DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Fiscal Year 2005
Annual Performance Plan
(Revised May 2005)

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

A Message From the Acting Inspector General

This is an update to our Fiscal Year (FY) 2005 Annual Performance Plan of the Department of Homeland Security's (DHS) Office of Inspector General (OIG). This update outlines the projects that we have underway or intend to undertake during the remaining of this fiscal year to evaluate the department's programs and operations.

In developing our FY 2005 Plan, including the revisions contained herein, 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 economy, effectiveness, and efficiency, as well as, to prevent and detect fraud, waste, and abuse in the department's programs and operations.

Richard L. Skinner

Richard L. Skinner
Acting Inspector General

Table of Contents

Chapter **Page**

Chapter 1 - OIG Mission and Responsibilities

The Homeland Security Act of 2002 provided for the establishment of an Office of Inspector General (OIG) to ensure independent and objective audits, inspections, and investigations of the operations of the Department of Homeland Security (DHS).

An Inspector General, who is appointed by the President and confirmed by the Senate, reports directly to both the Secretary of DHS and the Congress. Barring exceptional circumstances, the Inspector General may inspect, audit, or investigate anyone in the department or any program or operation of the department. To assure the Inspector General's independence and objectivity, the OIG has its own budget, contracting, and personnel authority separate from that of the department. Such authority enhances the OIG's ability to promote economy, effectiveness, and efficiency within the department and to prevent and detect fraud, waste, and abuse in the department's programs and operations.

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

- Conduct and supervise independent and objective audits and investigations relating to department programs and operations.
- Promote economy, effectiveness, and efficiency within the department.
- Prevent and detect fraud, waste, and abuse in the department's programs and operations.
- Keep the Secretary and Congress fully and currently informed of problems in department programs and operations.
- 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: This office consists of the Inspector General, the Deputy Inspector General, a congressional liaison and media affairs officer, and support staff. It provides executive leadership to the OIG with seven full-time equivalent (FTE) employees.

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 OIG subpoenas, False Claims Act and Civil Monetary Penalty Act claims, as well as suspension and debarment actions. The office has ten FTE.

Office of Audits: The Office of Audits (see Briefing Book for description of Audit responsibilities). It also performs grant and contract audits. The office has a total of 218 FTE.

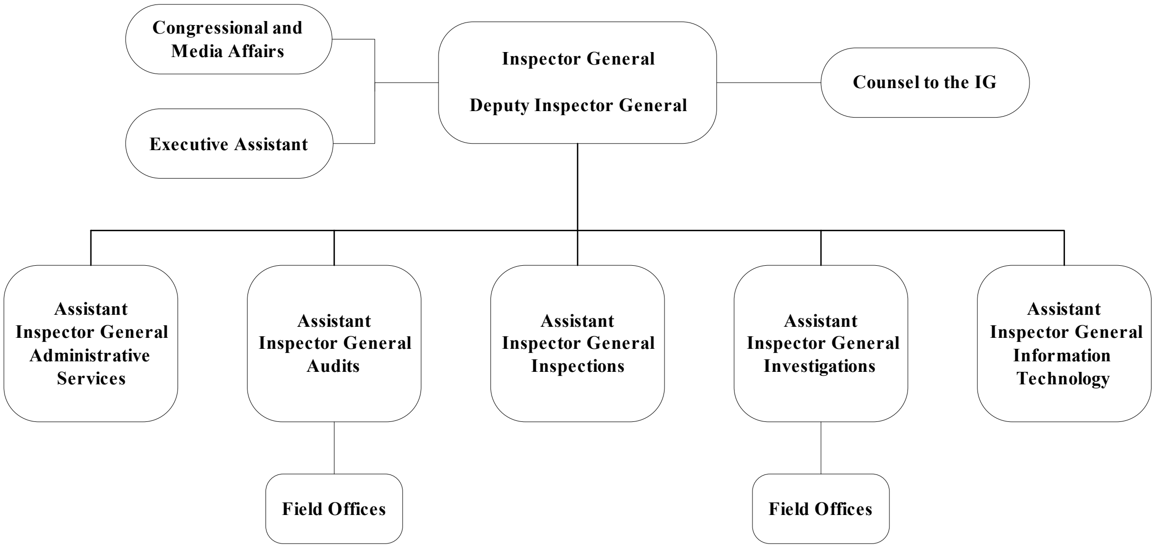
Office of Inspections and Special Reviews: The Office of Inspections and Special Reviews complements the work of the Office of Audits by providing quick and less-structured reviews of those DHS programs and operations that are of pressing interest to department managers, the Congress, or the Inspector General. This office has 31 FTE.

Office of Information Technology: The Office of Information Technology evaluates DHS' information management, cyber-infrastructure protection, and systems integration activities. Additionally, the office assesses DHS' information security program as mandated by the Federal Information Security Management Act. This office has 32 FTE.

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. Additionally, it oversees the investigative activity of the department's various internal affairs offices. This office has 172 FTE.

Office of Administration: The Office of Administration 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 Congress. This office has 32 FTE.

Organizational Chart


Congressional and Media Affairs
Executive Assistant
Inspector General
Deputy Inspector General
Counsel to the IG
Assistant Inspector General Administrative Services
Assistant Inspector General Audits
Assistant Inspector General Inspections
Assistant Inspector General Investigations
Assistant Inspector General Information Technology
Field Offices
Field Offices

Chapter 3 - FY 2005 Planning Approach

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

This plan describes more projects than may be completed in FY 2005, especially since developments and requests from DHS management and Congress during the year will necessitate some projects that cannot be anticipated. Resource issues too may require changes to the plan in some way as the year progresses. Also, the plan includes projects that were initiated but not completed during FY 2004. Finally, the plan contemplates that some jobs listed here will start during FY 2005 but will carry over into FY 2006.

In establishing priorities, we 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:

- Consolidation of Department components
- Border Security
- Transportation Security
- Infrastructure Threat Assessment
- Integration of Information Systems
- Security of Information Technology Infrastructure
- Human Capital Management
- Financial Management
- Contract Management
- Grants Management

In addition, in keeping with the priorities of both the Secretary and Congress, we 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, we will determine how well DHS is performing and will be able to recommend ways to improve the efficacy of DHS' programs and operations.

We also will strive to foster open communications and have a consultative and collaborative working relationship with management officials at all levels of the department.

Chapter 4 - Allocation of Resources

On October 18, 2004, President Bush signed the FY 2005 *Homeland Security Appropriations Act*, which provides the OIG with total budget authority of $82,317,000 and a total of 502 FTE.

Department of Homeland Security
Office of Inspector General

Salaries and Expenses
Classification by Objects
(Dollars in Thousands)

Object Classification		FY2004 Actual	FY2005 Enacted	Change
11.1	Perm Positions	$33,025	$41,087	$8,062
11.3	Other than perm	243	175	(68)
11.5	Other per comp	2,640	3,368	728
11.8	Spec Srvc Pay	4	-	(4)
12.1	Benefits	10,647	12,646	1,999
13.0	Benefits-former	-	-	-
	Total, pers. comp. & benefits	$46,559	$57,276	$10,717
21.0	Travel	$4,417	$5,371	$954
22.0	Transportation of things	235	72	(163)
23.1	GSA rent	4,150	6,173	2,023
23.2	Other rent	-	-	-
23.3	Communication, Utililities, and misc charges	1,933	3,110	1,177
24.0	Printing	28	51	23
25.1	Advisory & Assistance Services	4,343	2,674	(1,669)
25.2	Other Services	1,156	2,502	1,346
25.3	Purchase from Govt. Accts.	7,478	6,272	(1,206)
25.4	Operation & maintenance of facilities	-	-	-
25.5	Research & Development	-	-	-
25.6	Medical care	-	-	-
25.7	Operation & maintenance of equipment	88	123	35
25.8	Subsistence & Support of persons	-	-	-
26.0	Supplies & materials	729	909	180
31.0	Equipment	4,802	2,728	(2,074)
32.0	Land & Structures	2,549	1,641	(908)
41.0	Grants/Subsidies/Contributions	-	-	-
42.0	Indemnity	14	23	9
43.0	Interest and Dividends	-	-	-
44.0	Refunds	-	-	-
91.0	Unvouchered	28	100	72
99.0	Other			-
	Total, other objects	$31,950	$31,749	$(201)
	Total Direct Obligations	$78,509	$89,025	$10,516
	Unobligated balance, start of year	(5,122)	(7,708)	(2,586)
	Recoveries	(1,130)	(1,000)	130
	Unobligated balance, end of year	7,708	2,000	(5,708)
	Total Requirements	$79,965	$82,317	$2,153

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, our performance goals and measures will be updated annually for maximum effectiveness in meeting the changing needs of DHS, consistent with our statutory responsibilities. In addition to the mandatory requirements, performance measures identified here serve as a basis to determine the overall effectiveness of our work.

FY 2005
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.

2.4 Achieve at least 75% concurrence from DHS management with OIG 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.

3.4 Establish and implement an awards program for DHS OIG employees.

Chapter 6 - Performance Initiatives – Project Narratives

SPECIAL INITIATIVES

MAX/HR System Acquisition and Development (Final Report - February 2006)

In an effort to move forward with the proposed "pay for performance" model, Department of Homeland Security officials have awarded a blanket purchase agreement, with a maximum potential value of $175 million over three years, to Northrop Grumman IT to modernize the department's current human resources program. Department officials have indicated that the contract includes provisions charging Northrop Grumman with project management, integration services, performance measures, job classification and labor relations. Recent reports indicate that the contractor will also support training, communication, organizational change management and assist in the implementation of an enterprise-wide IT system in line with President Bush's E-Government initiative.

Audit Objectives: Determine effectiveness of the MAXHR strategy and proposed system as they relate to system development, oversight, training and development, clearance, recruitment and retention, assignments, and performance measurement of agency personnel-especially IT personnel. *Office of Information Technology*

DHS Procurement Systems (Final Report - January 2006)

The eight distinct procurement offices within DHS obligate and administer billions of dollars annually in acquiring everything DHS needs to deliver upon its mission, including information technology, telecommunications, and research and development. Further, these offices rely on a variety of IT systems to support their procurement functions, systems that are often inefficient, and costly to operate and maintain. In addition, these systems do not provide DHS managers with the information needed to adequately control procurement processes, and prevent fraud and misuse.

Audit Objectives: Determine the effectiveness of DHS efforts to reengineer its procurement processes, and develop and implement standard IT systems to support those processes. *Office of Information Technology and Office of Audits*

DHS Systems for Sharing Intelligence (Final Report - November)

Many of DHS' organizational elements have their own intelligence offices to support their respective missions. These offices rely on a variety of information systems to acquire and process intelligence data, and to share this information with other organizational elements, other federal agencies, and state and local governments. Generally, these systems were developed and operate solely to support their legacy agencies, and thus may not be interoperable, or capable of sharing data effectively.

Audit Objectives: Determine the efficiency and effectiveness of information systems used by DHS intelligence offices to acquire, process, and share information.
Office of Information Technology and Office of Inspections and Special Reports

Proposal to Merge ICE and CBP (Final Report - August)

On February 8, 2005, we initiated a special review that will examine the merits of a proposal to merge the bureaus of Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). The review was requested by the Chairman of the Senate Homeland Security and Governmental Affairs Committee at a hearing on January 26, 2005. Our review will include an examination of operations of CBP and ICE, as well as their interactions with other agencies and DHS entities. Also, we will consider the role of the "BTS element," i.e., the headquarters infrastructure that was proposed to be eliminated or "flattened" under the proposal. In addition to addressing the question of whether a merger should occur, we will seek to identify significant problems cited in support of the proposal that may warrant separate corrective attention. *Office of Inspections*

BORDER AND TRANSPORTATION SECURITY (BTS)

BTS Information Technology (IT) Integration (Final Report - February 2006)

Integrating component functions to enhance efficiency and create greater accountability is one of the top priorities within the department. In this regard, the BTS directorate - comprised of Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and Immigration and Customs Enforcement (ICE) - is challenged with providing seamless border services. A BTS chief information officer (CIO) position, recently created to provide directorate-wide IT governance, will identify redundancies and consolidate the various technology systems, programs, and networks across the six organizations as part of a BTS technology integration initiative. Also, the CIO will integrate the BTS infrastructure with the DHS IT infrastructure.

Audit Objectives: Determine the effectiveness of BTS' approach to improving IT management, including the organizational structure of the CIO; authorities and reporting relationships; ability to guide IT investments strategically; and, its management of the BTS IT integration initiative in correlation with the overall DHS IT integration initiatives. *Office of Information Technology*

IMMIGRATION AND CUSTOMS ENFORCEMENT BUREAU

ICE Budget Problems (Final Report - June)

In June of 2004, the Ranking Member of the House Select Committee on Homeland Security expressed concerns about ICE operational problems that allegedly stemmed from ICE's accounting system and budgetary controls. The concerns were based on confidential information received from ICE employees. In addition, the FY 2004 DHS financial statement audit raised questions about the accuracy of certain ICE account balances and reliability of accounting controls.

Audit Objective: Determine the validity of concerns about ICE's operational issues and ICE's financial system and whether ICE violated the *Anti-Deficiency Act***.** *Office of Audits*

Detention of Illegal Aliens (Final Report - July)

ICE is responsible for providing safe, secure and humane confinement of persons detained; providing effective control of persons released into the community during immigration proceedings or while awaiting removal; and, removing individuals, especially criminals and other threats to national security and public safety, who are unlawfully present in the United States. The immigration enforcement process starts with apprehension and ends with a grant of approval to stay in the United States or be removed. The Executive Office of Immigration Review (EOIR) of the Department of Justice (DOJ) determines the legal status and admissibility of an alien. Aliens are detained according to priorities, such as legal requirements, funding sources, availability of detention facilities, and resource limitations. As required by law, aliens convicted of aggravated felonies are the first priority, followed by other aliens convicted of criminal behavior, with administrative deportation cases given the lowest priority. The detention period varies according to the circumstances of each alien but can be as short as few days and as long as a period of years. The average detention stay is about 40 days.

Audit Objective: Determine whether ICE has sufficient resources and facilities to house detainees. *Office of Audits*

ICE Institutional Removal Program (Final Report - July)

ICE's Institutional Removal Program (IRP):

1. Identifies criminal aliens in federal, state, and local correctional facilities who may legally be "removed" or returned to their home countries because they were never entitled to be in this country 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.

Ideally, the IRP process begins with the identification of potentially deportable foreign-born inmates as they enter the correctional system. It 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 released into ICE custody for immediate removal. The IRP is a cooperative effort among ICE, the EOIR, and participating federal, state, and local correctional agencies. ICE statistics show that in FY 2001, of the 71,063 criminal aliens who the former Immigration and Naturalization Service (INS) removed, 30,002 were removed via the IRP. According to a DOJ OIG report, prior to the transfer of immigration functions to DHS, the INS did not effectively manage the IRP.

Audit Objectives: Determine whether ICE management: (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*

Treatment of Aliens Held on Immigration Charges (Final Report - September)

Shortly after the September 11, 2001, attacks, the Attorney General directed the Federal Bureau of Investigations and other federal law enforcement personnel to use "every available law enforcement tool" to arrest persons who "participate in, or lend support to, terrorist activities." One method used by law enforcement authorities to accomplish this objective is to detain aliens suspected of having possible ties to terrorism. Accordingly, many aliens were arrested and detained for violating federal immigration law. The DOJ OIG conducted a review to examine the treatment of detainees arrested in connection with the department's September 11 terrorism investigation focusing on the INS detainees housed at the Bureau of Prison's Metropolitan Detention Center in Brooklyn, New York, and the Passaic County Jail in Paterson, New Jersey. Numerous concerns surfaced regarding prolonged or indefinite detention, as well as other areas where inappropriate treatment of aliens occurred. The DOJ OIG made 21 recommendations; seven of those recommendations addressed improvements needed in ICE's policies and practices for detaining aliens. In response to the recommendations, ICE's Office of Detention and Removal Operations (DRO) issued new standards requiring ICE officials to visit detainees periodically to monitor conditions of confinement and address concerns, as appropriate. However, we have received a number of allegations of abuse involving detainees held at facilities used by DRO, as well as holding facilities used by the CBP to temporarily hold detainees for DRO.

Audit Objective: Assess the treatment of aliens held on immigration charges, including ICE's monitoring and oversight of the conditions of confinement for detainees. *Office of Audits*

Apprehension and Detention of Juveniles Who Enter the Country Illegally (Final Report - July)

ICE's Office of Detention and Removal has defined policy and procedures regarding the proper handling of unaccompanied alien juveniles taken into federal custody as a result of their unlawful immigration status. DHS' juvenile guidelines address the responsibilities related to unaccompanied alien juveniles who enter the United States illegally, violate their legal status, or commit a deportable crime. As part of the restructuring of INS, the responsibilities related to the apprehension, care, and custody of unaccompanied alien juveniles have been split among ICE, CBP, and the Department of Health and Human Services.

<u>Inspection Objectives</u>: Assess the effectiveness of coordination between CBP, and ICE after CBP apprehends and initially detains unlawful juvenile aliens at the border or at U.S. ports of entry. The OIG is (1) analyzing the process by which CBP informs ICE that a juvenile alien has been apprehended and the process for transferring the juvenile alien to ICE custody; (2) reviewing the effectiveness of the current policy of custody and transfer of unaccompanied juvenile aliens to the Office of Refugee Resettlement, Department of Health and Human Services; and (3) assessing the progress of BTS in implementing three open recommendations from a legacy Department of Justice OIG report. *Office of Inspections and Special Reviews*

Immigration and Customs Enforcement Compliance Enforcement Office (Final Report - June)

Admittance into the United States is based on certain terms and conditions. While most foreign visitors comply with these terms and conditions, an untold number violate their agreement with the United States, blend into society, and actively seek to avoid detection, arrest, or and removal. Consequently, U.S. immigration authorities need to identify, apprehend, detain and remove these individuals in an effective and efficient manner. To this end, sophisticated tracking and monitoring databases were developed and employed.

The newly-created Compliance Enforcement Office, in the National Security Investigations Division, oversees the compliance and enforcement of various programs aimed at protecting the United States by identifying and apprehending those individuals who have violated the purpose and terms of their admission into the United States, as well as identifying individuals and organizations using the U.S. immigration system who may constitute a threat to national security. Systems used to support this effort include the Student and Exchange Visitor Information System (SEVIS), the United States Visitor and Immigrant Status Indication Technology (US-VISIT), and the National Security Entry/Exit Registration System (NSEERS).

<u>Inspection Objectives</u>: Determine the effectiveness of ICE in identifying, locating and removing aliens who have violated the purpose and terms of their admission into the United States. We are examining the strategies, plans, procedures and systems used by the Compliance Enforcement Office and evaluating how data from systems such as SEVIS, US-VISIT, and NSEERS is used to locate immigration violators. *Office of Inspections and Special Reviews*

Removal of a Canadian National to Syria (Final Report - October)

We will evaluate the decision by the INS to remove a Canadian and Syrian citizen to Syria where he alleges that he was tortured. The INS at JFK International Airport detained this person on September 26, 2002, while he was returning to Montreal from a family vacation in Tunisia. He was carrying a Canadian passport. According to news reports, U.S. officials alleged that he had connections to al-Qaeda; and he was consequently detained and questioned before being removed (an "extraordinary rendition") to Syria. The Ranking Member of the House Committee on the Judiciary requested the review.

Inspection Objective: Evaluate how U.S. immigration officials arrived at their decision to remove this person to Syria. We are examining policies used by immigration officials to select among alternative destination countries for non-immigrants who are removed. *Office of Inspections and Special Reviews*

CUSTOMS AND BORDER PROTECTION BUREAU

Targeting of Oceangoing Cargo Containers (Final Report - June) (Mandatory)

On August 9, 2004, Congress enacted the *Coast Guard and Maritime Transportation Act of 2004*. The OIG is responsible for evaluating and reporting on the effectiveness of the cargo inspection targeting system for international intermodal cargo containers. An aspect of the CBP mission is to address the potential threat posed by the movement of oceangoing containers. Approximately 90% of the world's cargo moves by container. In 2002, approximately 7 million containers arrived at U.S. seaports. Inspectors assigned to seaports help determine which containers entering the country will undergo inspections, and then perform physical inspections of such containers. CBP is implementing a layered approach that attempts to focus resources on potentially risky cargo containers while allowing other cargo containers to proceed without disrupting commerce. As part of its layered approach, CBP employs its Automated Targeting System (ATS) computer model to review documentation on all arriving containers and help select or target containers for additional scrutiny. The ATS was originally designed to help identify illegal narcotics in cargo containers, but was modified to help identify all types of illegal contraband used by smugglers or terrorists. Other components of the layered approach include the Container Security Initiative and the Customs-Trade Partnership against Terrorism.

Audit Objective: Determine the effectiveness of the CBP Targeting System to detect potential acts of terrorism using oceangoing cargo containers, and identify any actions needed to remedy deficiencies in targeting containers for inspection. *Office of Audits*

Expenditures and Obligations for Port Security (Final Report - January 2006) (Mandatory)

According to Section 808 of the *Coast Guard and Maritime Transportation Act of 2004*, the OIG is required to review annually the funding of investigations, pilot programs, and grant programs established under Section 808 to ensure that the expenditures and obligations of funds are consistent with the purposes for which they are provided, and report the findings to Congress. The investigation programs include such items as methods or programs to increase the ability to inspect vessels, cargo, crewmembers, or passengers; equipment to accurately detect explosives, chemical or biological agents, or nuclear or radiological materials; improved tags and seals designed for use on shipping containers; tools to increase the awareness of maritime areas and mitigate the consequences of a transportation security incident; improved container design, including blast-resistant containers; and, methods to improve security and sustainability of port facilities. Pilot projects for implementing technology may test the effectiveness and applicability of new port security projects at U.S. ports. Grant programs include National Port Security centers, which are nonprofit institutions of higher learning conducting investigations in collaboration with ports and the maritime transportation industry focused on enhancing security of the nation's ports.

Audit Objective: Determine to what extent the expenditures and obligations of funds for investigations, pilot programs, and grant programs established under Section 808 are consistent with the purposes for which they are provided. *Office of Audits*

CBP's Agricultural Inspection Activities (Final Report - August)

CBP officers and agriculture specialists are responsible for ensuring that infectious plant or animal borne diseases are not introduced into the U.S. by examining passenger luggage and commercial cargo at international airports, seaports, and land border crossings. Under recent free trade agreements, the United States has seen a substantial increase in the numbers of requests for imports into this country. This has placed an added burden on CBP to continue to ensure scientific rigor in its assessment of potential health threats, while at the same time trying not to impede trade and legitimate travel. The 2003 outbreak of monkeypox from imported Gambian giant rats shed light on the lack of coordinated federal oversight to prevent future zoonotic disease outbreaks, as well as the confusing state and federal laws that govern such imports. The Centers for Disease Control and Prevention, the U.S. Department of Agriculture, and the U.S. Food and Drug Administration are responsible for any embargoes on importing, distributing, selling, or transporting of certain animal or vegetative species. These agencies, however, cannot enforce any bans without support from CBP and the U.S. Fish and Wildlife Service. Likewise, the CBP officers and agriculture specialists cannot detect or prevent diseases spread by animal or plant life without adequate support and intelligence from the other agencies.

Audit Objective: Determine to what extent CBP's resources, internal policies and procedures, and coordination with other governmental entities are adequate to detect potential bio-terrorist agents and threats, zoonotic and plant-borne disease characteristics, and potential threats of epidemics before they can be transmitted to the American public. *Office of Audits*

CBP's Efforts to Deploy Radiation Portal Monitors (RPM) to Priority Seaports (Final Report - September)

Approximately 90% of the world's cargo moves by container ships. In 2002, approximately seven million containers arrived at U.S. seaports. Terrorist action related to cargo containers and to U.S. ports could paralyze the maritime trading system and quickly disrupt U.S. and global commerce. To prevent this from happening, CBP is using RPM that are capable of detecting radiation from materials of greatest concern. There are 22 major seaports designated to receive RPMs. Several factors, such as seaport size, complexity of operations, and mix of private and public entities that own or lease the land, could influence the successful roll out of the RPMs.

Audit Objective: Determine to what extent CBP has a complete and workable plan for deploying and effectively operating RPMs at major U.S. seaports, and how the new technologies CBP is deploying will impact operations at the ports. *Office of Audits*

Contractor Oversight and Supervision of the US-VISIT Contract (Final Report - February 2006)

On May 19, 2003, DHS announced the establishment of US-VISIT, an automated system to track and control the entry and exit of all aliens entering and leaving the country through air, land and sea ports of entry. This entry-exit system will utilize biometric technologies, such as fingerprints and photographs in addition to machine-readable, tamper-resistant documents, to provide authorized personnel from CBP and other agencies at consular posts abroad with access to integrated alien arrival and departure data. US-VISIT is supported by a number of contracts, the largest of which recently was signed with Accenture LLP. The five-year Accenture LLP contract is valued at $10 billion.

Audit Objective: Determine to what extent the US-VISIT program vision, procurement strategy, and technology will meet program requirements and how well the US-VISIT program management office is monitoring and managing compliance with contract requirements. *Office of Audits*

Information Security Controls Implemented for the US-VISIT Program (Final Report - August)

The *Naturalization Service Data Management Improvement Act of 2000* mandated the creation of an automated entry exit system that integrates electronic alien arrival and departure information. As a result, the US-VISIT program is a top priority for DHS. The system is a continuum of security measures that begin before an individual enters the United States and continues through arrival and departure from the United States. US-VISIT aims to ensure the integrity of the immigration system, while safeguarding the personal privacy of our visitors. US-VISIT is intended to make it more difficult for an individual to claim another person's identity, by collecting biometric identifiers such as fingerprints and digital photos. The system also will collect information that will allow DHS to identify individuals that violate entry requirements or overstay or violate the terms of their stay.

Audit Objective: Determine whether the US-VISIT Program provides adequate system security controls over sensitive and biometric data. *Office of Information Technology*

Encounters with Suspected Terrorists at Ports of Entry (POE) (Final Report - September)

It is unlawful for any person to enter the United States at any place other than a designated POE. Inspection of visitors at POE facilitates legal entries of admissible persons and intercepts *mala fide* applicants for admission. *Mala fide* travelers include terrorists, would-be illegal aliens, alien smugglers, and other criminals. Various systems assist CBP inspectors in verifying that applicants for admission are not inadmissible and checking that they are not wanted by federal law enforcement officials.

Inspection Objectives: Assess actions taken by CBP inspectors when an alien who is the subject of a terrorism lookout alert applies for admission at a POE. We will analyze the procedures used by CBP at air and land POE, to determine whether appropriate U.S. agencies are contacted by CBP, and will review subsequent actions to resolve the alien's status. Also, we will examine the purposes of the various U.S. watch lists, related terrorism lookouts, and the criteria for entering the name of an alien on a watch list. *Office of Inspections and Special Reviews*

Container Security Initiative (CSI) (Final Report - July)

About 90% of the world's cargo moves by container. In 2002, approximately seven million containers arrived at U.S. seaports. Shipment of cargo via sea containers is the primary system of global trade, yet it is highly susceptible to use by terrorists. The CSI is a CBP initiative designed to strengthen port and maritime security without interrupting trade flows. The main emphasis of CSI is to protect trade that is moved by oceangoing sea containers from use by terrorists. The primary purpose of CSI is to protect the global trading system and the trade lanes between the CSI ports and the U.S. Under the CSI program, a team of officers is deployed to work with the host nation counterparts to target all containers that pose a potential threat. Announced in January 2002, CSI was first implemented in the ports shipping the greatest volume of containers to the United States. It is now operational in 25 ports.

Audit Objective: Determine the extent to which the CSI is using intelligence and automated information to identify and target containers that pose a risk for terrorism and employing non-intrusive and physical inspections to examine high-risk containers at foreign ports. Also, we will assess the procedures and practices over the physical security of containers while at the ports. *Office of Audits*

CBP Screening of Trucks Carrying Canadian Solid Waste (Final Report - July)

A Congressman from Michigan requested a review of the effectiveness of CBP's screening of trucks carrying Canadian solid waste. The concern was due to the reports of trucks from Canada coming into Michigan carrying medical waste, illegal drugs and large amounts of currency.

__Audit Objective__: Determine whether the methodologies and technologies used by CBP to screen trucks hauling solid waste from Canada are as effective as those used by CBP to screen other items of commerce entering the United States by commercial motor vehicle transport. *Office of Audits*

Use of Remote Surveillance Technology along United States Borders (Final Report - July)

The northern border separating mainland United States and Canada is 4,121 miles long and includes 430 official and unofficial ports of entry. The border is difficult to patrol, despite the presence of more than 1,000 agents. The southern border separating the United States and Mexico is 2,062 miles long and consists of 30 ports of entry and innumerable unofficial crossings. More than 10,000 border patrol agents are stationed on the southern border. Despite this large presence, illegal border crossings and significant drug smuggling activities occur frequently. Borders are monitored and protected by border patrol agents, video cameras, ground sensors, physical barriers, land vehicles, and manned aircraft. CBP has increased efforts to employ new and more sophisticated technological instruments and systems to increase surveillance of the border to detect and apprehend illegal crossers.

__Inspection Objectives__: Analyze use of remote surveillance technology along our borders. Specifically, we are: (1) evaluating the effectiveness of border surveillance, remote assessment, and monitoring technology in assisting CBP to detect illegal entry into the United States; (2) examining the effectiveness of the Integrated Surveillance Intelligence System (ISIS) as a baseline to assist CBP in detecting illegal entry into the United States; (3) assessing where ISIS coverage currently exists, where additional ISIS coverage is needed, and how technology initiatives - such as the Unmanned Aerial Vehicles - will complement ISIS in monitoring the United States' northern and southern borders; (4) evaluating the extent that CBP is emphasizing technology development and integration as a "force multiplier"; and, (5) examining how effective CBP is in using these technologies to accurately assess and respond to illegal traffic along the border. *Office of Inspections and Special Reviews*

TRANSPORTATION SECURITY ADMINISTRATION

TSA's Secondary Screening Procedures (Final Report - July)

In September 2004, TSA enhanced its secondary screening procedures after the near simultaneous crashes of two Russian passenger aircraft on August 24, 2004, believed to be caused by terrorists with explosive devices. One enhancement involved more frequent use of pat-down searches. According to recent media reports, TSA screeners at airport checkpoints are subjecting select female passengers to intrusive body searches as part of its revised secondary screening process. In reaction to the 300 complaints it has received, TSA is taking steps to prepare passengers for physical inspection.

Audit Objective: Determine whether TSA adequately advises passengers of their rights under the screening process, and how well TSA accommodates requests related to those rights. Additionally, we will determine whether secondary screening practices are applied proportionately to males and females; screeners are adequately trained to perform body searches; and, TSA has processes in place to investigate and resolve complaints about the process. *Office of Audits*

TSA Recruitment Program (NCS Pearson Contract) (Final Report - July)

As required by ATSA, TSA hired a federalized airport screener workforce within the mandated one-year time period. Troubled by press reports of perceived wasteful government spending by TSA's recruitment contractor, several U.S. Senators expressed concerns about the cost of recruitment activities performed at various nationwide resort hotels and requested us to review TSA's recruitment program. Congressional concerns included TSA's oversight, criteria governing the assessment center selection process, basis for selection of specific assessment center sites, number of recruitment trips to resort communities, and money spent on TSA recruitment as well as number of personnel hired.

Audit Objective: Determine to what extent TSA adequately managed and oversaw the establishment of screener assessment centers and the recruitment process to meet federal hiring mandates in a cost effective manner. *Office of Audits*

TSA Air Cargo Security (Final Report - July)

The air cargo industry is composed of thousands of shippers, 226 domestic and foreign aircraft operators providing services through 2,789 stations at United States airports, and approximately 3,200 Indirect Air Carriers with over 10,000 business locations. Together, these entities transport approximately $30 billion worth of goods per year, including an estimated 12.5 million tons of air cargo transported and 2.8 million tons on passenger planes. The purpose of the TSA air cargo security program is to provide an effective security framework that is risk-managed, addresses vulnerabilities in the pre-TSA system, is fiscally responsible, and does not unduly impede the flow of commerce. It directly supports TSA's goal of preventing terrorists and other individuals from disrupting the transportation system and harming its users.

Audit Objective: Determine whether the policies, procedures, and controls used by TSA ensure the security of cargo on passenger aircraft. The audit will include the known shipper program and the regulatory cargo inspection program. *Office of Audits*

Implementation of Aviation Security Requirements at Foreign Airports (Final Report - June)

Security at foreign airports is a major challenge for TSA. The agency is responsible for ensuring that appropriate security measures and protocols are established and implemented at foreign airports that fly planes to airports in the United States. TSA is required to conduct periodic security assessments of foreign air carriers and airports that fly domestically. After the "shoe bomber" incident, bombing attempt concerns were raised regarding the effectiveness of security screening at foreign airports to detect explosives on persons and carry-on baggage at foreign airports. The ranking member of the Select Committee on Homeland Security requested that we review efforts by TSA to address the threat from terrorists attempting to carry an explosive device on their person or in their carry-on luggage at a foreign airport.

Audit Objective: Determine whether the security program requirements for foreign air carriers and airports are compatible with the requirements for U.S. aircraft operators; determine the efficacy of TSA's efforts to perform periodic assessments at foreign airports; and, determine whether the security requirements at selected airports are met. *Office of Audits*

Aviation Security Service Fees (Final Report - July)

TSA requested that we review the collection of passenger security fees and the infrastructure security fees computed and collected by three different airlines. These fees were instituted after the federal government took over the responsibility for aviation security post September 11, 2001.

Audit Objective: Determine whether: (1) collection and remittance to TSA of passenger and infrastructure security fees are accurate, (2) the controls used by TSA and air carriers to ensure proper payment are effective, and (3) TSA complies with legislative reporting requirements and guidelines. *Office of Audits*

TSA's Revised Contact Center Procedures and Aircraft Inspection Requirements (Final Report - July)

The House of Representatives Committee on Government Reform requested that we review the circumstances that allowed a passenger to breach airport passenger security checkpoints on six separate occasions, hide weapons on commercial aircraft, and allow the weapons to remain undetected for a lengthy period of time. The Committee also asked that we review the contact center's procedures for reviewing and reacting to communications from the public that contain potential security violations, threat information, or criminal activities.

Audit Objective: Determine how the passenger breached security procedures; whether TSA's actions upon notification of the discovery of the prohibited items were appropriate; whether the corrective actions that TSA implemented were sufficient; and, whether there are any systemic problems that need to be addressed by TSA. *Office of Audits*

TSA's Federal Flight Deck Officer Program (Final Report - September)

The Arming Pilots Against Terrorism Act was enacted as part of the *Homeland Security Act of 2002*. It required TSA to establish a program to select, train, deputize, equip and supervise volunteer pilots of air carriers for the purpose of defending flight decks against acts of criminal violence and air piracy. Initially, the Federal Flight Deck Officer program was limited to volunteer pilots of passenger aircrafts. However, legislation was passed that expanded the eligibility to other passenger aircraft flight crew personnel and cargo flight crew members. 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 long-standing controversy in both the media and the Congress.

Audit Objective: Determine the efficacy of TSA's implementation of the Federal Flight Deck Officer program. We will focus on how the pilots are screened and selected for the program and the adequacy of the training provided. *Office of Audits*

Unisys Contract (Final Report - August)

TSA awarded a contract to Unisys to establish IT and telecommunications infrastructure support and services for TSA employees, set up a new security operation system for 429 airports, and expand security operations to other modes of transportation. The $1 billion task order has a 3-year base with two 2-year option periods. The Chairman of the Transportation and Infrastructure Committee requested that we review TSA's management and oversight for this contract.

Audit Objective: Determine how: 1) the contract and related task order is set up, including how much the government has paid and what products and services the government has received; 2) actual costs compare to what was planned; 3) contractor performance under the task order is measured and how the contractor is performing under those measures; and 4) TSA ensures appropriate use of small businesses and new technology through this contract. *Office of Audits*

TSA's Operating Procedures Allowing Law Enforcement Officers to Carry Weapons Onboard Commercial Aircraft (Final Report - August)

The House of Representatives Committee on Transportation and Infrastructure requested that we review procedures for law enforcement officials on aircraft due to concerns about the number of weapons carried aboard aircraft, TSA's inability to identify law enforcement officers who are authorized to carry weapons while on travel, and the safe and secure air transportation of such weapons.

Audit Objective: Determine: (1) the number of law enforcement officers who are authorized to carry weapons on commercial aircraft; (2) TSA's operating procedures governing law enforcement officers, other than air marshals, who are authorized to carry weapons on commercial aircraft; and, (3) whether current operating procedures ensure the safe and secure transport of weapons on commercial aircraft. *Office of Audits*

Departmental Procedures and Practices Regarding the Handling of Suspicious Passengers Aboard Commercial Aircraft (Final Report - July)

In June 2004, 14 Syrian males, traveling together on a flight from Detroit to Los Angeles, were observed constantly changing seats; grouping in three or four near the lavatory for lengthy periods; one of the individuals carrying a bag and cell phone into the lavatory and staying in the lavatory for an extended period; distracting the flight attendants by engaging them in conversation and constant requests for service; and, failing to comply with flight attendant commands. The activities of the Syrians were reported in a series of newspaper articles and raised concerns about the procedures followed by the U.S. Federal Air Marshals.

Audit Objective: Determine the adequacy of departmental policies and procedures for handling suspicious passenger activities on in-flight commercial aircraft and the specific circumstances relating to the events on Northwest Airlines Flight 327 on June 29, 2004, including the handling of the suspicious passengers after the plane landed. *Office of Audits*

TSA's Mass Transit Security Program (Final Report - September)

In 2002, Americans took over 9.6 billion trips using public transportation. The American Public Transportation Association estimates that over 14 million Americans ride public transportation each weekday; and that the public transportation system employs about 350,000 people in the United States. The U.S. Department of Transportation (DOT) estimates another 25 million use public transportation less frequently but on a regular basis. In the United States, there are 14 heavy rail transit systems such as metro, subway, rapid transit, or rapid rail that consist of more than 2,000 route miles, over 1,000 stations, and approximately 10,500 heavy rail cars. About one-half of these heavy rail stations are located underground. In addition, there are another 20 commuter rail transit systems operating between a central city and adjacent suburbs that cover more than 7,000 route miles and over 1,100 stations.

To meet the security needs of industries across all modes of transportation, TSA plans to balance risk and direct its resources to yield the greatest benefit possible for the security of the transportation system as a whole, taking a risk-based approach to resource allocation. Earlier this year, the Government Accountability Office (GAO) testified that the implementation of risk management principles and improved coordination could help enhance rail security. The roles and responsibilities between TSA and the DOT creates the potential for duplicating or conflicting efforts as both entities work to enhance security.

Audit Objective: Determine the adequacy of the actions that TSA has taken to assess potential terrorist threats to the mass transit systems of major U.S. metropolitan areas and to coordinate with other DHS components and external agencies. *Office of Audits*

EMERGENCY PREPAREDNESS AND RESPONSE (EP&R)

Compliance Audits of Federal Emergency Management Agency's (FEMA) Public Assistance Grants (Ongoing)

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, and Title 44 of the *Code of Federal Regulations*, provide guidance and requirements for administering disaster relief grants awarded by FEMA. We typically performs 60 annual audits of grantees and sub-grantees receiving disaster assistance grants, focusing on large grants and areas that are of concern to Congress and FEMA. These audits result in millions of dollars in questioned costs annually.

Audit Objective: Determine to what extent grantees and sub-grantees accounted for and expended FEMA funds according to federal regulations. *Office of Audits*

National Urban Search and Rescue Response System (US&R) (Final Report - July)

The US&R was created to provide specialized lifesaving assistance during major disasters or emergencies. Currently, 28 task forces in 19 states are part of this system. OIG began an audit of the National Urban Search and Rescue Response System to determine whether management control and criteria deficiencies noted by the FEMA OIG in 1997 and 1998, and by the FEMA Comptroller in 2002, have been corrected.

Audit Objective: Assess whether the system is achieving defined goals that relate to preparedness and whether preparedness funding has the intended effect on the system's capacity to respond to major disasters or emergencies. *Office of Audits*

EP&R IT Initiative to Support DHS Incident Management System (Final Report - July)

Within the department, EP&R is charged with providing strategic planning, guidance, and interoperable technologies to support emergency response coordination with other federal agencies, as well as with state and local governments. EP&R, largely through FEMA, relies on a number of information systems and related technologies to support its emergency response mission.

Audit Objective: (1) Review the directorate's approach to respond to and recover from terrorist attacks, major disasters, and other domestic emergencies; (2) assess the effectiveness of guidance and processes to support incident management; and; (3) identify and evaluate existing and proposed systems and other technologies to help carry out the EP&R mission. *Office of Information Technology*

EP&R's Multi-Hazard Flood Map Modernization Program (Final Report - July)

FEMA has initiated a modernization program, using advanced geo-spatial technologies, to generate accurate and updated flood maps in digital system format. FEMA anticipates that such efforts will benefit the nation when communities use the new maps to create effective zoning and building standards. Property owners access the maps on the internet to see if they need to obtain flood insurance, and government officials use the maps to accurately locate infrastructure and transportation systems to help manage homeland security risks.

Audit Objective: Determine the effectiveness of the multi-hazard flood map modernization, specifically addressing FEMA's program management approach; coordination of flood mapping requirements with federal, state, and local entities; and, acquisition and use of technology to meet program objectives. *Office of Information Technology*

SCIENCE AND TECHNOLOGY (S&T)

BioWatch Program (Final Report - September)

The mission of the BioWatch Program is to provide for early detection of aerosol releases of select pathogens through a comprehensive protocol of monitoring and laboratory analysis of biological agents. This program is designed to recognize rapidly the release of a biological agent, before the onset of clinical illness, and measure the extent of a release to assist the federal, state, and local emergency management authorities in responding to a terrorist attack. DHS provides funds and management oversight to the Centers for Disease Control (CDC), an agency of the Department of Health and Human Services, and the Environmental Protection Agency (EPA). DHS has primary responsibility for designing, funding, and managing the BioWatch program. The EPA provides services and technical expertise to the BioWatch Program, including establishing, deploying, operating, and maintaining network sensors. The CDC provides, among other things, technical expertise and laboratory analysis services. The partner agencies coordinate and manage their respective responsibilities through a Memorandum of Agreement, dated March 2004. DHS budgeted $118 million for the BioWatch Program in FY 2005.

Audit Objective: Determine to what extent DHS has designed and implemented management controls to coordinate among the partner agencies and to accomplish BioWatch program objectives. *Office of Audits*

DHS Efforts to Employ Automated Surveillance Systems (Final Report - February 2006)

With facial recognition technology, computers scan the faces of travelers and others who pass through checkpoints, and compare them with the facial features of suspected terrorists in a law enforcement database. The combination of facial recognition technology with closed-circuit television cameras and monitors in a specific area can be effective as a form of mass surveillance, as presently employed in the U.K. and in selected U.S. sites such as Baltimore, MD. Unlike facial recognition, identity recognition systems combine the image recognition target with identity information. Identity recognition builds an understanding of the identity by assembling additional critical factors to determine if a target has been identified correctly. Casinos have used closed-circuit TV, biometric technology, and non-obvious relationship awareness software to probe databases for years as part of their quest to identify cheaters and card counters.

Audit Objectives: Identify S&T's initiatives and progress in developing technologies for automated surveillance systems and applications for DHS components; review research and project priorities for automated surveillance systems; and, identify issues and challenges for DHS in using these technologies. *Office of Information Technology*

Setting Equipment Standards (Final Report - December)

In 2004, we surveyed activities of the Science and Technology Directorate. S&T has the responsibility to set specifications for operation, interoperability, security, and safety of equipment necessary for threat prevention, detection, and emergency response. S&T uses an integrated project team process guided by portfolio managers. Team members work together to research, develop, and produce new technology.

Inspection Objectives: Assess the effectiveness of the team process; coordination with other directorates within DHS; the extent that the department is relying upon S&T to develop equipment standards; and, S&T's progress to date in developing such standards. *Office of Inspections and Special Reviews*

INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (IAIP)

National Cyber Sector (Final Report - November)

DHS created the National Cyber Security Division in June 2003 to respond to the actions and recommendations described in *The National Strategy to Secure Cyberspace,* as well as to be the national focal point to address cyber security issues in the United States and abroad. Since most of the assets in the cyber world are owned by the private sector, it is critical for DHS to work with it in developing solutions. The President's strategy, the Summit Task Forces, and other public and private sector venues have called for such relationships. For example, five private sector task forces were formed in December 2003: Awareness for Home Users and Small Businesses; Cyber Security Early Warning, Best Practices and Standards; Corporate Governance, Best Practices and Standards; Technical Standards and Common Criteria; and, Security Across the Software Development Life Cycle: Secure Software to develop strategies to address the priorities outlined in *The National Strategy to Secure Cyberspace.*

Audit Objectives: Determine the extent that the private sector is working with DHS and whether DHS is meeting its needs in protecting and securing cyberspace. *Office of Information Technology*

DHS Counter-Terrorist Information Sharing with State and Local Governments (Final Report - March 2006)

State and local personnel have their own capabilities and opportunities to gather information on suspicious activities and terrorist threats. By working together, the federal government can maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. As GAO reported in August 2003, however, information on threats, methods, and techniques of terrorists is not routinely shared and the information that is shared is not perceived as timely, accurate, or relevant. Moreover, federal officials have not established comprehensive processes and procedures to promote sharing.[3]

The *Homeland Security Act of 2002* gives DHS responsibility for coordinating the distribution of information between federal agencies and state and local governments. DHS is expanding access to and use of the Joint Regional Information Exchange System (JRIES) via the Homeland Security Information Network (HSIN), to provide secure real-time connectivity in a collaborative environment for collecting and disseminating information among federal, state, local, and tribal government agencies involved in combating terrorism.

Audit Objectives: Determine whether: DHS' strategies, policies, and procedures for collaborating with state and local governments to improve information sharing are sufficient; information being shared with state and local governments is timely, relevant, and accurate; and, the modernized HSIN/JRIES system adequately supports information sharing activities. *Office of Information Technology*

Public Sector Infrastructure Protection (Final Report - December)

The nation's critical infrastructure is categorized into 13 infrastructure "sectors" and five types of key assets. There are eight federal lead departments and agencies, including DHS, which have a role in coordinating protection activities and cultivating long-term collaborative relationships. While other federal departments have lead responsibility for sectors involving agriculture, food, water, public health, energy, banking and finance, chemical industry and hazardous materials, and the defense industry base, DHS remains responsible for cooperation and coordination among the federal participants.

Inspection Objectives: Determine how well DHS is collaborating with and overseeing the work of other federal departments or agencies with respect to the identification of critical assets and coordination of mitigation strategies in a specific sector. This review may result in sequential studies and reports on other individual sectors. *Office of Inspections and Special Reviews*

Management of Critical Infrastructure/Key Asset Information (Final Report - October)

Homeland Security Presidential Directive 7 establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and protect them from terrorist attacks. To support this policy, IAIP is responsible for creating and maintaining a national database of potential terrorist targets.

Inspection Objectives: Determine the efficacy of the processes used by IAIP to develop a prioritized list of the nation's critical infrastructure and assets, including: (1) collecting, analyzing, and prioritizing information in the national asset database, as well as how the database is used to support management decisions; (2) tools and other resources used by IAIP that directly support the population or use of information in the database; (3) IAIP relationships with DHS organizations and entities that it engages to carry out critical infrastructure protection initiatives; and, (4) the status of the Protected Critical Infrastructure Information Program and the National Infrastructure Protection Plan, as each pertains to the database. *Office of Inspections and Special Reviews*

Homeland Security Operations Center (Final Report - August)

The Homeland Security Operations Center (HSOC) serves as the nation's nerve center for information sharing and domestic incident management - dramatically increasing the vertical coordination among federal, state, territorial, tribal, local, and private sector partners. The HSOC collects and fuses information from a variety of sources to help deter, detect, and prevent terrorist acts. Operating every hour of every day, the HSOC provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the DHS Office of Information Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. Information on domestic incident management is shared with emergency operations centers at all levels through the Homeland Security Information Network.

Inspection Objectives: Determine how well the IAIP collects and analyzes information to produce and disseminate a final analytical threat product. The review focuses on how the IAIP ensures that it receives all of the information it requires, how it manages its analytical operation, and how it ensures that the product meets the needs of its customers. Also, it assesses the IAIP's process to identify information requirements and prioritize its work efforts. *Office of Inspections and Special Reviews*

MANAGEMENT

DHS' FY 2005 Consolidated Financial Statements (Final Report - November) (Mandatory)

The *Accountability of Tax Dollars Act of 2002* requires that an annual financial statement audit be performed at DHS. We contracted with an independent public accounting firm to conduct the audit. Individual audits of CBP's and TSA's financial statements will be performed in conjunction with the consolidated statement audit.

Audit Objective: Report on the fairness of presentation of DHS' FY 2005 financial statements; obtain an understanding of internal controls over financial reporting, perform tests of those controls to determine audit procedures, and report on weaknesses identified during the audit; and, perform tests of compliance with certain laws, regulations, and provisions of contracts or grant agreements, non-compliance with which could have a material effect on the financial statements; and, report on non-compliance disclosed by the audit. *Office of Audits*

DHS' Information Security Program for FY 2005 (Final Report - September) (Mandatory)

In response to an increased threat to information systems and the highly networked nature of the federal computing environment, Congress, in conjunction with OMB, requires an annual review and report on agencies' compliance with the requirements under the *Federal Information Security Management Act* (FISMA). FISMA includes provisions aimed at further strengthening the security of the federal government's information and computer systems, through the implementation of an information security program and development of minimum standards for agency systems.

Audit Objectives: Perform an independent evaluation of DHS' information security program and practices to determine what progress DHS has made in resolving weaknesses cited in the prior year's review. *Office of Information Technology*

DHS' Information Security Program (Intelligence Systems) for FY 2005 (Final Report - August) (Mandatory)

Critical to evaluating DHS' intelligence program is identifying potential information security threats to DHS' intelligence systems. The loss or compromise of DHS' intelligence systems and the data contained on those systems can have severe consequences, affecting national security, U. S. citizens, and the department's missions. In response to the increasing threat to information systems and the highly-networked nature of the federal computing environment, Congress, in conjunction with the intelligence community's chief information officer and OMB, requires an annual evaluation and report on the security program for agencies' intelligence systems. FISMA and *Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems,"* requirements will be used as criteria for the evaluation.

Audit Objective: Perform an independent evaluation of DHS' information security program and practices for its intelligence systems. Additionally, we will determine what progress DHS has made in resolving weaknesses cited in the prior year's review. *Office of Information Technology*

Oversight of Contracted Information Technology-Related Testing Performed as Part of DHS' FY 2005 Audited Financial Statements (Final Report - November) (Mandatory)

Financial statement audits performed under the *Chief Financial Officers Act of 1990* are intended to play a central role in providing more reliable and useful financial information to decision makers and improve the adequacy of internal controls and underlying financial management systems. Computer-related controls are a significant factor in achieving these goals and should be considered during all four phases of the audit.

Audit Objectives: Determine whether contract 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, or other illegal acts and disasters, and to effectively protect the information infrastructure from security threats or other incidents that cause the systems to be unavailable. *Office of Information Technology*

Network Security at DHS (Final Report - August)

Adequate network security is needed to protect the confidentiality, integrity, and availability of sensitive information. The primary reason for developing controls and testing the security of an operational system is to identify potential vulnerabilities and subsequently repair them. The number of reported vulnerabilities is growing daily; for example, the number of new information system vulnerabilities reported has more than quintupled since the beginning of 1998, from an average of 20 to over 100 per month. At the same time, the number of computers per person in many organizations continues to rise, thus increasing the demands on systems administrators.

Audit Objective: Determine whether DHS has implemented adequate network security controls to protect its various networks. *Office of Information Technology*

Effectiveness of the Security Operations Center (SOC) (Final Report - July)

The SOC supports the DHS missions to prevent, minimize damage, and assist in recovery from terrorist attacks that occur within the United States by ensuring that the DHS "network backbone" remains operational. The components monitor for threats, vulnerabilities, and attack; implement countermeasures; and, respond to incidents. They report incidents to the national Computer Emergency Readiness Team and to DHS managers responsible for threat mitigation and continuity of service. Under consolidation plans, the SOC would coordinate and provide IT services to all nine DHS components. Since the network security is only as strong as its weakest links, the Center may not have the authority, responsibilities, or funding required to coordinate the DHS defense of its backbone network against poorly-maintained systems and attacks.

Audit Objectives: Determine whether control weaknesses place DHS backbone network operations at risk and whether additional responsibilities, funding, or authority are required to improve defense of the DHS network. *Office of Information Technology*

DHS Database Security (Final Report - August)

Databases and database management systems (DBMS) are frequently targeted for attack by malicious users. Such attacks can lead to identity or credit card theft, financial loss, loss of privacy, or a breach of national security. To counter this threat, an increasing number of security options are available to protect sensitive data housed in databases. However, for these measures to be effective, DBMS security controls must be properly configured and maintained. In addition, as database products become more complex and the attacks against them increase, a number of vulnerabilities have been identified that could be exploited by attackers. DBMS vendors have responded by issuing patches or fixes for discovered vulnerabilities, but these patches must be quickly and appropriately applied to ensure that sensitive data is adequately protected.

Audit Objective: Determine whether DHS has implemented adequate and effective controls over sensitive data contained in its mission critical databases. *Office of Information Technology*

Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency project (eMerge2) Consolidation Process (Ongoing)

The eMerge2 will bring together the financial, budget, and asset control activities of the 22 agencies which comprise DHS. EMerge2 will provide for accurate, relevant, and timely information, create a standards-based environment, leverage proven technologies to advance business operations, and institutionalize best practices. We can play an important role in ensuring that an IT investment of this magnitude is well managed and has a positive impact on DHS. Audit best practices suggest that the audit function should be involved throughout a project's life cycle rather than merely in post-implementation assessments.

Audit Objectives: Evaluate and monitor eMerge2 project plans; assess the completeness and appropriateness of eMerge2 systems and database design, including security aspects; review the user-acceptance and parallel test planning and results to demonstrate successful end-to-end system operations and preparedness for implementation; and, review the startup of production systems and associated system data to ensure data integrity is maintained and back-out plans in the event of a problem are effective. *Office of Information Technology*

Buy American Act Compliance (Final Report - June) (Mandatory)

The *Buy American Act of 1933* (BAA) was enacted during the Depression to foster and protect American industry and workers. The BAA requires federal agencies to grant a preference to American made goods and materials for public use. House Conference Report 108-774, accompanying H.R. 4567, *Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2005,* requires us to audit DHS' compliance with the BAA. In addition, the DHS Secretary must issue a report to the Committees on Appropriations that describes the articles, materials, and supplies acquired by the department during fiscal year 2005 that were manufactured outside of the United States. Additionally, DHS is required to provide an itemized list of all waivers granted with respect to articles, materials and supplies under the BAA.

Audit Objective: Assess to what extent DHS has policies and procedures in place to ensure DHS compliance with the BAA. *Office of Audits*

DHS Procurement Operations (Series of Final Reports between June 2005 - June 2006)

A formidable challenge for DHS is to provide consistent contract management throughout departmental components. Several DHS organizations have large, complex, high-cost procurement programs that need to be closely managed. In addition, DHS has had to set up a procurement office to support component organizations that became part of the agency without the accompanying procurement staff. DHS has developed an information system to provide a procurement reporting mechanism that provides a primary system for elements without a pre-existing system with the capability of accepting input from those elements that already have their own procurement data reporting system.

Audit Objective: We are implementing a five-part program to evaluate DHS procurement operations and controls, including: 1) an overall assessment of DHS procurement controls and volnerabilities; 2) a review of information technology systems supporting the acquisition process; 3) a review of procurement best practices; 4) reviews of major DHS acquisition programs, including ACE, Deepwater, and U.S. Visit as described elsewhere in this plan; and 5) participation in a procurement fraud prevention working group with the U.S. Attorney's Office. *Office of Audits*

UNITED STATES COAST GUARD

Coast Guard Marine Safety Mission (Final Report - September)

After the terrorist attacks of September 11, 2001, the Coast Guard's priorities shifted to ports, waterways, and coastal security, to support its role as the lead federal agency for maritime homeland security. The Homeland Security Act of 2002, however, prohibits the Secretary of Homeland Security from significantly reducing the missions of the Coast Guard, or the Coast Guard's capability to perform those missions. In addition, the

Homeland Security Act of 2002 requires the OIG to annually review the Coast Guard's performance of all its missions, with a particular emphasis on the non-homeland security missions. The Government Accountability Office (GAO) has also reviewed Coast Guard mission performance, and found that after September 11, 2001, resource hours for most homeland security missions increased while most non-homeland security mission hours decreased. These resource hours were based on the usage of Coast Guard major assets--cutters, boats, and aircraft.

However, approximately 23 % of Coast Guard personnel perform missions, such as marine safety, that do not require the use of the Coast Guard boats, cutters, or aircraft, and therefore have not been reviewed. This review will focus on the marine safety mission, one of the Coast Guard missions not included in the GAO review. Failure to properly conduct the marine safety mission could result in major marine accidents, such as oil spills and vessel collisions, resulting in potentially catastrophic, life-threatening, economic, and environmental disasters. In addition, we will also provide updated statistics on Coast Guard's resource hours and mission performance, building on the data initially reported to and presented by GAO, to show how resource hours and mission performance have changed during FY 2004.

Audit Objectives: Determine if the Coast Guard's increased attention to homeland security missions since September 11, 2001, has (1) affected its performance of the marine safety mission and (2) reduced its ability to accomplish marine safety functions such as inspections, environmental protection, and investigations. The audit will also report on resource hours for Coast Guard's other missions. *Office of Audits*

International Shipping Container Security (Final Report - February) (Mandatory)

On August 9, 2004, Congress enacted Public Law 108-293, the *Coast Guard and Maritime Transportation Act of 2004*. On November 25, 2002, Congress enacted the *Maritime Transportation Security Act of 2002*. Section 102 of the law requires the U.S. Coast Guard to establish a program to evaluate and certify secure systems of international intermodal transportation and detailed specific requirements for the program. In section 809(c), the law requires that the Coast Guard prepare a plan to implement the secure systems of transportation required in section 102 of the *Maritime Transportation Security Act of 2002*. The plan is to include: 1) a timeline for establishing standards and procedures; 2) an assessment of the resources necessary to evaluate, certify, and validate secure systems of transportation; 3) the establishment of a user certification fee to fund the system and enhance cargo security; 4) an analysis of the need for, and feasibility of, establishing a system to inspect, monitor, and track intermodal shipping containers within

the U.S.; and, 5) an analysis of the need for, and feasibility of, developing international standards to enhance physical security of shipping containers. Section 809(d) of the law, requires us to report to Congress by February 2006 on the progress made by the department in implementing the plan.
Audit Objective: Determine whether the Coast Guard is implementing its Transportation Secure System plan pursuant to the requirements set forth in the *Maritime Transporation Security Act of 2002. Office of Audits*

Coast Guard Civilian Payroll (Final Report - May)

The Chairman of the Subcommittee on Homeland Security requested that we review Coast Guard's civilian pay expenses, based on two reprogramming requests that were not adequately justified. As a result of discrepancies related to the reprogramming requests, the Committee was concerned with how the Coast Guard was obligating, tracking, and accounting for civilian pay expenses.

Audit Objective: Determine the reason for the reprogramming requests related to civilian pay expenses; and, whether the Coast Guard has adequate internal controls over the associated budget process. *Office of Audits*

U.S. Coast Guard Enterprise Architecture Development Process (Final Report - January 2006)

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 DHS enterprise architecture framework establishes the roadmap to achieve an agency's mission through optimal performance of its core business processes within an efficient information technology environment.

Audit Objectives: Determine whether the U.S. Coast Guard has aligned its strategic plans and individual business priorities within an appropriate enterprise architecture framework; and, developed a transitional strategy to the DHS enterprise architecture model. *Office of Information Technology*

Coast Guard Helicopter Interdiction Tactical Squadron (HITRON) (Final Report - August)

HITRON was established in 1999 to interdict "go fast" boats transporting drugs to the United States. In May 2003, the Secretary announced that the HITRON would be used for counter-terrorism missions. Located in Jacksonville, FL, HITRON currently consists of eight leased commercial helicopters, which were procured and modified to perform the Coast Guard's Airborne Use of Force Mission. Of particular concern is whether the Coast Guard acted properly when it amended aircraft performance and safety equipment requirements for the award-winning aircraft.

Audit Objective: Determine whether: (1) the management oversight exercised by the Coast Guard over the aircraft procurement and modification phases of the project was adequate; (2) the Coast Guard's decision to transfer contract administration duties and responsibilities for the HITRON project to the Integrated Coast Guard Systems (Deepwater) is cost effective; and, (3) the ever-increasing use of HITRON aircraft to perform homeland security missions is having an adverse impact on the Coast Guard's traditional non-homeland security mission. *Office of Audits*

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES (CIS)

CIS IT Modernization (Final Report - July)

Current priorities of CIS are to implement solutions for improving immigration customer services, eliminate immigration adjudication backlogs, and promote national security. Ensuring effective and efficient use of IT to support those priorities will be a challenge for CIS.

Audit Objective: Determine the effectiveness of efforts underway within CIS to re-engineer processes and modernize IT. Specifically: assess CIS IT modernization plans; determine how well CIS is implementing the plans and managing IT across the organization; and, identify effective practices or lessons learned from comparable organizations that CIS might consider and apply as it modernizes its IT operations. *Office of Information Technology*

Provision of H-1B Non-immigrant Temporary Worker Status (Final Report - July)

The H-1B Temporary Worker status is a nonimmigrant immigration classification and is used to hire a foreign national professional for a temporary period of time. There must be an employer/employee relationship with the employer filing for H-1B status on behalf of the employee. There are two steps involved in acquiring H-1 B status. The first involves the Department of Labor (DOL) and requires an attestation from the employer that the "prevailing wage" for the particular position is being paid. Upon receipt of an approved Labor Condition Application, the actual H-1B application is submitted to U.S. Citizenship and Immigration Services. This application includes documentation about the nature of the position and the individual's qualifications. If approved, the individual must obtain the H-1B visa overseas or have a CIS approved change of status to H-1B.

The U.S. limits the total number of new H-1B petitions issued each year to private and for-profit companies to a worldwide quota of less than 65,000 per fiscal year. Based on reports that CIS had exceeded the 65,000 person ceiling by over 10,000 approvals, Senator Grassley and Congressman Hostettler asked the OIG to conduct a review.

Inspection Objective: Review the deliberations and actions taken by officials of USCIS regarding the bureau's provision of H-1B non-immigrant temporary worker status to more aliens in 2005 than was statutorily authorized. Examine how the over-issuance occurred and whether it was done in deliberate disregard of the statutory limit. *Office of Inspections and Special Reviews*

An Examination of the Vulnerabilities and Potential Abuses in the L Visa Program (Final Report - August) (Mandatory)

The L-1 visa program allows companies to transfer their foreign employees with special knowledge of the company or managerial or executive skills to the United States. The program has a five-year limit on employees with specialized skills staying in the U.S. and a seven-year limit on executives. Unlike the H-1B visa program, Congress has not limited the number of L-1 visas granted each year. The number of L-1 visas granted is estimated to be in the hundreds of thousands.

Inspection Objective: Review the vulnerabilities and potential abuses of the L Visa (intracompany transferee) visa program. This review is mandated by section 415 of the Consolidated Appropriations Act of 2005, which directs us to report our findings to the Committees on the Judiciary of the House of Representatives and the Senate.

We will examine and evaluate the adjudication of L petitions by Citizenship and Immigration Services (CIS) Regional Service Centers, with particular emphasis on fraud detection. We will examine operations, conduct interviews of CIS staff, and review appropriate documents. We will request assistance from the Department of State, Bureau of Consular Affairs, to evaluate L petitions and visa applications from the perspective of the overseas posts, and will solicit examples of misrepresentation and abuse. We will examine workplace compliance with the terms of the program, and examine Immigration and Customs Enforcement files related to the same. *Office of Inspections and Special Reviews*

Review of CIS Alien Security Checks (Final Report - September)

CIS conducts security checks during its benefit application process in order to prevent ineligible persons from obtaining immigration benefits, as well as to help law enforcement agencies identify risks to national security and the community. Currently, CIS performs approximately 35 million security checks each year, primarily via the Interagency Border Inspection System (IBIS), but also through fingerprint-based and other searches. In 2002 and 2003 reports, the DOJ's OIG noted that CIS's introduction of mandatory IBIS checks suffered from delayed field implementation, inadequate database access and training, and insufficient guidance for interpreting results. Other reports have suggested a conflict between CIS' goals to conduct thorough and accurate security checks and to hasten application processing, a major focus of CIS since the release of its "Backlog Elimination Plan" in June 2004. CIS is making several changes to its conduct of security checks, including the 2004 creation of an internal Office of Fraud Detection and National Security with responsibility for overseeing security checks.

Inspection Objective: Determine the efficacy of security checks that CIS conducts to prevent unqualified persons, particularly terrorists and criminal aliens, from receiving benefits. *Office of Inspections and Special Reviews*

OFFICE OF STATE AND LOCAL GOVERNMENT COORDINATION AND PREPAREDNESS (SLGCP)

We plan to audit management controls and oversight of federal grants within DHS. These audits will review internal controls, policies, and procedures that govern the process of making and monitoring federal grants and determine to what extent funded programs meet their desired results. We will make recommendations on how to improve the grant application receipt, review, and award process, grant monitoring and oversight, and the effectiveness of the grants in achieving program objectives.

Over the longer term, we plan to conduct a number of program audits that will result in a top-to-bottom assessment of the effectiveness of DHS' grants management. These program audits will be coordinated with and complemented by financial compliance audits of grantees and sub-grantees in each of the programs.
During FY2005, much of our focus will be on the largest grants and the organization that manages them - the Office of State and Local Government Coordination and Preparedness. Specific audits are detailed below.

1. States' Management of First Responder Grants (Final Report - September)

DHS awards federal "first responder" grant funds to states to assist local jurisdictions in acquiring specialized training, conducting preparedness exercises, acquiring equipment needed to respond to and manage terrorist incidents involving weapons of mass destruction, and planning and administering the grants. In FY 2003, Congress appropriated approximately $4 billion for first responder grants. The program has received substantial congressional and public interest in how states are using these grants. In 2004, we reported slow spending of first responder grant funds due to delays caused by needed planning efforts, lengthy administrative processes, and vendor backlogs.

Audit Objective: Determine to what extent states are effectively and efficiently implementing the first responder grant program, achieving the program goals, and spending funds according to grant requirements. *Office of Audits*

2. Use of Office of Domestic Preparedness' (ODP) Urban Area Security Initiative (UASI) Grant Funds by Cities (Final Report - February 2006)

The FY 2003 and 2004 UASI grant programs provide funds for unique planning, equipment, training, and exercise needs of large urban areas. Additionally, it assists them in building an enhanced and sustainable capacity to prevent, respond to, and recover from threats or acts of terrorism. FY 2003 funding was $602 million. FY 2004 funding increased to $671 million. The DHS budget request for FY 2005 set aside $1.2 billion to support at least 50 critical urban areas. There is substantial congressional and public interest in how this money is spent. To date, little audit or analysis has been done in the area.

<u>Audit Objective</u>: Determine whether the process for selecting recipient urban areas is effective and fair; and, whether funds are spent expeditiously and in compliance with grant guidelines and defined priorities. *Office of Audit*
s

3. State Homeland Security Assessment and Strategy (SHSAS) Program Audit (Final Report - September)

To assist states in conducting their threat, risk, and needs assessments, and in developing a three-year strategy, the Office of Justice Programs developed an on-line data collection tool. State agencies were scheduled to input data beginning August 15, 2000. DHS' Office of Domestic Preparedness (ODP) launched its FY 2003 SHSAS process on July 1, 2003. As part of this effort, ODP has refined the SHSAS process that was originally established in FY 1999. The refined process will serve as a planning tool for state and local jurisdictions, and will assist ODP and its partners in better allocating federal resources for homeland security.

<u>Audit Objective</u>: Determine the effectiveness of the SHSAS in achieving the intent of the law, in allocating federal resources equitably, and in achieving a fair return on funding allocations. *Office of Audits*

4. FEMA's Fire Management Assistance Grants (Series of Final Reports in FY 2005 and FY 2006)

The Fire Management Assistance grant program provides funds to local governments, through states, to fight fires on nonfederal forests or grasslands. In FY 2003, FEMA appropriated approximately $50 million for these grants, which have received very little oversight by FEMA.

<u>Audit Objective</u>: Determine to what extent grant recipients accounted for and expended grant funds according to federal regulations. *Office of Audits*

National Response Plan (NRP) (Final Report - July)

The NRP is intended to integrate the myriad federal, state, and local government, as well as the private sector and non-governmental organizations, plans for domestic prevention, preparedness, response and recovery into a single all-discipline, all-hazards response plan.

Audit Objective: Determine to what extent: (1) DHS has fully and effectively coordinated the preparation of the plan with appropriate federal, state, and local government officials, the private sector, and nongovernmental organizations; (2) the plan meets the expectations of an all-discipline, all-hazards plan; and, (3) DHS developed and conducted effective training and exercise programs relating to the NRP. *Office of Audits*

Exercise Top Officials (TOPOFF) (Final Report - July)

In April 2005, ODP will conduct the next *TOPOFF* exercise. *TOPOFF 3* will use a series of exercise activities of increasing complexity to simulate weapons of mass destruction (WMD) terrorist attacks in Connecticut and New Jersey. Additional *TOPOFF* activities will be conducted in the United Kingdom as part of a partnership to strengthen security in both nations. *TOPOFF 3* will be the third congressionally mandated WMD national exercise. The first was conducted in May 2000. *TOPOFF 2* was conducted in May 2003. The objectives of *TOPOFF 3* are to: (1) improve the nation's capacity to prevent, respond to, and recover from terrorist attacks according to DHS protocols, the Interim National Response Plan, and the National Incident Management System; (2) identify baseline capabilities and establish performance standards for a range of probable threats; (3) synchronize the goals and objectives of *TOPOFF* with those of the nation; (4) improve international coordination and cooperation in response to a terrorist event; and, (5) assess and strengthen government, non-government, and private sector partnerships to prevent, respond to, and recover from WMD incidents.

Inspection Objectives: Evaluate ODP's efforts undertaken to develop, plan, and coordinate the exercise and determine whether preparation for and conduct of the exercise effectively achieves the established goals. We are examining the development of exercise objectives, scenarios developed to support those exercise objectives, performance evaluation plans, and exercise control measures. *Office of Inspections and Special Reviews*

MULTI-COMPONENT

Data Mining Operations (Final Report - January 2006)

Data mining refers to the use of computer programs to examine vast stores of records, including private information, for hidden patterns and relationships among disparate pieces of information. It is an increasing practice in the federal government to support a range of activities - from improving performance and human resource management to analyzing intelligence and uncovering terrorist activities. For example, GAO recently surveyed 128 federal departments and agencies and found that 52 used or planned to use data mining programs. Within DHS, a number of component organizations use data mining, raising concerns about the lack of oversight to help minimize duplicative data mining systems and activities and ensure that the information sharing does not violate personal privacy rights. Additionally, more central oversight would help ensure that some areas, such as linking violent criminal information to terrorist databases, benefit from greater use of data mining and related systems.

Audit Objectives: Determine whether there are opportunities for improved management and oversight of data management systems and activities within DHS. Identify the various data mining systems and activities within DHS; determine whether there are redundancies and inefficiencies, and opportunities for streamlining. In addition, we will identify opportunities for coordinating data mining efforts with other federal agencies.
Office of Information Technology

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/oig

Richard L. Skinner	**Acting Inspector General**
Richard L. Skinner	**Deputy Inspector General**
Richard N. Reback	**Counsel to the Inspector General**
Richard Berman	**Assistant Inspector General/Audits**
Elizabeth Redman	**Assistant Inspector General/Investigations**
Robert Ashbaugh	**Assistant Inspector General/Inspections and Special Reviews**
Frank Deffer	**Assistant Inspector General/Information Technology**
Edward F. Cincinnati	**Assistant Inspector General/Administration**
Tamara Faulkner	**Congressional Liaison and Media Affairs**
Denise S. Johnson	**Executive Assistant to Acting 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 Ave., Room 330
Captain J.F. Williams Federal Building
Boston, MA 02110
(617) 223-8600 / Fax: (617) 223-8651

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

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

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

Indianapolis, IN
5915 Lakeside Blvd.
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

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

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

Philadelphia, PA
Greentree Executive Campus
5002 D Lincoln Drive West
Marlton, NJ 08053
(856) 968-4907 / Fax: (856) 968-4914

San Francisco, 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
654 Plaza
654 Munoz Rivera Ave, Suite 1700
San Juan, PR 00918
(787) 294-2500 / Fax: (787) 771-3620

Location of Investigative Field Offices

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

Boston, MA
408 Atlantic Ave., Room 737
Captain J.F. Williams Federal Building
Boston, MA 02110
(617) 777-7576

Buffalo, NY
138 Delaware Avenue, Room 524
Buffalo, NY 14202
(716) 843-5700 X520

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

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

Del Rio, TX
Amistad National Recreation Area
4121 Highway 90 West
Del Rio, TX 78840
(830) 775-7492 x239

Detroit, MI
Levin Federal Courthouse
231 W. Lafayette, Suite 1044
Detroit, MI 48226
(313) 226-2163 / Fax: (313) 226-6405

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

El Paso, TX
1200 Golden Key Circle, Suite 230
El Paso, TX 79925
(915) 629-1800 / Fax: (915) 594-1330

Houston, TX
5850 San Felipe Rd., Suite 300
Houston, TX 77057
(713) 706-4600 / Fax: (713) 706-4622

Laredo, TX
109 Shiloh Dr., Suite 430
Laredo, TX 78045
(956) 723-4021 / Fax: (956) 717-6465

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, Room 510
McAllen, TX 78501
(956) 618-8145 / Fax: (956) 618-8151

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

New York City, NY
Suite 2407
525 Washington Boulevard
Jersey City, NJ 07310
(201) 798-8165 / Fax (201) 659-5911

Philadelphia, PA
Greentree Executive Campus
5002 B Lincoln Drive West
Marlton, NJ 08053
(856) 968-6600 / Fax: (856) 968-6610

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

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

Seattle, WA
1110 3rd Ave., Suite 116
Seattle, WA 98101
(206) 262-2110 / Fax: (206) 262-2495

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

San Juan, PR
654 Plaza
654 Munoz Rivera Ave, Suite 1700
San Juan, PR 00918
(787) 294-2500 / Fax: (787) 771-3620

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

Washington, DC (Washington Field Office)
245 Murray Drive, SW
Building 410
Washington, DC 20528
(202) 254-4096 / Fax: (202) 254-4292

The Yuma, AZ, agents are temporarily operating out of the El Centro, CA, field office.

Appendix B – Acronyms

ACE	Automated Commercial Environment
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
BAA	Buy American Act of 1933
BTS	Border and Transportation Security
CBP	Customs and Border Protection
CDC	Centers for Disease Control
CIO	Chief Information Officer
CIS	Citizenship and Immigration Services
CPO	Chief Privacy Officer
CSI	Container Security Initiative
DBMS	Database Management Systems
DFO	Disaster Field Office
DHS	Department of Homeland Security
DOJ	Department of Justice
DOT	Department of Transportation
DRO	Detention and Removal Operations, Office of
eMerge2	Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency Project
EOIR	Executive Office of Immigration Review
EP&R	Emergency Preparedness and Response
EPA	Environmental Protection Agency
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FTE	Full-time equivalent
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HITRON	Helicopter Interdiction Tactical Squadron
HSARPA	Homeland Security Advanced Research Projects Agency
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
HSOC	Homeland Security Operations Center

IAIP	Information Analysis and Infrastructure Protection
IBIS	Interagency Border Inspection System
ICAO	International Civil Aviation Organization
ICE	Immigration and Customs Enforcement
IDS	Integrated Deepwater System
INS	Immigration and Naturalization Service
IRP	Institutional Removal Program
ISIS	Integrated Surveillance Intelligence System
IT	Information Technology
JRIES	Joint Regional Information Exchange System
NDCP	National Drug Control Program
NFIP	National Flood Insurance Program
NRP	National Response Plan
NSEERS	National Security Entry/Exit Registration System
ODP	Office of Domestic Preparedness
OIAPR	Office of Internal Affairs And Program Review
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
POE	Ports of Entry
RPM	Radiation Portal Monitors
S&T	Science and Technology
SEVIS	Student and Exchange Visitor Information System
SHSAS	State Homeland Security Assessment and Strategy
SLGCP	State and Local Government Coordination and Preparedness
SOC	Security Operations Center
TOPOFF	Top Officials
TSA	Transportation Security Administration
TSCC/CMO	Transportation Security Coordination Center/Crisis Management Office
UASI	Urban Area Security Initiative
US&R	National Urban Search and Rescue Response
US-VISIT	United States Visitor and Immigrant Status Indication Technology
WCF	Working Capital Fund
WMD	Weapons of Mass Destruction
WYO	Write-Your-Own

Appendix C – Performance Goals, Measures, and Accomplishments

FY 2004

Performance Goals and Indicators	Fiscal Year 2004 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.	96%
1.2 Achieve at least 75 % concurrence with recommendations contained in OIG audit and inspection reports (excludes grant audits).	92%
1.3 Complete draft reports for at least 75% of inspections and audits within six months of the project start date (excludes grant audits).	44%
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.	62%
2.2 At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.	75%
2.3 Provide audit coverage of $500 million of DHS grant programs.	103%
2.4 Achieve at least 75% concurrence from DHS management with OIG recommendations on grant audits.	61%

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 2005 Initiative
3.2	Establish and implement an employee training program for DHS OIG.	In process
3.3	Establish and implement a performance evaluation program for employees of DHS OIG.	100%
3.4	Establish and implement an awards program for DHS OIG employees.	100%

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.

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 Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.