrated Deepwater System
III	Interstate Identification Index

INS	Immigration and Naturalization Service
IRP	Institutional Removal Program
IT	Information Technology
LESC	Law Enforcement Support Center
MSST	Maritime Safety and Security Teams
NCR	National Capital Region
NCRCC	National Capital Region Coordination Center
NDCP	National Drug Control Program
NFIP	National Flood Insurance Program
NSEERS	National Security Entry Exit Registration System
ODP	Office of Domestic Preparedness
OIG	Office of Inspector General
OJP	Office of Justice Programs
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
POE	Ports of Entry
S&T	Science and Technology
SCI	Sensitive Compartmented Information
SENTRI	Secure Electronic Network for Traveler's Rapid Inspection
SEVIS	Student and Exchange Visitor Information System
SHSAS	State Homeland Security Assessment and Strategy
TARS	Tethered Aerostat Radar System
TSA	Transportation Security Administration
TWIP	Transportation Worker Identification Program
US-VISIT	United States Visitor and Immigrant Status Indication Technology System
VSO	Visa Security Office
VWP	Visa Waiver Program

Appendix C - Performance Goals, Measures, and Accomplishments

FY 2003

Performance Goals and Indicators	**Fiscal Year 2003 Actual Performance**
Goal 1. Add value to DHS programs and operations.	
1.1 Provide audit and inspection coverage of 75 % of DHS' critical mission areas, the President's Management Agenda, and the most serious management challenges facing DHS	83%
1.2 Achieve at least 75 % concurrence with recommendations contained in OIG audit and inspection reports (excludes grant audits).	84%
1.3 Complete draft reports for at least 75% of inspections and audits within six months of the project start date (excludes grant audits).	67%
Goal 2. Ensure integrity of DHS programs and operations.	
2.1 At least 75% of substantiated investigations are accepted for criminal, civil, or administrative action.	80%
2.2 At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.	57%
2.3 Provide audit coverage of $500 million of DHS grant programs	$404 million.

2.4	Achieve at least 75% concurrence with recommendations on grant audits.	99%

Goal 3. Deliver quality products and services.

3.1	Establish and implement an internal quality control review program covering all elements of DHS OIG.	FY 2004 Initiative
3.2	Establish and implement an employee training program for DHS OIG.	FY 2004 Initiative
3.3	Establish and implement a performance evaluation program for employees of DHS OIG.	In process
1.1	Establish and implement an awards program for DHS OIG.	In process

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.

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.