

**DEPARTMENT OF HOMELAND SECURITY**

**Office of Inspector General**



**FISCAL YEAR 2007**

**ANNUAL PERFORMANCE PLAN**

# **The Department of Homeland Security**

## **Office of Inspector General**

### **Fiscal Year 2007 Annual Performance Plan**

---

**The Government Performance and Results Act (GPRA) of 1993, Public Law 103-62, requires agencies to submit to the Office of Management and Budget (OMB) an annual performance plan covering each program activity in the agency's budget. The annual performance plan is to provide the direct linkage between the strategic goals outlined in the agency's strategic plan and what managers and employees do day-to-day. The plan is to contain the annual performance goals the agency will use to gauge its progress toward accomplishing its strategic goals and identify the performance measures the agency will use to assess its progress.**

---

## A Message From the Inspector General

I am pleased to present the *Fiscal Year 2007 Annual Performance Plan* for the Department of Homeland Security's (DHS) Office of Inspector General (OIG). This plan, which is our fifth, outlines the projects that we intend to undertake this fiscal year to evaluate DHS's programs and operations. This promises to be another challenging and demanding year as we attempt to address the many complex issues confronting DHS in its daily effort to reduce America's vulnerability to terrorism, and to minimize the damage and recover from man-made attacks and natural disasters that may occur. To ensure that we have a sufficient focus on disaster assistance, I have established a new Office of Disaster Assistance Oversight within the OIG. A Deputy Inspector General will manage the Office.

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



Richard L. Skinner  
Inspector General



# Table of Contents

| <b>Chapter</b>   | <b>Page</b> |
|--|-------------|
| 1. OIG Mission and Responsibilities .....                                | 1           |
| 2. OIG Organizational Structure .....                                    | 2           |
| 3. FY 2007 Planning Approach .....                                       | 4           |
| 4. Allocation of Resources .....   | 6           |
| 5. Performance Goals and Measures .....                                  | 7           |
| 6. Performance Initiatives: Project Narratives.....                      | 9           |
| • Disaster Recovery .....  | 9           |
| • Special Initiative.....  | 20          |
| • Civil Rights Civil Liberties.....                                      | 21          |
| • Customs and Border Protection.....                                     | 21          |
| • Domestic Nuclear Detection Office.....                                 | 29          |
| • Federal Emergency Management Agency.....                               | 29          |
| • Immigration and Customs Enforcement.....                               | 31          |
| • Management.....  | 36          |
| • Office of Intelligence and Analysis.....                               | 46          |
| • Office of Policy .....   | 48          |
| • Preparedness.....  | 49          |
| • Science and Technology.....  | 55          |
| • Transportation Security Administration.....                            | 60          |
| • United States Citizenship and Immigration Services.....                | 65          |
| • United States Coast Guard.....   | 66          |
| • United States Secret Service.....                                      | 71          |
| • Multi-Components.....  | 71          |
| Appendix A - OIG Headquarters and Field Office Contacts .....            | 76          |
| Appendix B - Table of Acronyms .....                                     | 82          |
| Appendix C - FY 2006 Performance Goals, Measures, and Accomplishments... | 85          |



---

## 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 (IG), who is appointed by the President and confirmed by the Senate, reports directly to both the Secretary of DHS and the Congress. Barring narrow and exceptional circumstances, the IG may inspect, audit, or investigate anyone in the department, or any program or operation of the department. To ensure the IG'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, efficiency, and effectiveness within the department, and to prevent and detect fraud, waste, and abuse in the department's programs and operations.

### **Specifically, OIG's key legislated responsibilities are to:**

- Promote economy, efficiency, and effectiveness in the management of DHS's programs and supporting operations;
- Conduct and supervise audits, investigations, and reviews relating to the department's programs and support operations;
- Detect and prevent fraud, waste, and abuse;
- Review existing and proposed legislation and regulations, and make appropriate recommendations;
- Maintain effective working relationships with other federal, state, and local governmental agencies, and nongovernmental entities regarding the mandated duties of the IG;
- Inform the Secretary of the DHS and the Congress of serious problems and recommend corrective actions and implementation measures;
- Comply with the audit standards of the Comptroller General of the Government Accountability Office (GAO); avoid duplication of GAO activities; and
- Report violations of federal criminal law to the U.S. Attorney General.

## Chapter 2 - OIG Organizational Structure

The OIG consists of the following components:

***The Executive Office*** consists of the IG, the Deputy IG, a congressional liaison and media affairs officer, an executive assistant, and support staff. It provides executive leadership to the OIG with six full-time equivalent (FTE) employees.

***The Office of Counsel to the Inspector General*** provides legal advice to the IG; 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 12 FTEs.

***The Office of Audits*** conducts and coordinates audits and program evaluations of the management and financial operations of DHS. Auditors examine the methods employed by agencies, bureaus, grantees, and contractors in carrying out essential programs or activities. Audits evaluate whether established goals and objectives are achieved and resources are used economically and efficiently; whether intended and realized results are consistent with laws, regulations, and good business practice; and whether financial accountability and the reliability of financial statements are ensured. The office has 145 FTEs.

***The Office of Disaster Assistance Oversight*** is responsible for providing an aggressive and ongoing audit and investigative effort designed to ensure that disaster relief funds are being spent appropriately, while identifying fraud, waste, and abuse as early as possible. The office works to ensure accountability and to prevent problems before they occur. The focus is weighted heavily toward prevention, including reviewing internal controls, and monitoring and advising DHS officials on contracts, grants, and purchase transactions before they are approved. The office also meets with applicants, contractors, and grantees to advise them of the requirements and assess their capability to account for the funds. This office has 75 FTEs. The office also has temporary employees dedicated to Gulf Coast Hurricane Recovery operations.

***The Office of Inspections*** compliments the work of the OIG 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 IG. This office has 41 FTEs.

***The Office of Information Technology*** conducts audits and evaluations of DHS's information management, cyber infrastructure, and systems integration activities. The office reviews the cost effectiveness of acquisitions, implementation, and management of major systems, and telecommunications networks across DHS. In addition, it evaluates the

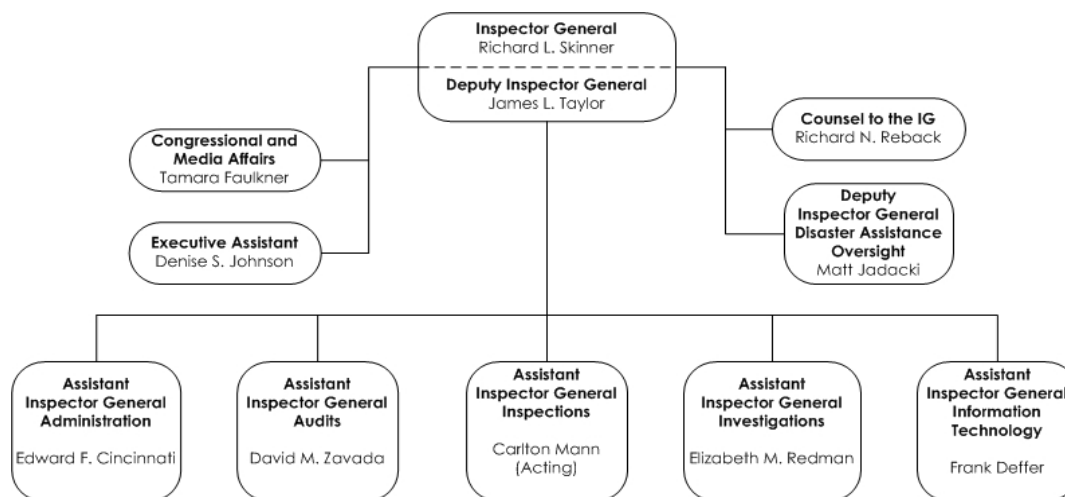


systems and related architectures of DHS to ensure they are effective, efficient, and implemented according to applicable policies, standards, and procedures. The office also assesses DHS's information security program as mandated by the Federal Information Security Management Act (FISMA). This office has 42 FTEs.

**The Office of Investigations** conducts investigations into allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, and grantees. This office examines specific allegations, reports, or other information indicating possible violations of laws or regulations. Additionally, it monitors the investigative activity of DHS's various internal affairs offices. This office has 189 FTEs; approximately 25 of whom are currently dedicated to the work generated by hurricanes Katrina and Rita. This office also has 19 temporary employees dedicated to Gulf Coast hurricane recovery operations.

**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; correspondence; printing and distribution of OIG reports; and oversight of the personnel, procurement, travel, and accounting services provided to the OIG on a reimbursable basis by the Bureau of Public Debt. The office also prepares the OIG's annual performance plans and the semiannual reports to the Congress. This office has 35 FTEs.

### Department of Homeland Security Office of Inspector General Management Team



## Chapter 3 - FY 2007 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 DHS programs and operations. In devising the plan, OIG endeavors to assess DHS's progress in meeting what it considers to be the major management challenges.

This plan describes more projects than may be completed in FY 2007, especially since developments and requests from DHS management and the 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. The plan includes projects that were initiated, but not completed during FY 2007. Finally, the plan also contemplates that some jobs will start during FY 2007, but will carry over into FY 2008.

In establishing priorities, the OIG placed particular emphasis on legislative mandates, such as the Chief Financial Officers Act and the FISMA, DHS's strategic goals, the President's Management Agenda, the Secretary's priorities, congressional priorities, and the most serious management challenges facing DHS.

DHS's priority goals are divided into seven policy clusters:

- Control Our Borders
- Detect and Defend Against Weapons of Mass Destruction
- Strengthen Screening of Travelers and Workers
- Secure Critical Infrastructure Systems
- Build a Nimble, Effective Emergency Response System
- Encourage a National "Culture of Preparedness"
- Strengthen DHS Core Management, Policy, and Operational Integration

The President's Management Agenda addresses the following:

- Strategic Management of Human Capital
- Competitive Sourcing
- Improved Financial Performance
- Expanded Electronic Government
- Budget and Performance Integration
- Eliminating Improper Payments
- Real Property

The OIG has identified the following as the most serious FY 2007 management challenges facing DHS:

- Catastrophic Disaster Response and Recovery
- Consolidating the Department's Components
- Contract Management
- Grants Management
- Financial Management
- Human Capital Management
- Department-wide Information Technology (IT) Infrastructure
- Security of IT Infrastructure
- DHS Component IT Management
- Information Sharing
- Infrastructure Protection
- Border Security
- Transportation Security
- Rail and Mass Transit Security
- Trade Operations and Security

In addition, keeping with the priorities of both the Secretary and the Congress, OIG will focus attention on DHS's non-homeland missions. Particular attention will be given to the U. S. Coast Guard's (USCG'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's activities. Rather, they represent those activities that are the core of DHS's mission and strategic objectives. By answering certain fundamental questions within each of these program and functional areas, the OIG will determine how well DHS is performing and will be able to recommend ways to improve the efficacy of DHS's programs and operations.

The OIG will strive to have a consultative and collaborative working relationship with senior management of DHS while at the same time providing, where such criticism is warranted by the facts, constructive and objective criticism of DHS's programs and operations.

## Chapter 4 - Allocation of Resources

The FY 2007 appropriation provides \$85,185,000 for the Office of Inspector General. This amount is \$11,000,000 below the President's budget request; however, the language provides up to a \$13,500,000 transfer from the Disaster Relief Fund.

### STANDARD OBJECT CLASSIFICATION SCHEDULE (Dollars in Thousands)

| Object Classification                    |  | FY2006<br>Enacted | FY2007<br>Enacted | FY2007<br>Change |
|--|--|-------------------|-------------------|------------------|
| 11.1                                     | Perm Positions                             | \$ 40,781         | \$ 42,044         | \$ 1,263         |
| 11.3                                     | Other than perm                            | \$ -              | \$ -              | \$ -             |
| 11.5                                     | Other per comp                             | \$ 3,447          | \$ 3,587          | \$ 140           |
| 11.8                                     | Spec Srvc Pay                              | \$ -              | \$ -              | \$ -             |
| 12.1                                     | Benefits                                   | \$ 13,049         | \$ 13,545         | \$ 496           |
| 13.0                                     | Benefits-former                            | \$ -              | \$ -              | \$ -             |
| <b>Total, pers. comp. &amp; benefits</b> |  | <b>\$ 57,277</b>  | <b>\$ 59,176</b>  | <b>\$ 1,899</b>  |
| 21.0                                     | Travel                                     | \$ 4,046          | \$ 4,176          | \$ 130           |
| 22.0                                     | Transportation of things                   | \$ 76             | \$ 96             | \$ 20            |
| 23.1                                     | GSA rent                                   | \$ 7,426          | \$ 7,550          | \$ 124           |
| 23.2                                     | Other rent                                 | \$ 613            | \$ 623            | \$ 10            |
| 23.3                                     | Communication, Utilities, and misc charges | \$ 2,922          | \$ 2,982          | \$ 60            |
| 24.0                                     | Printing                                   | \$ 40             | \$ 41             | \$ 1             |
| 25.1                                     | Advisory & Assistance Services             | \$ 583            | \$ 989            | \$ 406           |
| 25.2                                     | Other Services                             | \$ 1,595          | \$ 1,671          | \$ 76            |
| 25.3                                     | Purchase from Govt. Accts.                 | \$ 5,649          | \$ 5,796          | \$ 147           |
| 25.4                                     | Operation & maintenance of facilities      | \$ -              | \$ -              | \$ -             |
| 25.7                                     | Operation & maintenance of equipment       | \$ 313            | \$ 319            | \$ 6             |
| 25.8                                     | Subsistence & Support of persons           | \$ -              | \$ -              | \$ -             |
| 26.0                                     | Supplies & materials                       | \$ 743            | \$ 767            | \$ 24            |
| 31.0                                     | Equipment                                  | \$ 804            | \$ 899            | \$ 95            |
| 32.0                                     | Land & Structures                          | \$ -              | \$ -              | \$ -             |
| 91.0                                     | Unvouchered                                | \$ 100            | \$ 100            | \$ -             |
| 99.0                                     | Other                                      | \$ -              | \$ -              | \$ -             |
| <b>Total, other objects</b>              |  | <b>\$ 24,910</b>  | <b>\$ 26,009</b>  | <b>\$ 1,099</b>  |
| <b>Total Appropriation</b>               |  | <b>\$ 82,187</b>  | <b>\$ 85,185</b>  | <b>\$ 2,998</b>  |

## 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 the Congress. To accommodate uncontrollable or unpredictable factors, the OIG's performance goals and measures will be updated annually for maximum effectiveness in meeting the changing needs of DHS, consistent with the OIG's statutory responsibilities. In addition to the mandatory requirements, performance measures identified serve as a basis to determine the overall effectiveness of OIG work.

### FY 2007

#### Performance Goals and Indicators

##### Goal 1. Add value to DHS programs and operations.

- 1.1 Provide audit and inspection coverage of 75 percent of DHS's strategic objectives, the President's Management Agenda, and major management challenges facing DHS.
- 1.2 Achieve at least 85 percent concurrence with recommendations contained in OIG audit and inspection reports.
- 1.3 Complete draft reports for at least 75 percent of inspections and audits within 6 months of the project start date, i.e., entrance conference.

##### Goal 2. Ensure integrity of DHS programs and operations.

- 2.1 At least 75 percent of substantiated investigations are accepted for criminal, civil, or administrative action.
- 2.2 At least 75 percent of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.
- 2.3 Provide audit coverage of each of DHS's grant programs.
- 2.4 Achieve at least 85 percent concurrence from DHS management with OIG recommendations on grant audits.

**Goal 3. Deliver quality products and services.**

- 3.1 Establish and maintain an internal quality control review program covering all elements of DHS OIG.
- 3.2 Establish and maintain a training program for all DHS OIG employees.

## Chapter 6 – Project Narratives

### DISASTER RECOVERY

In order to focus on and establish a continuous oversight presence in disaster-related activities, we created the Office of Disaster Assistance Oversight. The addition of this office will strengthen our ability to react quickly and efficiently to a variety of disasters, further advance our collaborative efforts with the federal Inspector General community, and achieve a holistic approach to federal disaster response and recovery oversight through the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE).

#### Catastrophic Disaster Response

During a natural or man-made catastrophic disaster, the Office of Disaster Assistance Oversight will deploy experienced staff to FEMA's Emergency Operations Center, Joint Field Offices (JFOs), applicable National Processing Service Centers, and other FEMA field locations, as appropriate, to provide on-the-spot advice, assistance, and oversight to DHS, FEMA, state, and local officials. Major oversight activities include:

- Participating in all senior-level meetings at FEMA Headquarters and providing continuous, on-sight oversight of JFO operations by attending daily status, all hands, and senior staff meetings with JFO staff, state and local officials, and with Emergency Support Functions representatives.
- Monitoring mission assignments, reviewing supporting documentation, and coordinating and meeting with OIG officials from other federal organizations to discuss their roles and devise plans to provide the most review/audit coverage.
- Reviewing JFO-issued contracts and contracting procedures for disaster-related services and determining compliance with federal acquisition policies, procedures, and requirements.
- Identifying, documenting, and reviewing/auditing potential FEMA and state disaster management problems and issues in the area of debris removal, emergency protective measures, assistance to individuals and households, temporary housing, longer-term public assistance repairs and restorations, and hazard mitigation, as well as other support areas, e.g., property management.
- Attending public assistance applicant briefings and kick-off meetings with FEMA, state, and local officials; overseeing the development of larger public assistance projects to ensure work eligibility and reasonableness; performing interim reviews

Department of Homeland Security

of sub-grantees claims; and following up on specific issues and complaints about sub-grantee practices that are not in compliance with program requirements.

- Reviewing major grant recipients' financial management systems and internal control and coordinating with state auditors to develop review/audit strategies.
- Responding to Congressional requests/inquiries, briefing IG and other interested parties on the results of our oversight, and coordinating with our Office of Investigations as to known or suspected fraud, waste, or abuse.
- Coordinating with state and local government audit and investigative organizations.

**Objectives:** Our focus will be on staying current on all disaster relief operations and activities, and evaluating (1) FEMA's implementation of existing response and recovery policies and procedures, (2) its development of new policies and procedures based on the magnitude of the disaster event, and (3) the adequacy of the internal control environment as hundreds of millions and potentially billions of dollars are provided for response and recovery activities.

**Disaster Assistance Grants (Nation-wide)**

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended, governs disasters declared by the President of the United States. Title 44 of the Code of Federal Regulations provides further guidance and requirements for administering disaster assistance grants awarded by FEMA to individuals, and to states and local governments. We will perform audits of grantees and sub-grantees focusing on large grants (generally in excess of \$3 million) with suspected problems, and areas that are of interest to Congress and FEMA. The audits will include both open and recently closed applications and projects, and will focus on costs as well as the eligibility of the grant applicant and the eligibility of the work funded by the grant. The audits will focus primarily on public assistance grants, but may include hazard mitigation grants and grant assistance provided to individuals and households.

**Review Objectives:** Determine (1) the eligibility of the grantee or sub-grantee and of the work funded by the grant and (2) whether grantees or sub-grantees accounted for and expended FEMA funds according to federal regulations.

**Assessment of FEMA's Readiness to Respond to the Next Catastrophic Disaster**

Following Hurricane Katrina, many organizations identified numerous serious problems that resulted in FEMA's failure to effectively respond to the disaster. FEMA has been working to improve its readiness and now claims to be better prepared to respond to the next catastrophic disaster. We will review the steps FEMA has taken to improve its



capability in those areas identified as most seriously deficient in its response to Hurricane Katrina.

**Review Objective:** Determine to what extent FEMA is better prepared to respond to a catastrophic disaster than prior to Hurricane Katrina.

### **FEMA Acquisition Management Review**

The success of any disaster relief effort depends in great part on effectively employing the U.S. government's capacity to deploy efficiently and rapidly the means of relief and reconstruction: services, materials, and their supporting systems. This requires acquisition processes that are well structured and optimized for use in contingency situations. FEMA was not systemically well-poised to provide the kind of acquisition support needed for a catastrophic disaster such as Hurricane Katrina.

We will conduct an acquisition management review at FEMA that will address major issues such as:

- Organizational alignment and leadership;
- Policies and processes;
- Acquisition workforce; and
- Information management.

**Review Objectives:** Determine where there are opportunities to improve the efficiency and effectiveness of FEMA's acquisition management and monitoring efforts in providing goods and services for disaster response and recovery.

### **Multilayered Disaster Contracts**

In the aftermath of Hurricane Katrina, FEMA has awarded over \$7 billion in federal contracts to hundreds of companies. The IG community and GAO have reported that the management and oversight of these disaster contracts has been dismal. Gulf Coast businesses, especially small businesses, allege that they are being shut out of participating in the recovery efforts because they cannot enter into the multi-tiered subcontracts except at the very bottom where profitability is very low. Prices paid under contracts, both prime contracts and all their sub-contracts, are not readily available to the public or to Congress. Without visibility over contracting, Congress and the American people are unable to determine for themselves whether tax dollars are being spent efficiently and effectively.

**Review Objectives:** Determine the extent of multi-layered disaster contracts regarding Hurricane Katrina and document the various problems associated with them. This work may highlight particular case studies to illustrate the problem.

### **FEMA's Storage and Maintenance of Housing Assets**

FEMA's response to the needs of disaster victims includes providing temporary housing. FEMA provides rental assistance money to rent a different place to live or government-provided housing such as travel trailers, mobile homes, or other types of modular housing when rental properties are not available. During hurricanes Katrina and Rita, in excess of \$2.5 billion was spent on travel trailers and mobile homes. FEMA's plans for future disasters include maintaining an inventory of housing assets at storage facilities located in strategic areas of the country for expedited response to housing needs. Our review will evaluate the need for maintaining these facilities as to overall cost effectiveness, as well as the capabilities and preventive maintenance procedures to safeguard housing assets at these locations from overall deterioration.

**Review Objective:** Determine the overall cost effectiveness of maintaining FEMA storage facilities as well as the overall capability, controls, and procedures in place to ensure the proper maintenance of the housing assets to prevent damages from deterioration.

### **Accountability for Travel Trailers, Mobile Homes, and Modular Homes**

In response to the housing needs for victims of hurricanes Katrina and Rita, disaster assistance operations involved acquisitions of travel trailers, mobile homes, and modular homes. Our auditors and contractors will review FEMA's management of these housing assets and will evaluate internal controls in place to ensure the housing purchased is properly accounted for and managed for the life cycle of the assets.

**Review Objective:** Determine the effectiveness of internal controls for management of housing assets from purchase to final disposition.

### **FEMA's Exit Strategy for Transitional Housing in the Gulf Coast Region**

Tens of thousands of FEMA-purchased manufactured homes and travel trailers are occupied by 100,000 Gulf Coast evacuee families in scores of Transitional Housing (TH) sites throughout Louisiana, Mississippi, and Alabama, where FEMA pays for security. According to FEMA's Office of Gulf Coast Recovery, the TH sites that will be operating for five or more years are already plagued with violence, drugs, and gang activity. A July 2006 report on the situation at 20 of FEMA's TH sites by the *Save the Children* organization painted a bleak picture of dysfunctional communities. The lack of alternative housing in the Gulf Coast region suggests that these TH sites may be permanent. The current situation is a recipe for human tragedy and a brewing public relations nightmare for DHS/FEMA. This review will assess how well FEMA is addressing the situation, what role other federal agencies should have in transitional housing, and whether FEMA has devised a road map for transferring the TH sites to local governments.

**Review Objectives:** Determine (1) the efficacy of DHS/FEMA's strategy for dealing with the problem of the TH sites becoming dysfunctional communities; (2) whether there is

adequate coordination among federal agencies, local authorities, and voluntary organizations; and (3) whether DHS/FEMA has formulated a coherent exit strategy.

### **Fraud Vulnerability of FEMA's Individuals and Households Program**

FEMA's Individuals and Households Program (IHP) provides eligible applicants with cash grants for temporary housing, home repair or replacement, and other disaster-related needs. In response to hurricanes Katrina and Rita, over \$6.7 billion in assistance has been awarded. Of this, GAO estimated that approximately \$1.0 billion was paid based on potentially fraudulent applications. This review will use a case management methodology to identify the causes of the fraud in the IHP.

**Review Objective:** To identify vulnerabilities and control weaknesses that enable fraud in FEMA's IHP.

### **FEMA's Debris Removal Program**

Removing debris created by hurricanes Katrina and Rita will be an extremely costly and time-consuming endeavor throughout the Gulf Coast. Our office is conducting numerous reviews of local governments' debris removal operations because the costs will be reimbursed by FEMA's Public Assistance grant program. There have been long-standing problems associated with debris removal and monitoring operations, and those problems are exacerbated by the size of the debris problem in the Gulf Coast. In response to these problems, FEMA is retooling its debris removal program and implementing new policies and procedures.

**Review Objective:** Determine the efficacy of FEMA's debris program including its recent retooling effort, and identify best practices.

### **FEMA's Section 406 Mitigation**

FEMA provides public assistance grants to state and local governments to repair or restore infrastructure damaged by disasters. A component of that program allows for funding mitigation measures that the state or local government determines to be necessary to meet a need for governmental services and functions in the area affected by the major disaster. The opportunities for mitigation in the Gulf Coast will be enormous and the costs substantial. We will conduct a performance review of FEMA's implementation and management of the mitigation component of its public assistance grant program in the hurricanes Katrina and Rita recovery process.

**Review Objective:** To determine how effectively FEMA is managing public assistance mitigation grants across the hurricane damaged Gulf Coast.

### **FEMA's Hazard Mitigation Grant Program**

Authorized under Section 404 of the Stafford Act, the Hazard Mitigation Grant Program (HMGP) provides grants to states and local governments to implement long-term hazard mitigation measures after a major disaster declaration. The purpose of HMGP is to reduce the loss of life and property due to natural disasters and to enable mitigation measures to be implemented during the immediate recovery from a disaster. The program may provide a state with up to 7.5 percent of the total disaster grants awarded by FEMA. States that meet higher mitigation planning criteria may qualify for a higher percentage. To date, FEMA has committed about \$3 billion in HMGP funds to states along the Gulf Coast for hurricanes Katrina and Rita.

**Review Objective:** Determine how effectively FEMA and the states are managing the Hazard Mitigation Grant Program after hurricanes Katrina and Rita.

### **FEMA's National Flood Insurance Program ([Mandatory](#))**

FEMA manages the National Flood Insurance Program (NFIP). Pursuant to section 1345 of the National Flood Insurance Act of 1968 (42 U.S.C. 4081) and subpart C of part 62 of title 44, Code of Federal Regulations, FEMA has arrangements with individual private sector property insurance companies through the Write Your Own (WYO) program. Participating companies offer flood insurance coverage to eligible applicants and arrange for the adjustment, settlement, payment, and defense of all claims arising from policies of flood insurance issued under this Program. The WYO Company acts as a fiscal agent of the federal government. When Hurricane Katrina made landfall in August 2005, there was damage from wind and flooding. We will investigate whether, and to what extent, in adjusting and settling claims resulting from Hurricane Katrina, insurers under the WYO program improperly attributed damages to flooding, covered under the insurance provided by the NFIP, rather than to windstorms which are covered under the insurance of the individual private sector property insurers or by wind-storm insurance pools in which such insurers participated.

**Review Objective:** Determine whether the NFIP WYO program was effective in properly attributing the damage from Hurricane Katrina to either flooding or windstorm.

### **Fire Management Assistance Grant Program**

The *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, as amended by the *Disaster Mitigation Act of 2000*, authorizes state governments and Indian Tribal Governments to request federal funds under the Fire Management Assistance Grant (FMAG) Program for the mitigation, management, and control of any fire burning on publicly (nonfederal) or privately owned forest or grassland. Under the FMAG program, the state or Indian Tribal Government may request an FMAG declaration while a fire is burning uncontrolled and threatens such destruction as would constitute a major disaster.

FMAG declaration requests are submitted to the appropriate FEMA Regional Director for approval.

**Review Objective:** Determine whether the state (grantee) accounted for and expended fire management assistance grant funds in accordance with federal regulations and FEMA guidelines.

### **Data Mining to Identify Duplication of Benefits**

FEMA has an array of assistance programs available to aid victims in recovering from damages sustained in Presidentially declared disasters. FEMA's Disaster Housing Program provides eligible applicants with assistance in the form of cash grants to make repairs to their home as well as other types of housing assistance for victims who need to rent. FEMA also provides travel trailers and mobile homes to victims displaced by a disaster. Other housing options include hotels, motels, and apartments. The Federal Insurance Administration within FEMA manages the NFIP that provides flood insurance to property owners within participating communities. The maximum coverage that can be obtained is \$250,000.

The Computer Science Corporation maintains the database of active and cancelled flood policies as well as claims paid. Records of housing assistance, i.e., rental assistance that FEMA provides, are maintained in the National Emergency Management Information System (NEMIS); and hotels, motels, and apartments are maintained in other databases.

**Review Objectives:** Determine whether: (1) recipients of FEMA's Disaster Housing home repair grant assistance have also received benefits from the NFIP; (2) duplication of assistance to victims has occurred among the various housing programs such as rent, trailers, mobile homes, hotels, and other forms of housing assistance.

## ***Carryover Projects from FY 2006***

### **Presence at FEMA Field Offices in the Gulf**

As DHS began operating Joint Field Offices in Alabama, Mississippi, Texas, Florida, and Louisiana, auditors and investigators were on site to provide oversight and technical assistance to FEMA and state and local officials. Currently, we have auditors at FEMA's recovery offices in Louisiana, Mississippi, and Florida to provide a visible OIG presence to prevent misspending on questionable contracts and grant activities.

Key tasks to be completed:

- Oversee contract activities for disaster-related services.
- Review public assistance projects as they are being prepared by FEMA.

Department of Homeland Security

- Review major grant recipients to determine whether they have financial management systems that are adequate for managing the grants.
- Conduct interim reviews of large public assistance grant recipients to ensure that they are documenting their costs and that the costs they claim are eligible for FEMA reimbursement.
- Conduct final audits of FEMA sub-grantees as the rebuilding projects by local governments are completed. The objective of these audits will be to determine whether the costs were properly accounted for and expended according to federal regulations and FEMA guidelines. The audits will be conducted via in-house staff and contract auditors.

**FEMA's Management and Oversight of Federally Declared Disasters Designated as FEMA -1577-DR-CA and FEMA-1585-DR-CA**

The California Office of Emergency Services (OES) requested that we review FEMA's management of federally declared disasters FEMA-1577-DR-CA and FEMA-1585-DR-CA, winter storms of late 2004 and early 2005, respectively. Among OES assertions is that FEMA, in administering these disasters, violated federal regulations prescribed by the Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended, Title 44 of the Code of Federal Regulations, Part 206, the Public Assistance Policy Digest (FEMA 321), and the Public Assistance Guide (FEMA 322).

***Audit Objective:*** Determine whether FEMA properly managed the Public Assistance Program for the above noted disasters.

**Review of FEMA's Solicitation and Award of Temporary Housing Maintenance & Deactivation Contracts**

Following Hurricane Katrina, FEMA awarded 37 task order contracts to maintain and deactivate trailers in Alabama, Louisiana, Mississippi, and Texas. Several of the unsuccessful bidders complained to FEMA, Congress, and the media that FEMA:

- Provided inconsistent information to bidders,
- Awarded contracts to unqualified bidders,
- Awarded contracts to contractors with excessive costs,
- Did not properly consider small and minority-owned businesses,
- Provided inadequate debriefing to unsuccessful bidders,
- Awarded contracts to "low ball" bidders, and
- Intends to destroy documentation supporting unsuccessful bids.

Congress held a hearing on the subject in May 2006. Shortly thereafter, two members asked us to review the contract.

***Review Objective:*** Determine whether FEMA properly solicited and awarded contracts for temporary housing maintenance and deactivation.

---

### **Use of the Disaster Relief Fund following DHS's Establishment of the Preparedness Directorate**

A DHS reorganization that took effect October 18, 2005, nearly two months after Hurricane Katrina made landfall, eliminated the Emergency Preparedness & Response Directorate. FEMA, which had been part of that Directorate, was placed directly under the DHS Secretary. The reorganization created a DHS Preparedness Directorate separate from FEMA, which absorbed some of FEMA's preparedness functions. These changes in organizational responsibilities create a situation whereby FEMA and the Preparedness Directorate may have overlapping funding objectives related to various preparedness and readiness activities. Given the broad funding spectrum of FEMA's Disaster Relief Fund (DRF), it is critical that the DRF be monitored to ensure that it is being used appropriately.

**Review Objective:** Determine whether FEMA is using the DRF for eligible expenses following DHS's establishment of the Preparedness Directorate.

### **Selected Components of FEMA's Individual and Households Program**

Several components of FEMA's Individual Assistance grant program provide non-housing assistance for disaster victims. For example, victims may be able to get reimbursement for generators, chain saws, medical and dental costs, lost personal property, automobiles, and funerals.

**Review Objectives:** Determine the efficacy of FEMA's policies and procedures for: (1) determining what costs will be paid, (2) ensuring applicant eligibility, (3) processing claims, (4) managing recertification for rental assistance, and (5) ensuring recoupment of overpayments, duplicate payments, and payments to ineligible recipients.

### **FEMA's Technical Assistance Contracts**

In the aftermath of Katrina, FEMA awarded sole source contracts to four companies for the installation, operations, maintenance, and deactivation of temporary housing units, among other tasks. The total value of these contracts is anticipated to be almost \$3 billion. Though all four companies were among the top 50 construction contractors in the country, the contract files did not contain documentation describing the process used to select these firms over other large firms. In addition, some of the task orders on these contracts were not definitized for several months, and FEMA initially did not have trained and experienced staff to monitor the costs or performance of these contracts.

**Review Objectives:** Determine the adequacy of contract documents, price reasonableness, the effectiveness of the inspection and payment processes, the effective use of warranties, and FEMA's adherence to effective contracting practices.



### **Contractor Billings for Hotels and Motels**

FEMA provides for temporary housing for disaster victims in hotels until such time as the victims can be transferred to longer term housing programs such as apartments, travel trailers, and mobile homes. Immediately after Hurricane Katrina, the American Red Cross provided hotel and motel rooms for evacuees until October 24, 2005. They were awarded a contract on October 20, 2005 for \$250 million to provide housing and pharmaceutical assistance to eligible evacuees for the period from August 29 to October 24, 2005. Subsequent to October 24, 2005, FEMA assumed responsibility for providing hotel and motel rooms for Katrina evacuees and awarded a task order under a General Services Administration (GSA) contract. Under this task order, the contractor was to be paid a flat rate of \$2.48 per night per room with the actual lodging costs to be paid separately.

**Review Objective:** Determine whether lodging rates were reasonable, allowable, and measurable; whether evacuees were eligible to receive lodging; and whether FEMA and the American Red Cross followed effective contracting practices.

### **FEMA Mission Assignments**

In any declared disaster or emergency, FEMA may direct other federal agencies, through mission assignments, to perform activities to support state and local governments. The agencies can request reimbursement from FEMA for eligible costs incurred during performance of the mission as the work is completed. We are reviewing FEMA mission assignments to the five DHS components that received the largest mission assignments: Federal Protective Service, USCG, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and National Communication System. FEMA awarded \$775 million in Katrina mission assignments to those five DHS components.

**Review Objective:** To determine whether mission assignments were managed to satisfy mission requirements, funds were spent effectively and accurately accounted for, contracting followed proper procurement procedures, adequate documentation was maintained, and that purchased property was managed according to governing laws and regulations.

### **FEMA Sheltering and Transitional Housing for Evacuees**

Hurricanes Katrina and Rita produced more than one million evacuees. Many are still living in transitional housing. We are reviewing FEMA's planning for sheltering evacuees, and implementation of transitional housing that included long-term sheltering, hotels and motels, apartments, travel trailers and manufactured homes, cruise ships, and fixed facilities. We will include FEMA's coordination with state and local governments and voluntary agencies, and assess how well evacuee needs were met. The review will identify the actions FEMA is taking to be better prepared to provide housing to evacuees of future catastrophic disasters and recommend ways to prevent problems that occurred during the response to Hurricane Katrina.



**Review Objective:** Determine to what extent FEMA's transitional housing program met the needs of the hurricane victims and to identify weaknesses that need to be addressed for future disasters.

### **FEMA's Property Management**

Disaster assistance operations involve numerous acquisitions of personal property by FEMA as well as other agencies. We will review FEMA's management of personal property and will evaluate internal controls to ensure that personal property purchased during disaster operations is properly accounted for and managed. Personal property received through international donations also will be part of this effort.

**Audit Objective:** Determine the efficacy of FEMA's property management system for disaster operations, i.e., how personal property is acquired, received, issued, disposed of, controlled, and tracked by the JFOs, Agency Logistics Centers, Territory Logistics Centers, and Remote Storage Sites.

### **Potential for Duplication Among Federal Disaster Assistance Programs**

We are preparing an inventory of federal disaster assistance programs and assessing their potential for duplication of benefits. This is a high-level review rather than an effort to identify specific incidents of duplication. We plan to use case studies to demonstrate the importance of applying safeguards to these programs to prevent both intentional and inadvertent duplication of benefits. Some instances of overlapping programs have already surfaced, such as individuals receiving both cash for rental assistance and housing provided by federal agencies.

**Review Objective:** To produce a baseline report that identifies programs and areas within the federal government that are at risk of providing duplicate benefits to disaster victims.

### **Potential for Improved Intergovernmental Coordination and Data Sharing Among Federal Agencies**

A variety of federal agencies collect data that may benefit FEMA in activities such as determining eligibility of individuals for assistance and preventing duplicate assistance payments. Similarly, FEMA collects data that might be useful to other agencies. For example, FEMA data might contain information on the post-disaster location of missing children or others displaced by a disaster.

**Review Objective:** Determine how interagency data sharing might improve the effectiveness of disaster response and recovery.

### **Hurricane Katrina Fraud Task Force**

Our investigators continue to be active participants on the Department of Justice Fraud Task Force established by the U.S. Attorney General on September 8, 2005. As a result of hurricanes Katrina and Rita, we have established offices in Baton Rouge, Louisiana, Biloxi, Mississippi, Mobile, Alabama, and Hattiesburg, Mississippi. We have staffed these offices primarily with temporary investigators who are Cadre of On-Response Employees or Disaster Assistance Employees. We will continue to fully participate on the task force during FY 2007.

### **After Action/Lessons Learned**

The Homeland Security Roundtable of the PCIE/ECIE has been focused on Hurricane Katrina since September 2005. Twenty-two OIGs have participated in reviewing their agencies' and departments' roles in the federal government's response to the hurricane. We have created an after action/lessons learned subgroup of the Roundtable to evaluate our experiences in eight key areas:

- Law Enforcement
- Contracts
- Data Sharing
- State and Local Liaison
- Training
- Funding and Staffing
- Reporting
- Mission Assignments

***Review Objective:*** To inform the PCIE/ECIE of lessons learned from the OIG community's response to Hurricane Katrina.

## **SPECIAL INITIATIVE**

### **DHS Plan for Implementation of Secure Systems of Transportation *(Mandatory)***

Sec. 809(c) of the Coast Guard and Maritime Transportation Act of 2004 requires the Secretary of DHS to submit to the Congress a plan for the implementation of secure systems of international intermodal transportation as directed by Sec. 70116 of title 46, United States Code. Sec. 70116 includes requirements for establishing standards and procedures for screening and evaluating U.S. bound cargo prior to loading at a foreign port, standards for securing cargo and monitoring that security while in transit, and performance standards to enhance the physical security of shipping containers. Also, the plan must include a timeline for establishing the standards and procedures under Sec. 70116(b).

Sec. 809(d) requires our office to submit an evaluation of the progress made by DHS in implementing the plan to the Congress one year after the plan is issued. However, DHS has not issued the plan.

**Audit Objective:** Determine DHS's progress in implementing its plan to secure systems of international intermodal transportation

## CIVIL RIGHTS CIVIL LIBERTIES

### *Carryover Project from FY 2006*

#### **Treatment of Immigration Detainees Housed at Immigration and Customs Enforcement Facilities**

This audit addresses the treatment of immigration detainees held at Immigration and Customs Enforcement (ICE) facilities on immigration charges. ICE established detention standards at its facilities to ensure the overall safety, security, and well-being of detainees in its care. The audit will cover five detention facilities.

**Audit Objective:** Determine the extent to which ICE facilities that house immigration detainees complied with detention standards.

## CUSTOMS AND BORDER PROTECTION

#### **Targeting of Oceangoing Cargo Containers – 2008 (Mandatory)**

Section 809 (g) of the Coast Guard and Maritime Transportation Act of 2004 (Public Law 108-293) requires our office to evaluate and report on the effectiveness of the cargo inspection targeting system for international intermodal cargo containers.

In FY 2005, approximately 11 million cargo containers arrived at U.S. seaports. Since Customs and Border Protection (CBP) officers are not able to review or inspect every container, CBP developed the Automated Targeting System (ATS) to assist in the selectivity and targeting of high-risk shipments. ATS uses weighted rules to evaluate and score shipments to determine whether the containers that make up the shipment are subject to immediate release, document review, or to an inspection. CBP's automated targeting capabilities are essential to the layered risk-management process employed to identify and inspect the high-risk cargo that warrants screening and inspection. The FY 2006 Presidential budget request for ATS was \$28.3 million.

Department of Homeland Security

**Audit Objective:** Determine the effectiveness of the CBP Targeting System in detecting potential acts of terrorism using oceangoing cargo containers.

**Review of SBIInet Baseline**

The Secure Border Initiative (SBI) is a comprehensive effort to secure our borders that includes CBP's program to modernize border patrol operations called SBIInet. The SBIInet is a new start, major acquisition program intended to gain operational control of the Nation's borders through improved use of technology, infrastructure, and personnel. CBP is using a high-risk acquisition strategy that is dependent on hiring a systems integration contractor to provide national and sector solutions for achieving the program's objective. Lacking organic capacity, CBP must also build the capacity to manage the program, and award and administer its many complex contract actions and interagency agreements as it starts the program. Further, CBP has yet to set an Acquisition Program Baseline, which is needed to establish performance and schedule requirements, estimate total acquisition costs, and justify program budgets.

**Audit Objectives:** Determine the extent of CBP's development and implementation of the SBIInet acquisition program baseline. Determine whether CBP has policies, capabilities, and practices to manage SBIInet program risks.

**Automated Commercial Environment Cargo Selectivity And Targeting**

CBP is developing the Automated Commercial Environment (ACE), a new cargo processing system that was initiated to modernize the targeting, inspection, enforcement, border security, revenue collection, and trade statistics processes for all cargo entering and leaving the United States. The ACE contract was started in August 2001 and is scheduled for completion in September 2011 at an estimated cost of \$3 billion. A segment of the contract is to design the new cargo selectivity and targeting (CS&T) module that will modernize and consolidate the legacy targeting systems. CBP's automated targeting capabilities are essential to the layered risk-management process employed to identify and inspect the high-risk cargo that warrants screening and inspection. Selectivity and targeting is further complicated by the dynamic nature of international trade with 134 million conveyances, \$31 billion in revenue at 308 ports of entry, and more than two million pounds of illegal drugs.

**Audit Objective:** Determine the extent to which CBP has established clearly defined and validated requirements for the CS&T module of ACE.

**Carrier Fines Processing at U.S. Ports of Entry**

CBP is responsible for assessing and collecting duties, taxes, and fees, on imported and other goods and services. In FY 2005, CBP collected \$31.4 billion at 308 ports of entry. When carriers bring merchandise into the United States, CBP releases the merchandise and collects estimated duties, taxes, and fees based on entry documents filed. The purpose of fines for carrier violations is to encourage compliance with Customs laws and regulations

CBP has the authority to assess penalties and fines, and seize merchandise for violation of CBP laws or those of other federal agencies. CBP also mitigates penalties, decides petitions, and cancels claims in accordance with national policies and procedures for processing fines, penalties, and forfeiture cases. Laws, regulations, and mitigation guidelines designed to afford the claimant the greatest possible due process strictly govern the processing and disposition of these cases.

***Audit Objective:*** To determine if the fines process is an effective tool to increase carrier performance and compliance with the law.

### **Security Controls for Automated Commercial Environment**

The ACE Secure Data Portal is essentially a customized computer screen similar to a web site home page that connects CBP, the trade community, and other government agencies by providing a single, centralized, on-line access point for communications and information. ACE revolutionizes how CBP processes goods imported into the United States by providing an integrated, fully automated information system to enable the efficient collection, processing, and analysis of commercial import and export data. Currently, the ACE Secure Data Portal, the on-line access point to ACE, is accessible to more than 1,000 CBP and trade community users.

***Audit Objective:*** Determine whether DHS has implemented adequate and effective security controls over the ACE to ensure the efficient collection, processing, and analysis of commercial import and export data.

### **Automated Targeting System Security Controls**

Approximately nine million oceangoing cargo containers arrive annually at seaports in the United States, making it impossible to physically inspect each container without hampering the flow of commerce. To determine which containers to inspect, CBP inspectors at overseas Container Security Initiative ports and U.S. seaports rely on the ATS. Based on information received by CBP on cargo and passengers, ATS assesses a risk rating to cargo and passengers. Inspectors then use this information to determine whether an inspection should be conducted, and if so, what type of inspection is warranted.

***Audit Objective:*** Determine whether adequate logical and physical access, configuration management, and continuity of operations controls have been implemented for the ATS and its data.

### **Evaluation of the Secure Border Initiative**

In October 2005, DHS announced the SBInet, a program to provide an array of technologies, sensors, and systems to improve border security. The SBInet contract is scheduled for award in September 2006. At the same time, DHS expects to meet a

Department of Homeland Security

congressional request to prepare an overall strategy for immigration policy enforcement and border security by the end of April. Once the strategy is complete, the agency in June will begin to create an operational plan with supporting metrics.

**Audit Objectives:** Determine whether DHS has adequate technical strategies, implementation plans, contractor oversight, funding, and reporting procedures for the program.

**A Review of Customs and Border Protection's Procurement of Untrained Canines (Congressional)**

In February 2006, CBP issued a solicitation seeking vendors to provide untrained canines to train for use by the DHS. In April 2006, a total of \$71.6 million was awarded to seven vendors for the purchase of 2,725 dogs, at an average cost of \$26,000 per dog. A casual search of several Internet sites revealed that untrained dogs of the same breed and age as those being sought under the contract are readily available for approximately \$1,000 per animal. Moreover, several news reports discussing the use of canines in security and detection operations have indicated that the cost of a fully trained dog is approximately \$6,000-\$10,000.

**Inspection Objectives:** Determine (1) the reasonableness of the cost of the untrained dogs, (2) whether each vendor awarded a contract possessed a federal license to engage in the sale of dogs at the time of responding to the solicitation or have obtained such license since award, (3) whether each vendor possessed a valid breeder's license at the time of responding to the solicitation or have obtained such license since award, (4) whether CBP acquisitions personnel determined the necessity to validate license information, (5) the criteria used by CBP acquisition personnel to determine that dog trainers who are not breeders would more appropriate for procuring untrained dogs, (6) were subcontracting plans submitted by any vendors; if so, were the subcontractors properly licensed, (7) whether CBP acquisition personnel conducted investigations regarding trainers' ability to care for the dogs, (8) the additional cost to CBP to train the dogs and for dog handlers, (9) the capacity of CBP's dog training facility, (10) the percentage of dogs that are deemed unfit for service and CBP's plan for disposing of those dogs deemed unfit, and (11) the role of the dog deployment in CBP's overall border protection strategy.

***Carryover Projects from FY 2006***

**Targeting Oceangoing Cargo Containers 2007 (Mandatory)**

Sec. 809(g) of the Coast Guard and Maritime Transportation Act of 2004 (Public Law 108-293) requires our office to annually evaluate and report on the effectiveness of the cargo inspection targeting system for international, intermodal cargo containers. Due to the high volume of international intermodal containers arriving into the United States (approximately nine million in FY 2004), CBP officers are not able to review or inspect

every container. As a result, CBP developed the ATS to assist in targeting high-risk shipments. ATS evaluates and scores shipments based on weighted rules. The score received determines whether the container(s) that constitute the shipment are subject to immediate release, document review, or inspection. The Department of Homeland Security Appropriations Act, 2006, includes \$28.3 million for ATS, an increase of \$5.4 million over FY 2005. This is the third in a series of annual audits.

**Audit Objective:** Determine the effectiveness of CBP's targeting system in detecting potential acts of terrorism using oceangoing cargo containers.

### **Follow-up Review on Recommendations from Audit of Procedures to Detect Uranium in Two Smuggling Incidents**

In September 2004, we issued an audit report entitled, *Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents (OIG-04-39)*. This audit report included recommendations to enhance the training and search procedures followed by CBP inspectors as well as the effectiveness of the radiation detection equipment. The Chairmen and Ranking Members of four House and Senate Committees requested that we determine the status of CBP's implementation of these recommendations.

**Audit Objective:** Determine the status of the recommendations made in our initial report on CBP's procedures to detect uranium at the ports of entry.

### **Interagency Inspectors General Review of U.S. Export Control Activities (Mandatory)**

The United States controls the export of dual-use commodities, i.e., goods and technologies that have both civilian and military uses, and munitions for national security and foreign policy purposes under the authority of several laws, primarily the Export Administration Act of 1979 and the Arms Export Control Act of 1976. This is the eighth and final audit required by Congress for export control.

**Audit Objective:** Determine the consistency of outbound inspection activity and follow up on DHS actions and plans to implement the recommendations of the prior audit reports.

### **ACE e-Manifest Functionality for Trucks (Release 4)**

The ACE contract was started in August 2001 and it is scheduled for completion in September 2011 at an estimated cost of \$3 billion. The ACE e-Manifest Functionality for Trucks (Release 4) provides an electronic truck manifest, a primary inspector interface, and expedited importation processing. The deployment of this release is to provide CBP officers with better enforcement capabilities while expediting the movement of cargo into the United States. This release meets the Trade Act of 2002 requirement that CBP provide an automated manifest for the trade. Release 4 was initially deployed during December 2004 at the Port of Blaine, Washington. Several setbacks resulted in the decision to discontinue deployment of Release 4 at the other six scheduled ports until all issues were



Department of Homeland Security

resolved. As a result of this setback, Release 4 was rescheduled to start in April 2005 at various other ports. Trucks are the first mode of transportation released under ACE.

**Audit Objective:** Determine to what extent CBP is effectively detecting and resolving problems in the deployment of ACE as of Release 4.

**CBP's Agricultural Inspection Activities**

On March 1, 2003, functions of several border agencies including the former U.S. Customs Service and the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service were transferred to CBP. This transfer divided inspection activities between USDA and CBP.

CBP has more than 41,000 employees to manage control and protect our Nation's borders at and between the port of entry. CBP's Office of Field Operations oversees 25,000 of these employees, including the 19,000 CBP officers and agriculture specialists, and oversees programs and operations at 20 field operations offices, 317 ports of entry, and 14 pre-clearance stations in Canada and the Caribbean. In FY 2004, CBP agriculture specialists intercepted more than 1.5 million prohibited items.

**Audit Objective:** Determine the extent to which CBP conducted agricultural inspection activities transitioned from USDA to prevent or minimize the introduction of harmful, exotic pests and diseases in the United States.

**One Face at the Border Initiative**

CBP is responsible for securing the U.S. borders. In the past, travelers entering the United States underwent two immigration and customs inspections conducted by separate groups of DHS employees. To increase employee flexibility and operational efficiency in securing the border, CBP began the "One Face at the Border" initiative. The initiative combined Customs and former Immigration and Naturalization Service (INS) personnel into a consolidated workforce on July 25, 2004. CBP expects that having fully trained CBP Officers will expedite the inspection process for the vast majority of travelers and trade passing through our nation's ports of entry.

**Audit Objective:** Determine whether CBP has adequate plans, controls, and measures for implementation of One Face at the Border.

**Border Patrol Background Checks**

The Border Patrol was established in 1924 and transferred into DHS – CBP in March 2003. The Border Patrol's mission is to prevent the entry of terrorists and their weapons of terrorism, and to enforce the laws that protect America's homeland by the detection, interdiction, and apprehension of people who attempt to illegally enter or smuggle people or contraband across our borders. Border patrol agents patrol nearly 6,000 miles of



international land border with Canada and Mexico, and nearly 2,000 miles of coastal border.

In May 2005, President Bush announced his commitment to hire an additional 6,000 agents by the end of 2008, bringing Border Patrol's total strength to 18,000 agents. Before appointment, tentative selectees must undergo and satisfactorily complete a background investigation. The background investigation will include at least a personal interview, a check of past arrest records, a credit check, and interviews of employers and personal references.

***Audit Objective:*** Determine the extent of controls over CBP's background checks for Border Patrol agents.

### **Recruiting, Hiring and Training of Border Patrol Agents**

Public Law 108-458 requires the Border Patrol to increase the number of new agents, not less than 2,000 each year, beginning in fiscal year (FY) 2006 and going through FY 2010. Last year, CBP launched a national recruiting campaign with plans to hire up to 2,100 new agents in 15 months. With the 2006 emergency war supplemental and the FY 2007 appropriations, CBP expects to receive funding to hire an additional 2,000 agents. The House Homeland Security Committee held a hearing in May 2005 questioning whether the Federal Law Enforcement Training Center had capacity for 2,000 additional Border Patrol agents per year. By December 31, 2008, CBP expects the Border Patrol agent workforce to be over 18,000, approximately 6,400 more than the number of agents currently employed.

***Audit Objective:*** Determine to what extent CBP has the capability to recruit, hire, and train new agents.

### **Customs and Border Protection Contract with Chenega Technical Services Corporation for Inspection Equipment Maintenance**

Alaska Native Corporations are eligible to participate in the Small Business Administration's 8(a) Business Development program. They have procurement advantages compared to other 8(a) firms, such as ability to win sole-source contracts without dollar limits. CBP used these advantages to award Chenega Technical Services Corporation a sole-source contract worth up to nearly \$500 million over nine years. Due to the size and nature of this procurement, we are examining issues related to its award and oversight.

***Audit Objectives:*** Determine the propriety of CBP's decision to use the 8(a) Business Development program for equipment maintenance and Chenega Technical Services Corporation, and determine Chenega Technical Services Corporation's compliance with, and CBP oversight of, subcontracting limits.

### **Laptop Computer Security - CBP**

As the weight and price of laptops have decreased and their computing power and ease of use have increased, so has their popularity for use as primary or alternate computers for government personnel. However, due to their portability, the use of laptops significantly increases the risk of theft or loss. As a result, there is increased risk that national security or sensitive data may be exposed, possibly resulting in harm to our national infrastructure. Consequently, government organizations that provide for the use of laptop computers must take steps to ensure that the equipment and the information that is stored on them are adequately protected.

***Audit Objective:*** Determine whether CBP has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptops.

### **Review of Security, Immigration, and Trade Policies Along the Michigan – Canadian Border**

Michigan is the principal gateway for international trade with Canada. To illustrate, the Ambassador and Blue Water Bridges rank as the top two commercial crossings on the U.S. – Canada border, with more than 4.7 million annual truck crossings and 19.4 million annual passenger crossings. The Michigan Department of Transportation is currently operating under an implicit border policy embedded within the State Long Range Plan. However, it would like to adopt an explicit border policy because, as it stands, no single authority regulates or coordinates border crossing policies or lobbies for improvements. Currently, a mixture of government agencies on both sides of the border controls the border. Michigan has been featured heavily in reports of travelers with watchlist records who seek entry to the United States.

***Inspection Objectives:*** Determine whether security policies and agreements between the U.S. and Canadian governments, the State of Michigan, and local law enforcement entities—with potential focus on security procedures in effect at the Ambassador and Blue Water Bridges—are sufficient to prohibit travelers with watchlist records from gaining entry to the United States.

### **Recent Chinese Smuggling Cases' Affect on the Container Security Initiative and Customs-Trade Partnership Against Terrorism ([Congressional](#))**

In January and April 2005, 32 and 39 Chinese nationals, respectively, were found emerging from containers arriving at the Port of Los Angeles. Irrespective of their purpose, of greater concern is that they could have been members of terrorist organizations or that the container could have contained a weapon of mass destruction. The containers involved were targeted by DHS for examination or document review, yet apprehension of the nationals resulted only because of the vigilance of dockworkers.

The Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Homeland Security requested that we review whether current layers of container security are effective in mitigating the smuggling threat; whether DHS is learning from and adjusting its operations based on these incidents; and whether additional changes should be considered.

**Inspection Objectives:** Determine (1) the lessons learned from these recent human smuggling incidents; and (2) whether DHS is incorporating these lessons learned from these events into its targeting systems and operations.

## DOMESTIC NUCLEAR DETECTION OFFICE

### Survey of Domestic Nuclear Detection Office Activities (Congressional)

DHS, through its Domestic Nuclear Detection Office (DNDO), has a leading role in improving detection capabilities to reduce nuclear and radiological threats. It must coordinate with the Department of Energy, which also oversees nuclear detection programs. Important aspects of DNDO's mission relate to the expansion of government nuclear detection and response capabilities, the linkage of related efforts, and monitoring of detection systems. DNDO can help prevent a domestic nuclear/radiological incident or significantly reduce the consequences of such an incident through the effective execution of work in these mission areas.

**Inspection Objectives:** Survey DNDO's (1) efforts to enhance nuclear detection and response capabilities at all levels of government, link related efforts and ensure appropriate information sharing, and maintain effective monitoring and awareness of detection systems; (2) progress in engaging other governmental and nongovernmental partners to further DNDO's mission; and (3) coordination activities with federal agencies with similar responsibilities. This review will serve to establish a baseline for future reviews.

## FEDERAL EMERGENCY MANAGEMENT AGENCY

### FEMA Logistics Systems

FEMA relies on a number of automated logistics systems to support its disaster planning and recovery activities. In 2005, these systems were hard pressed during Hurricane Katrina to keep up with overwhelming support requirements, including the ability to track the transportation of personnel and supplies to stricken areas. In the aftermath of Hurricane Katrina, FEMA initiated efforts to improve its logistics processes and related systems.

**Audit Objective:** Determine the effectiveness of FEMA's plans and approaches to reengineering its logistics processes and improving the capabilities of related IT systems.

### **FEMA's Oversight and Effectiveness of the Pre-Disaster Mitigation Grant Program in Reducing Affects from Natural Hazards**

FEMA's Pre-Disaster Mitigation (PDM) program provides funds to state, local, and tribal governments for hazard mitigation planning and the implementation of mitigation projects before a disaster event. Mitigation measures are intended to reduce the overall risks to people and property, and to reduce reliance on funding from disaster declarations. PDM grants are to be awarded on a competitive basis and without reference to state allocations, quotas, or other formula-based allocation of funds.

***Inspection Objectives:*** Determine (1) what ranking and evaluation process FEMA employs in its grant making and whether the process, procedures, and guidance are effective in furthering program goals; and (2) whether there are tangible examples that such measures have reduced the negative effects of natural hazards.

### **A Review of the World Trade Center Captive Insurance Company ([Congressional](#))**

In 2003, Congress provided FEMA \$1 billion to establish a captive insurance company or other appropriate insurance mechanism to handle claims against the City of New York and its contractors arising from debris removal at the World Trade Center site. In March 2003, in collaboration with FEMA, the City of New York established the World Trade Center Captive Insurance Company (WTCCIC). Since WTCCIC's inception, more than 8,000 individual claims have been submitted, but no claims have been paid, while the WTCCIC has spent several million dollars in federal funds on legal fees to defend New York City and other named insured against these claims.

***Inspection Objective:*** Determine (1) why the WTCCIC has chosen to litigate all claims instead of settling whenever possible, and (2) what procedures have been established to receive, review, and pay medical, hospital, surgical, and disability benefits to injured persons, and funeral and death benefits to dependents, beneficiaries, or personal representatives of persons who were killed.

### ***Carryover Projects from FY 2006***

#### **Upgrade of the National Emergency Management Information System – eNEMIS**

Within DHS, FEMA has been delegated responsibility for coordinating emergency response and recovery activities with other federal agencies, as well as with state and local governments. Ensuring interoperable information technology is critical to effectively accomplish this mission. In our report, *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery* (OIG-05-036), we identified problems and issues regarding FEMA's IT management approach.

Specifically, we reported that IT systems cannot effectively handle increased workloads, are not adaptable to change, and lack needed real-time reporting capabilities.

As part of its effort to improve its emergency management systems, FEMA is transforming the NEMIS into a web-based application, called eNEMIS. This effort involves modernization of the current NEMIS components, including the integration and consolidation of supporting systems to create a user-friendly, single point-of-access resource. The effort affects approximately 13,000 users, including DHS employees, temporary employees, contractors, and other federal and state employees from 27 different government organizations.

**Audit Objectives:** As a follow-up to our September 2005 report, we will determine the effectiveness of FEMA's approach to procuring and implementing eNEMIS to improve support for emergency management operations.

### **Laptop Computer Security - FEMA**

As the weight and price of laptops have decreased and their computing power and ease of use have increased, so has their popularity for use as primary or alternate computers for government personnel. However, due to their portability, the use of laptops significantly increases the risk of theft or loss. As a result, there is increased risk that national security or sensitive data may be exposed, possibly resulting in harm to our national infrastructure. Consequently, government organizations that provide for the use of laptop computers must take steps to ensure that the equipment and the information that is stored on them are adequately protected.

**Audit Objective:** Determine whether FEMA has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptops.

## **IMMIGRATION AND CUSTOMS ENFORCEMENT**

### **Audit of MOU between DHS and the General Services Administration - Joint Audit with the General Services Administration OIG**

The Homeland Security Act of 2002 transferred responsibility for protecting buildings, grounds, and property that are owned, occupied, or secured by the federal government and the persons on the property, from the GSA to DHS. In March 2003, DHS and GSA concluded a Memorandum of Understanding (MOU) to define new roles and relationships between the ICE Federal Protective Service (FPS) and GSA concerning the security of GSA-controlled space. In June 2006, a new MOU was concluded between DHS and GSA that more clearly identifies the roles, responsibilities, and operational relationships between ICE/FPS and GSA. This MOU defines respective FPS and GSA roles in areas such as law

Department of Homeland Security

enforcement, facility security, technical guidance and assistance, contractor security guards, security equipment, and security services billings. Recent DHS and GAO audits have noted problems and challenges. Since the formation of DHS in 2003, audits have noted unresolved issues related to FPS funding and billing for facility security services and the transfer of GSA functions to FPS.

**Audit Objective:** Determine the extent to which the FPS and GSA's Public Building Services are fulfilling their respective responsibilities under the June 2006 MOU to provide for security for GSA-controlled space and facilities. This audit will be conducted jointly with the GSA OIG.

**DHS's Progress in Implementing Memorandums of Understanding with States and Local Governments Under Section 287(g) of the Immigration and Naturalization Act (Congressional)**

The prisons and jails in this country are estimated to book roughly 630,000 foreign-born nationals on criminal charges annually. Too often, the criminal aliens among this population are not removed from the country upon completion of their criminal sentences, but released into society. To combat this problem, Immigration and Customs Enforcement will expand its Criminal Alien Program and its 287(g) agreements with state/local correctional institutions to ensure these aliens are properly identified while in jail and removed immediately after serving their sentences. Currently, there are four correctional/detention facilities around the country that participate in the 287(g) program, while numerous agencies have pending requests with ICE for such agreements.

**Inspection Objectives:** Determine (1) the progress ICE has made in expanding the 287(g) program to other jurisdictions; and, (2) how the \$5 million that was appropriated for the program in FY2006 was spent.

**DHS and Department of State Staffing of Visa Security Processing**

On September 26, 2003, the Departments of State (State) and Homeland Security signed an MOU, per the Homeland Security Act of 2002. This MOU set the terms under which the two departments will work together in the visa adjudication process (Section 428 of the Homeland Security Act). However, overlap in missions and responsibilities between State and DHS staff continues to pose a problem in some embassies. This review will assess the competing authorities and procedures in visa screening that result when State Diplomatic Security Bureau Officers, State Consular Affairs Bureau Anti-Fraud Officers, and DHS Visa Security Officers are all present in a single embassy. It is proposed as a joint review with State at the U.S. Embassy in Manila, Philippines.

**Inspection Objectives:** Determine (1) areas of authority and mission overlap between the Department of State and DHS in visa security issues; (2) the effectiveness of the MOU between State and DHS in guiding visa security coordination and cooperation; and (3) opportunities to clarify procedures and reduce duplication of effort.

---

### **Effectiveness of S, T, and U Visas in Prosecuting Human Trafficking**

On October 28, 2000, the Victims of Trafficking and Violence Protection Act, Public Law No. 106-386, created three new visa classes: an S-Visa for informants, a T-Visa for victims of trafficking, and a U-Visa for victims or witnesses who have suffered substantial physical or mental abuse and agree to cooperate with the government [8 USC Section 1101 (a)(15)].

***Inspection Objectives:*** Determine how often and for what purpose S, T, and U special visas are used, and whether they have assisted in the successful prosecution of trafficking cases.

### ***Carryover Projects from FY 2006***

#### **ICE Detainee Tracking Process**

ICE responsibilities are (1) to provide adequate and appropriate custody management to support removal; (2) to facilitate the processing of illegal aliens through the immigration court; and (3) to enforce their departure from the United States. ICE secures bed space in detention facilities, and monitors these facilities for compliance with national detention standards. Detainees are often transferred from one facility to another for various reasons including medical, change of venue, recreation, security issues, or other ICE needs. During fiscal year 2005, ICE detained in custody an average of 18,500 aliens per day and formally removed 204,193 aliens from the United States.

***Audit Objective:*** Determine whether ICE has an effective system to track the location of detainees and respond to public inquiries.

#### **Risk Management Advisory on SBInet Program Initiation**

DHS has announced its secure border initiative strategy for controlling the border and reducing illegal immigration, which includes a CBP-led program to modernize border patrol operations and technology. This critical component of the secure border initiative is called SBInet, a new major acquisition program, replacing two previous efforts to gain control of the borders: the integrated surveillance intelligence system and the America's shield initiative. CBP plans to award a multi-year contract to hire a systems integrator in September 2006.

We will review CBP's approach and plans for SBInet, relate and analyze findings and recommendations about other DHS programs and contracts, and advise program officials on managing risks. We will focus this review on the two most critical risk areas for initiating a major acquisition program: (1) operational requirements and (2) organizational capacity.



**Review Objective:** To identify what lessons can be learned from previous and current major acquisition programs to minimize risks to accomplishing SBIInet's objectives.

### **Federal Protective Service's Contract Guard Program**

The Federal Protective Service (FPS) is the component within DHS responsible for managing the physical security in and around federal facilities nationwide, investigating incidents and criminal complaints occurring on federal properties, and conducting risk assessments of federal facilities. FPS has oversight of more than 10,000 contract security guards responsible for deterring unauthorized, illegal, or potentially life-threatening activities directed toward more than one million employees and daily visitors, as well as information, programs, and property at federally owned and leased facilities nationwide. FPS contract guards usually carry firearms and are deployed at fixed or roving posts in and around the perimeter of federal facilities. They often operate security-screening devices, such as magnetometers and x-ray machines, and respond to calls for security services in and around federal buildings. FPS uses contract inspectors, physical security specialists, or other representatives designated by the contracting officer to perform the critical function of monitoring contractor performance and performing guard post inspections.

GSA policy requires that prospective service contract employees, including guards, undergo limited criminal history checks. FPS conducts these checks to determine an applicant's eligibility to function in a position of trust and to identify potential risks or threats to the safety and security of personnel and property. The background check process begins once a guard has received basic training from the contractor and has passed an FPS administered written examination. Guards who are armed must also pass a GSA firearm qualification test before being placed on active duty.

**Audit Objective:** Determine to what extent controls are in place to monitor contractor performance and compliance with contract provisions.

### **Coordination Between the Federal Bureau of Investigation and Immigration and Customs Enforcement on Investigations of Terrorist Financing (Congressional)**

At the request of the Chairman of the Senate Finance Committee, we will conduct a review of allegations made by an ICE special agent in charge that the Federal Bureau of Investigation (FBI) intentionally mishandled a terrorist finance investigation being conducted by his office. In addition, we will examine the success and effectiveness of a memorandum of agreement between the FBI and ICE that prescribes the cooperative measures with regard to terrorist finance investigations. This is to be a joint review with the Department of Justice OIG.



**Inspection Objectives:** Determine whether: (1) the actions of ICE and FBI personnel were appropriate; and (2) whether the agreement promotes effective and efficient cooperation and coordination of terrorist finance investigations.

### **Removal of a Canadian Citizen to Syria (Congressional)**

Our office is evaluating 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; 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 Objectives:** Determine how U.S. immigration officials arrived at their decision to remove this person to Syria and whether the decision was made within prescribed INS policies.

### **Assessment of the Effectiveness of ICE Fugitive Operations Teams**

ICE has received significant funding to support its fugitive apprehension teams. The teams are supposed to identify, locate, and apprehend fugitives. Even though ICE's resources for this activity are growing, so is the absconder population. This is a follow-up review to our recently issued *Review of the Immigration and Customs Enforcement's Compliance Enforcement Unit*.

**Inspection Objectives:** To determine the efficacy of (1) the processes used by the teams to locate and apprehend absconders and fugitives, (2) the removal of apprehended absconders and fugitives, and (3) whether participating on the teams runs counter to ICE's mission.

### **Assessment of the Effectiveness of ICE's Management of Post-Final Order Custody Reviews**

Sec. 241(a) of the Immigration and Nationality Act provides that "[e]xcept as otherwise provided in this section, when an alien is ordered removed, the Attorney General shall remove the alien from the United States within a period of 90 days (in this section referred to as the 'removal period')." 8 USC §1231(a)(1)(A). The statute provides exceptions when removal within the 90-day period is not possible (such as when the alien's country of citizenship will not accept the alien). It also permits detention to continue beyond the 90-day period for aliens charged with certain types of immigration violations who have not been removed, or where the Attorney General determines that the aliens present a risk to the community or a risk of flight. Pursuant to 8 Code of Federal Regulations §241.4(h), aliens held more than 90 days after issuance of a final removal order are entitled to an administrative review to determine if their continued custody is warranted.

Department of Homeland Security

In *Zadvydas v. Davis*, 533 U.S. 678 (2001), the U.S. Supreme Court held that habeas proceedings were available as a forum for challenges to unreasonable post-removal detentions and that six months is a reasonable period in which to determine whether removal is achievable.

A previous Department of Justice OIG report found disagreement over the Immigration and Naturalization Service's (INS) obligations under the 90-day rule and delinquencies in completing the post-order custody reviews. See *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks*, chap. 6 (June 2003).

**Inspections Objectives:** Determine ICE's compliance with applicable removal time limits after the issuance of final orders of removal, and the reasons for exceptions or instances of noncompliance.

## MANAGEMENT

### **FY 2007 Audit of DHS's Consolidated Financial Statements ([Mandatory](#))**

The Chief Financial Officers Act 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, FLETC's, and the Transportation Security Administration's (TSA's) financial statements will be performed in conjunction with the consolidated statement audit.

**Audit Objectives:** Ascertain and report on the fairness of presentations of DHS's FY 2007 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; perform tests of compliance with certain laws, regulations, and provisions of contracts or grant agreements, noncompliance with which could have a material effect on the financial statements; and, report on noncompliance disclosed by the audit. This audit addresses financial performance in the President's Management Agenda.

### **FY 2007 Audit of DHS's Internal Controls over Financial Reporting ([Mandatory](#))**

The DHS Financial Accountability Act requires an annual audit of DHS's internal controls over financial reporting to express an opinion about whether DHS maintained effective internal control.

The OMB Circular A-123, *Management's Responsibility for Internal Control* (Revised), requires agencies' management to assess and document internal control over financial reporting; identify needed improvements; take corresponding corrective action; and make

an assertion about the effectiveness of internal control over financial reporting. The audit will assess DHS management's assertion and effort to implement the Circular, and it addresses financial performance in the President's Management Agenda.

***Audit Objective:*** Ascertain and report on the effectiveness of DHS's internal controls over financial reporting in conjunction with the FY 2007 DHS consolidated financial statement audit.

### **Office of National Drug Control Policy Review (*Mandatory*)**

Under 21 U.S.C. 1704 (d) and the Office of National Drug Control Policy (ONDCP) Circular *Drug Control Accounting*, our office is required to perform a review of assertions made by management related to FY 2006 obligations for the National Drug Control Program at the following DHS bureaus: ICE, CBP, and the USCG. This audit addresses in part financial performance in the President's Management Agenda.

***Review Objective:*** Ascertain and report on the reliability of management's assertions included in their Annual Accounting of Drug Control Funds.

### **National Procurement Fraud Task Force**

Our audit and investigative staff will be active participants on the Department of Justice National Procurement Fraud Task Force, which was established in October 2006. The multi-agency task force will strengthen the government's efforts to fight procurement fraud, focusing resources at all levels of government to increase enforcement in areas of procurement fraud. Its mission is to increase coordination among federal law enforcement to detect and combat procurement fraud. Due to the size and number of contracts awarded by DHS each year, we expect to play a major role on the task force.

### **Audit of DHS's Corrective Action Plan Process and Implementation of OMB Circular A-123**

In FY 2006, DHS began a concerted effort to develop corrective action plans to address numerous material weaknesses in internal control that were identified by the DHS financial statement audit. DHS also began implementing OMB Circular A-123, *Management's Responsibility for Internal Control* (Revised), which requires management to assess and document internal control over financial reporting; identify needed improvements; take corresponding corrective action; and make an assertion about the effectiveness of internal control over financial reporting. Corrective action plans are an integral part of implementing OMB Circular A-123 because they identify needed improvements and corresponding remedial actions.

***Audit Objective:*** Determine the adequacy of DHS's process for developing competent, corrective action plans and how this process is integrated into DHS's plan to fully

*Department of Homeland Security*

implement OMB Circular A-123. This audit addresses financial performance in the President's Management Agenda.

**Audit of ICE's Progress in Improving Financial Management**

Since its creation in 2003, ICE has struggled with severe weaknesses in its financial management and reporting. In FY 2006, ICE contracted with a public accounting firm to help it begin addressing those weaknesses, starting with the development of corrective action plans.

***Audit Objective:*** Determine ICE's progress in implementing its corrective action plans and moving to a more stable, long-term financial management organization and capability.

**Status of Acquisition Function at DHS**

In response to the Secretary's 2005 request, we conducted the 30-day study and issued *Department of Homeland Security's Procurement and Program Management Operations* (OIG-05-53). The report identified numerous deficiencies and proposed multiple recommendations with which DHS generally concurred. In response to the report, DHS established new guidelines and directives, and implemented other steps to improve oversight over its procurements, although responding to Hurricane Katrina added additional complexity to an already strained system. This audit would update the information contained in the 30-day study and potentially identify new issues in programs that have major procurements, such as adequacy of small and disadvantaged business utilization.

***Audit Objective:*** Determine how well DHS manages and supports complex procurement programs.

**Secure Border Initiative Procurements Over \$20 Million (*Mandatory*)**

The Fiscal Year 2007 Department of Homeland Security Appropriations Act requires us to review and report on any contract or task order relating to the SBI program valued at more than \$20 million. The Conferees included this provision to reflect their concern about DHS's ability to manage and oversee the major technology contracts they expect to be part of SBI.

***Audit objective:*** Assess DHS's management of cost, schedule, and performance for each SBI contract or task order valued at more than \$20 million.

**Sole Source Acquisitions**

Full and open competition for contracts is generally presumed to provide the best value to the government (and taxpayers). Without proper competition, the government may be unable to ensure reasonable cost and performance. Federal acquisition regulations require agencies to justify in writing their use of other than full and open competition. Allowable

justifications for sole source awards include special programs, such as Small and Disadvantaged Business Development. Past GAO and OIG audits identified both improper use of sole source awards and poor cost controls for legitimate sole source awards throughout the government. At present, DHS plans seven sole source awards in fiscal year 2006 that will each exceed \$10 million. Given DHS's fundamental deficiencies and weak control environment, sole source awards leave DHS vulnerable to excessive cost and poor performance.

**Audit Objective:** Determine how well DHS justifies and controls sole source acquisitions to assure reasonable cost and performance.

### **Audit of DHS' e-Gov Initiatives (Congressional)**

The President's Management Agenda includes expanding Electronic Government (e-Gov). E-Gov uses improved internet-based technology to make it easy for citizens and businesses to interact with the government, save taxpayer dollars, and streamline citizen-to-government communications. DHS has a number of initiatives underway under e-Gov, including those involving disaster management, grants, and financial management.

**Audit Objective:** Determine what progress DHS is making in implementing its e-Gov programs.

### **Annual Evaluation of DHS's Information Security Program for Fiscal Year 2007 (Mandatory)**

In response to the increasing threat to information systems and the highly networked nature of the federal computing environment, Congress, in conjunction with the Office of Management and Budget, requires an annual review and reporting of agencies' compliance with the requirements under the 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 Objective:** Determine what progress DHS has made in resolving weaknesses cited in the prior year's review.

### **Laptop Computer Security—DHS**

As the weight and price of laptops have decreased and their computing power and ease of use have increased, so has their popularity for use as primary or alternate computers for government personnel. However, due to their portability, the use of laptops significantly increases the risk of theft or loss. As a result, there is increased risk that national security or sensitive data may be exposed, possibly resulting in harm to our national infrastructure. Consequently, government organizations that provide for the use of laptop computers must

Department of Homeland Security

take steps to ensure that the equipment and the information that is stored on them are adequately protected.

**Audit Objective:** Determine whether DHS has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptops. This effort will summarize the results of our laptop security audits at CBP, S&T, OIG, and FEMA.

**Internet Protocol Version 6**

Internet Protocol Version 6 (IPv6) has been recognized as a critical enabling technology for federal agencies. IPv6 will help ensure that the Internet can support a growing user base and the increasingly large number of IP-enabled devices. OMB Memorandum 05-22, "Transition Planning for IPv6," directs agencies to implement the IPv6 protocol within their network backbone by June 2008. In support of this goal, agencies are required to meet a number of interim milestones, including completion of two inventories of IP devices and technologies, completion of an IPv6 transition impact analysis, and development of an IPv6 transition plan. Agencies are required to submit a completed IPv6 transition plan, as well as a progress report on the inventory and impact analysis, as part of their enterprise architecture assessment in February 2006.

**Audit Objective:** Determine the adequacy of DHS's plans and progress in implementing Ipv6, and determine whether DHS components have adequate security controls on deployed IPv6 devices and systems.

**Oversight of Contracted Information Technology-Related Testing Performed as Part of DHS's FY 2007 Audited Financial Statements ([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 DHS'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.

**Review of DHS Financial Systems Consolidation**

The Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency project (eMerge2) will bring together the financial, budget and asset control

activities of the DHS 22 component agencies. As part of this effort, DHS is making plans to consolidate all DHS components on financial systems currently run by CBP and USCG.

***Audit Objectives:*** Determine whether DHS has justified adequately its approach to consolidating financial systems under the eMerge2 program.

### **Technical Security Evaluation Program of DHS Sites (Sites To Be Determined)**

Information security is an important goal for any organization that depends on information systems and computer networks to carry out its mission. Toward that end, DHS has developed an agency-wide information system security program. However, because DHS components and their sites are decentralized, it is difficult to determine the extent to which DHS staff members are complying with security requirements and their respective work sites.

***Audit Objectives:*** On an ongoing basis, at DHS sites, determine the effectiveness of safeguards and compliance with technical security standards, controls, and requirements.

### **Internet Use and Management**

The use of the Internet provides tremendous research capabilities to DHS employees to assist them in the performance of their jobs. However, the Internet also offers the opportunity to browse web sites for personal reasons. Some web sites that could be used for personal use are banking or stock trading, chat room and electronic mail-email, shopping, auctions, sports, sexually explicit, and gambling. Improper use of the Internet could result in decrease in productivity and could foster a hostile environment by allowing sexually explicit material into the workplace via the Internet.

***Audit Objectives:*** Determine the effectiveness of DHS and DHS component efforts to ensure proper and secure use and management of Internet access.

### **Evaluation of DHS's Safeguarding Practices for Personally Identifiable Information**

The loss of personal identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. OMB has required that each agency implement an effective information privacy management program. As is required by the Privacy Act, FISMA, and other laws and policies, DHS must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure, or sharing and to protect associated information systems from unauthorized access, modification, disruption, or destruction.

***Audit Objective:*** Determine the adequacy of the administrative, system, and physical safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.



Department of Homeland Security

**Portable Electronic Devices**

Handheld devices are becoming more feature-rich and portable, and wireless devices and their respective technologies are merging. The mobile phone, for instance, has increased functionality that now allows it to serve as a personal digital assistant (PDA) as well as a telephone. Smart phones are merging mobile phone and PDA technologies to provide normal voice service and email, text messaging, paging, Web access, and voice recognition. Next-generation mobile phones, already on the market, are quickly incorporating PDA, infrared, wireless Internet, e-mail, and global positioning system capabilities. However, each new development will present its own security risks, and government agencies must address these risks to ensure that critical assets remain protected. Vulnerabilities may exist when using PDAs attached to personal computers or other network-connected devices.

***Audit Objective:*** Determine whether adequate physical and logical access controls have been implemented for government-issued portable electronic devices that connect to DHS networks and are used to process or store sensitive DHS information.

**DHS Personnel Security Clearance Screening (Congressional)**

The DHS Personnel Security Division has the mission to “ensure the highest levels of confidence in employee and contractor trustworthiness, loyalty, integrity and reliability.” However, one of the most important challenges confronting DHS is completing background checks on its employees and ensuring that employees have the necessary security clearance to perform their duties.

***Inspection Objectives:*** Determine the progress of DHS’s Personnel Security Division in (1) implementing needed DHS policies; (2) establishing position risk designations; (3) obtaining and updating clearances for executive, senior, other employees, and contractors; (4) ensuring agency compliance with its directives, particularly reciprocity; (5) establishing whether DHS should have investigative authority; (6) establishing whether DHS should use a polygraph examination to strengthen the background review process; and, (7) how clearance processing time affects program performance.

***Carryover Projects from FY 2006***

**FY 2006 Audit of DHS’s Consolidated Financial Statements (Mandatory)**

The Chief Financial Officers Act 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, FLETC’s and TSA’s financial statements will be performed in conjunction with the consolidated statement audit.



***Audit Objectives:*** Ascertain and report on the fairness of presentations of DHS's FY 2006 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; perform tests of compliance with certain laws, regulations, and provisions of contracts or grant agreements, noncompliance with which could have a material effect on the financial statements; and, report on noncompliance disclosed by the audit. This audit addresses financial performance in the President's Management Agenda.

### **FY 2006 Audit of DHS's Internal Controls over Financial Reporting ([Mandatory](#))**

The DHS Financial Accountability Act requires an annual audit of DHS's internal controls over financial reporting to express an opinion about whether DHS maintained effective internal control.

The OMB Circular A-123, *Management's Responsibility for Internal Control* (Revised) requires agencies' management to assess and document internal control over financial reporting; identify needed improvements; take corresponding corrective action; and make an assertion about the effectiveness of internal control over financial reporting. The audit will assess DHS management's assertion and effort to implement the Circular, and it addresses financial performance in the President's Management Agenda.

***Audit Objective:*** Ascertain and report on the effectiveness of DHS's internal controls over financial reporting in conjunction with the FY 2006 DHS consolidated financial statement audit.

### **FY 2006 Audit of DHS Corrective Action Plans**

DHS and its components are developing corrective action plans to address the ten material weaknesses identified by the financial statement auditor in the FY 2005 audit report. An effective corrective action plan process is an important tool and control activity for correcting problems and holding responsible parties accountable for progress. The corrective action plan process is an important element of DHS's internal control structure. We contracted with DHS's financial statement auditor to perform a series of performance audits to assess DHS's progress in implementing an effective corrective action plan process, in support of the FY 2006 audit of internal control over financial reporting, as required by the DHS Financial Accountability Act.

***Audit Objective:*** To determine the adequacy of DHS's progress in implementing an effective corrective action plans process.

### **Office of National Drug Control Policy Follow-Up Review ([Mandatory](#))**

The ONDCP has requested additional procedures based on our reports (OIG-06-25, OIG-06-26, and OIG-06-27) on Reporting of FY 2005 Drug Control Funds for ICE, CBP, and

Department of Homeland Security

the USCG. This review addresses in part financial performance in the President's Management Agenda.

**Review Objective:** To evaluate DHS's controls surrounding ONDCP reprogramming, transfers, and fund control notice requirements.

**Shirlington Limousine and Transportation**

In April 2004, DHS awarded Shirlington Limousine and Transportation, Inc., a \$3.8 million contract to provide employee shuttle service and executive transportation. DHS awarded the contract under the "historically underutilized business zone" (HUBZone) program, which requires that the contractor be a small business, located in a designated HUBZone, and owned and controlled by one or more U.S. citizens, and that at least 35 percent of its employees reside within a HUBZone. In October 2005, Shirlington Limousine obtained a \$21 million DHS contract to continue providing employee and executive transportation. Congressional requesters asked us to examine the circumstances surrounding these contract awards.

**Audit Objective:** Determine whether Shirlington Limousine and Transportation, Inc. met the HUBZone criteria; DHS took reasonable steps to determine that Shirlington was a responsible bidder; and the extent of competition for these awards.

**MAX<sup>HR</sup> Tasks under the Northrop Grumman Blanket Purchase Agreement (Congressional)**

DHS awarded Northrop Grumman Information Technology (Northrop Grumman) a June 2004 blanket purchase agreement (BPA) to support DHS human resources initiatives, including, but not limited to, MAX<sup>HR</sup>. Congress requested that we determine the (a) rationale for using a BPA; (b) deliverables produced; (c) deliverables expected; (d) scheduled completion; (e) money expended; (f) DHS role in executing, managing, and overseeing this BPA; (g) Northrop Grumman's role in executing, managing, and overseeing this BPA; (h) roles of any subcontractors and their deliverables; and (i) appropriateness of one BPA that requires many dissimilar functions.

**Audit Objectives:** Determine the DHS rationale for using a BPA and whether DHS improperly "bundled" dissimilar functions; and assess the adequacy of DHS oversight of MAX<sup>HR</sup> task orders under the Northrop Grumman BPA.

**Training and Qualifications of Acquisition Workforce**

DHS purchased almost \$10 billion of goods and services in fiscal year 2004 through almost 60,000 procurement actions such as contracts, delivery orders, and interagency agreements. DHS, in accordance with statute and government-wide policies, has minimum education, experience, and training requirements for program and project managers; contracting officers; contracting professionals; ordering officials; and contracting officer's technical

representatives. In April 2005, the Office of Federal Procurement Policy (part of the Office of Management and Budget) revised acquisition training requirements. Many DHS components have legacy policies from their previous departments. Human capital is the third cornerstone of GAO's framework for assessing an agency's acquisition function.

**Audit Objective:** Determine to what extent the DHS acquisition workforce meets federal and DHS education, experience, training, and certification requirements; and, the adequacy of measures used to oversee compliance with acquisition workforce training and qualifications requirements.

**Oversight of Contracted Information Technology-Related Testing Performed as part of DHS's Fiscal Year 2006 Audited Financial Statements (Mandatory)**

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

**Audit Objectives:** Determine whether contracted auditors performed sufficient testing to evaluate DHS's general and application controls over critical financial systems and data to reduce the risk of loss due to errors, fraud, and other illegal acts and disasters, and to effectively protect their information infrastructure from security threats or other incidents that cause the systems to be unavailable.

**Technical Security Evaluation Program of DHS Sites (Dulles Airport)**

Information security is an important goal for any organization that depends on information systems and computer networks to carry out its mission. Toward that end, DHS has developed an agency-wide information system security program. However, because DHS components and their sites are decentralized, it is difficult to determine the extent to which DHS staff are complying with security requirements and their respective work sites.

**Audit Objectives:** On an ongoing basis, at DHS sites, determine the effectiveness of safeguards and compliance with technical security standards, controls, and requirements.

**Technical Security Evaluation Program of DHS Sites (Reagan National Airport)**

Information security is an important goal for any organization that depends on information systems and computer networks to carry out its mission. Toward that end, DHS has developed an agency-wide information system security program. However, because DHS

Department of Homeland Security

components and their sites are decentralized, it is difficult to determine the extent to which DHS staff are complying with security requirements and their respective work sites.

**Audit Objectives:** On an ongoing basis, at DHS sites, determine the effectiveness of safeguards and compliance with technical security standards, controls, and requirements.

## OFFICE OF INTELLIGENCE AND ANALYSIS

### **Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for Fiscal Year 2007 (Mandatory)**

Identifying potential information security threats to DHS's intelligence systems is key in evaluating DHS' intelligence program. The loss or compromise of DHS's intelligence systems and the data contained on those systems can have severe consequences, affecting national security, U. S. citizens, and DHS'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 Director National Intelligence, Chief Information Officer, and the Office of Management and Budget, require an annual evaluation and reporting of the security program over agencies' intelligence systems. FISMA and the Director, Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems, requirements will be used as criteria for the evaluation.

**Audit Objective:** Determine what progress DHS has made in resolving weaknesses cited in the prior year's review.

### **Homeland Infrastructure Threat and Risk Analysis Center**

The assessment of risks across and within infrastructure sectors is a core DHS responsibility and a central feature of DHS's infrastructure protection mission. DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) is designed to perform these types of risk assessments by integrating "infrastructure-specific vulnerability and consequence data with threat information." HITRAC produces incident reports, threat warnings, strategic planning information, the Terrorist Target Selection Matrix, attack-specific threat scenarios, and sector-specific threat assessments and threat products for distribution among the intelligence community, DHS, and infrastructure sector stakeholders. HITRAC threat products are designed to support immediate responses to threats and strategic planning to improve the protective standing of critical infrastructures.

**Inspection Objectives:** Determine (1) how HITRAC integrates consequence, vulnerability and threat information, and its management of this enterprise; (2) whether HITRAC risk assessment products integrate the full range of necessary information and provide actionable guidance on risk mitigation activities; (3) whether HITRAC threat products are

comprehensive, actionable, and effectively tailored to their intended audience; and (4) the timeliness, appropriateness, and utility to the recipient of HITRAC threat product distribution.

### **Information Sharing at the National Operations Center (Congressional)**

DHS's National Operations Center (NOC) provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC—which operates 24 hours a day, seven days a week, 365 days a year—coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents. It collects and fuses information from more than 35 federal, state, territorial, tribal, local, and private sector agencies. It shares information on domestic incident management with Emergency Operations Centers at all levels through the Homeland Security Information Network.

***Inspection Objectives:*** Determine what functional and organizational changes the NOC made to better manage the flow of information following Katrina, specifically what new procedures were instituted to ensure that incoming reports are properly reported within the NOC and to the Secretary.

### **Intelligence and Analysis' Fusion Center Initiative (Congressional)**

Executive Orders 13311 and 13356 will enhance the Nation's ability to share terrorism information. Additional laws and regulations have further eased the sharing of terrorism information between agencies. In addition, many states and localities established "information fusion centers" to provide a better tool for sharing and analyzing terrorism information. A 2006 survey indicated that at least 40 states and U.S. territories are developing or already have state or local intelligence-fusion centers. However, there is no national strategy and there are no protocols to define how the federal government will collaborate with these centers.

***Inspection Objectives:*** Determine (1) what problems and challenges are being encountered; (2) the extent to which intelligence and analysis (I&A) has been actively working to coordinate the development of, and relationship between, the fusion centers and the federal government on a national level; (3) how funding and activities are targeted in fusion centers to help carry out the DHS mission, (4) the merits of detailing I&A staff to the centers, and (5) how successful I&A is being in backfilling positions vacated to staff the Fusion Center Initiative.

### *Carryover Project from FY 2006*

#### **Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for Fiscal Year 2006 (Mandatory)**

Identifying potential information security threats to DHS's intelligence systems is key in evaluating DHS's intelligence program. The loss or compromise of DHS's intelligence systems and/or the data contained on those systems can have severe consequences, affecting national security, United States 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 Director National Intelligence, Chief Information Officer and the Office of Management and Budget, require an annual evaluation and reporting of the security program over agencies' intelligence systems. FISMA and the Director, Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, requirements will be used as criteria for the evaluation.

**Audit Objective:** Determine what progress DHS has made in resolving weaknesses cited in the prior year's review.

## OFFICE OF POLICY

### *Carryover Project from FY 2006*

#### **DHS Management of Overseas Operations**

Federal strategies to promote homeland security stress the need to work in an international context, and the DHS Strategic Plan underscores the importance of international efforts in advancing America's homeland security. DHS was created with a considerable overseas presence formed by the international operations of its legacy organizations. DHS has since undertaken several significant initiatives to expand foreign operations further: the Container Security Initiative, the Immigration Assistance Program, and the Visa Security Program. The Intelligence Reform and Terrorism Prevention Act of 2004 calls for considerable future expansion of CBP pre-clearance facilities at airports around the world. The bulk of DHS staff and resources are nested in the operational components, with only a small headquarters staff having overarching responsibilities for the panoply of DHS international programs and activities. Several DHS components are conducting international operations. However, few overseas posts with a multi-component DHS presence have either a DHS Attaché or a Senior Homeland Security Representative to oversee DHS activities and coordinate with ambassadors. Rather, each component's international affairs office coordinates its individual overseas missions and operations. The Department of State OIG has reported on oversight and coordination difficulties as a result of the expansion of DHS assets at U.S. embassies.



**Inspection Objectives:** Determine: what international programs and activities DHS supports; how DHS provides strategic management of and effective internal controls for its international programs and activities; how and whether DHS: ensures effective communication and coordination between international programs and activities; how and whether DHS provides adequate representation for its international programs and activities. This will include an evaluation of the recruitment, training, and deployment of personnel, and the budgeting for overseas operations. We will evaluate the interagency coordination of personnel and operational requirements, especially between DHS (and its components) and the Department of State (and its Chiefs of Mission) - especially at posts where multiple DHS components operate.

## PREPAREDNESS

### **State Management of Homeland Security Grant Funds**

Homeland security grants encompass several different grant programs aimed at increasing the capability of state and local governments to respond to terrorist attacks in their communities. These grant funds are awarded by the Office of Grants and Training (OGT) based on a combination of current threat estimates, critical assets within the urban area, and population density. Our audit will focus on the states' (1) methodology for identifying high-threat, high density urban areas; (2) assessment of threats, vulnerabilities, capabilities, and prioritized needs; (3) funding allocation methodology; (4) expenditure of grant funds on high priority requirements; and (5) measurement of improvements as a result of the grants and identification of best practices. This effort is part of our continuing effort to evaluate state management of homeland security funds. We have already completed or started work in nine states and will begin reviews in six additional states.

**Audit Objective:** Determine to what extent states are effectively and efficiently managing and expending homeland security grant funds to achieve established goals.

### **Grants Financial Management Oversight and Accountability**

OGT has stewardship for homeland security grants awarded to states, local governments, Indian tribal governments, and United States territories. In FY 2006, grants awarded by OGT exceeded \$3.3 billion and included preparedness grant programs such as the Homeland Security Grant Program, Urban Areas Security Initiative, Law Enforcement Terrorism Prevention Program, Metropolitan Medical Response System, and Citizen Corps Program. Past and ongoing OIG audits of the states' and U.S. territories' management of these grant programs have shown that OGT may lack sufficient oversight of grant expenditures and overall financial management by the grantees.

Department of Homeland Security

**Audit Objective:** Determine to what extent OGT is effectively monitoring grant expenditures and grantee adherence to the financial terms and conditions of the grant awards.

**Grants Performance Oversight**

In FY 2006, preparedness grants awarded by OGT to state and local governments, and United States territories exceeded \$3.3 billion. The grants were awarded to provide grant recipients the resources that are critical to building and sustaining capabilities to implement state and urban area homeland security strategies for increased preparedness. Past and ongoing OIG audits of the states' and United States territories' management of these grant programs have shown problems with the states strategies for using homeland security funds to increase preparedness. As a result, it is uncertain whether state and local governments, and United States territories are better prepared.

**Audit Objective:** Determine to what extent OGT is effectively monitoring preparedness of state and local governments, and United States territories, and the impact of homeland security grant funds.

**National Cyber Security Review**

The Director, National Cyber Security Division (NCSA), formerly part of the DHS Information Analysis and Infrastructure Protection directorate, has been elevated to Assistant Secretary for Cyber & Telecommunications, reporting directly to the Secretary. In its former role, NCSA was charged with coordinating the implementation of the National Strategy to Secure Cyberspace and served as the single National point of contact for the public and private sector regarding cyber security issues. NCSA was also charged with identifying, analyzing, and reducing cyber threats and vulnerabilities; disseminating threat warning information; coordinating incident response; and providing technical assistance in continuity of operations and recovery planning. In carrying out its role, NCSA was to work closely with industry in solving the critical and complex task of protecting the nation's cyber infrastructure.

**Audit Objective:** Determine whether DHS's National Cyber Security Division has managed the implementation of the National Strategy to Secure Cyberspace and DHS's cyber security program.

**The Office of Infrastructure Protection's Resource Requirements ([Congressional](#))**

The Office of Infrastructure Protection (IP) identifies and assesses current and future threats to the Nation's physical and informational infrastructure, issuing timely warnings to prevent damage to the infrastructure that supports our community and economic life. The Preparedness Directorate budgeted \$619,244,000 and 445 FTEs for Infrastructure Protection and Information Security in FY 2006, and requested FY 2007 budget as \$549,140,000 and 445 FTEs.



**Inspection Objectives:** Determine whether (1) the physical space and number of full-time permanent staff assigned to the Infrastructure Protection office is adequate to meet its broad responsibilities, and (2) what particular challenges IP faces in the use of contractors or temporary employees.

### **Administering Lessons Learned From Exercises (Congressional)**

DHS's April 2005 Top Officials Three Exercise (TOPOFF 3) was a congressionally mandated exercise designed to strengthen the Nation's capacity to prevent, prepare for, respond to, and recover from large-scale terrorist attacks involving weapons of mass destruction. TOPOFF 3 was the most comprehensive terrorism response exercise ever conducted in the United States. It provided a realistic test of the Nation's homeland security system. It brought top officials together to identify and address problems, share knowledge, and develop skills for managing complex terrorist events. The exercise extended the learning derived from earlier TOPOFF exercises. Given that these exercises are costly and time-consuming, as well as the primary preparatory mechanism prior to a real disaster, a failure to clearly identify lessons learned and provide corrective plans to address deficiencies for local, state, and federal response entities can lead to confusion, chaos, and ultimately compound tragedy if a real disaster should occur.

**Inspection Objectives:** Determine, in the aftermath of large TOPOFF exercises, (1) how the DHS addresses the remedial needs where deficiencies have been determined to exist, and (2) the process used to determine, formulate, and distribute lessons learned and address remedial needs.

### **Review of Vulnerability Assessment Methodologies**

There are a wide variety of vulnerability assessment methodologies in use by public and private entities. DHS's Office of Infrastructure Protection is attempting to establish vulnerability assessment output standards; assist entities in evaluating, modifying, or developing vulnerability assessment methodologies; and, participate in vulnerability assessments of critical sites, operational systems, states, and regions. IP is developing a suite of tools known as Risk Analysis and Management for Critical Asset Protection (RAMCAP), which will allow for comparability of consequence, vulnerability, threat, and risk measurements. RAMCAP is intended to provide asset owners and operators a means to calculate the potential consequences and vulnerability to an attack using a common and consistent system of measurements, or the means to convert the results from prior assessments performed with select approved methodologies into results that can be compared to those obtained using RAMCAP methodologies.

**Inspection Objectives:** Determine (1) how DHS is encouraging the use of basic vulnerability assessment standards; (2) the effectiveness of DHS's use of relative risk values to allocate funds; and (3) how risk assessments are used in developing overarching departmental priorities.

### **Review of Petroleum and Natural Gas Sub-sectors**

DHS is responsible for leading, integrating, and coordinating efforts to protect critical infrastructure sectors, eight of which are primarily overseen by other federal departments. The petroleum sub-sector is a key component of the energy sector, and damage to associated infrastructure could pose a significant public safety hazard and harm the economy. Similarly, damage to the natural gas sub-sector also poses public safety and economic risks, as natural gas meets one-fifth of the nation's electrical needs.

***Inspection Objective:*** Determine the scope and effectiveness of DHS efforts to support the Department of Energy's protection of the petroleum and natural gas sub-sectors.

### **Use of Critical Infrastructure Data for Programmatic Analysis**

The National Infrastructure Protection Plan envisions a comprehensive, national inventory of assets, known as the National Asset Database (NADB), to support its risk management framework. A maturing NADB is essential to the development of a comprehensive picture of the Nation's critical infrastructure and key resources as well as management and resource allocation decision-making. In June 2006, we issued a report, *Progress in Developing the National Asset Database*, which contained four recommendations to improve the development and quality of the NADB. However, that review did not fully assess the extent that the NADB is used to inform programmatic analyses.

***Inspection Objective:*** Determine the extent that DHS is using the NADB to support its risk management framework.

## ***Carryover Projects from FY 2006***

### **The Effectiveness of the State of New York's Urban Area Security Initiative Grant Program**

In FY2006, the Urban Area Security Initiative (UASI) funding was significantly reduced to \$711 million, was bundled with similar grants, and was part of the total \$1.6 billion Homeland Security Grant Program. Grant requirements remained essentially the same from year to year, except for costs relating to certain operational activities and time limits set to states for the obligation of funds to local units. The OGT determined funding using a combination of current threat estimates, critical assets within the urban area, and population density. Our audit will focus on the State of New York's (1) methodology for identifying high-threat, high density urban areas, (2) assessment of threats, vulnerabilities, capabilities, and prioritized needs, (3) funding allocation methodology, (4) expenditure of grant funds on high priority requirements, and (5) measurement of improvements as a result of the grants and identification of best practices.

**Audit Objective:** Determine whether New York effectively and efficiently implemented the UASI Grant Program, achieved the goals of the program, and spent funds according to grant requirements.

### **States' Management of First Responder Grants Program (Seven Audits)**

OGT (formerly the Office for Domestic Preparedness) is responsible for enhancing the capabilities of state and local jurisdictions to respond to, and mitigate the consequences of, incidents of domestic terrorism. To meet this responsibility, OGT 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 incidents involving weapons of mass destructions, and planning and administering grants. Between 2003 through 2005, Congress appropriated approximately \$5.2 billion for first responder grants. The program has received substantial congressional and public interest in how states have been and 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 process, and vendor backlogs. In addition, the audits completed in 2006 that reported that states’ efforts for managing grant awards need improvement.

**Audit Objective:** Determine whether Florida, Pennsylvania, Ohio, Michigan, New Jersey, Georgia, and West Virginia are effectively and efficiently implementing the First Responder Grant Program, achieving the goals of the program, and spending funds according to grant requirements.

### **Assistance to Firefighters Grant Program**

The Assistance to Firefighters Grant Program (AFGP), authorized by the Federal Fire Protection and Control Act of 1974, as amended, awards 1-year grants directly to fire departments of a state to enhance their abilities with respect to fire and fire-related hazards. The primary goal is to provide assistance to meet fire departments’ firefighting needs. Management of the AFGP falls under the OGT. FY 2003 AFGP grant applications totaled 20,063 and requested grant awards totaling nearly \$2.5 billion. OGT, through a determination of eligibility and competitive evaluation, awarded 8,745 grants in FY 2003 with award amounts totaling \$705.2 million. Three OIG contractors will conduct ten grant expenditure audits each at rural, suburban, and urban fire departments in three states. Those audits will focus on the AFGP’s Firefighting Vehicles Acquisition Program and the Fire Operations and Firefighter Safety Program. We will summarize the results of the ten audits conducted in each state in three separate reports to OGT.

**Audit Objective:** Determine whether rural, suburban, and urban fire departments (grant recipients) in California, Illinois, and New York properly accounted for and used AFGP funds in compliance with federal requirements and the grant program guidance.

### **Management of the State of Homeland Security Grant Program by the State of Colorado**

OGT requested that we perform an audit of the State of Colorado's Homeland Security Grant Program. In its letter, the Office of Grants and Training noted that a 2005 Colorado State Auditor's Performance Audit of the program and monitoring visits by both program and financial officials identified a number of pervasive and serious weaknesses with the state's management of the program. Taken as a whole, program management weaknesses indicate the potential for a severe breakdown of internal controls related to financial management and reporting, grants management, and monitoring of the state's sub-grantees, and strategic management and equitable distribution of resources.

**Audit Objective:** Determine whether the State of Colorado expended its State Homeland Security Grant Program funds according to federal laws, regulations, and the applicable terms and conditions of the grant award agreement.

### **Review of the National Biosurveillance Integration System**

The Office of Preparedness serves as a lead agency in the development and operation of the National Biosurveillance Integration System (NBIS). The purpose of this system is to detect biological and chemical attacks, and coordinate the real-time integration of biosurveillance data with threat information and recommended responses. This function is aligned with the DHS strategic goal of awareness, which includes identifying and understanding threats, assessing vulnerabilities, determining potential impacts, and disseminating timely information to our homeland security partners and the public.

The DHS Medical Officer will ensure a coordinated and unified approach to medical readiness by providing data-driven, scientifically based policy and advice to advocate public health needs. NBIS officials forecast that 20 percent of agencies representing the U.S. health community will be sharing timely information through the system in FY07, in support of the DHS Medical Officer's role.

**Audit Objectives:** Our objectives are to determine whether NBIS meets user requirements in support of The Strategy for Pandemic Influenza, and assess the extent to which NBIS complies with information security and privacy standards and policies.

### **Assessment of Highway Watch Program**

Every day up to 3.2 million tractor-trailers use U.S. highways. To leverage the skills of these "eyes and ears" along this vast and open transportation network, the Office of Domestic Preparedness is administering a cooperative agreement with the American Trucking Association to expand the Highway Watch® program to promote security awareness and information sharing among all segments of the commercial motor carriers and transportation community. Between FY2003 and FY2005, the Trucking Security Grant Program provided \$46 million to train the Nation's transportation community to recognize

potential highway safety hazards, and to detect security threats and avoid becoming a target for terrorist activity. Trained Highway Watch members make their reports to the Highway Watch Call Center, which routes the call to the appropriate law enforcement authorities. Security-related information is forwarded to the Highway Information Sharing and Analysis Center where it is processed, analyzed, and shared with government intelligence officials and other law enforcement agencies.

***Inspection Objectives:*** Determine whether the roles of responsibilities of the various entities involved in the grant program and Highway Watch are clearly defined and whether the grant program is fulfilling its mission of enhancing security on our Nation's highways.

### **Equipment Eligibility and Identification Under the Buffer Zone Protection Plan**

In FY 2005, DHS announced the availability of \$91.3 million in grant funding to protect and secure areas surrounding critical infrastructure and key resource sites such as chemical facilities, dams, and nuclear plants across the country. Through its Buffer Zone Protection Plan (BZPP), DHS is providing funding to states to purchase equipment that will extend the zone of protection beyond the gates of these critical facilities. The approach provides federal, state, local officials, and first responders with the necessary tools and resources to protect their community assets. Initial BZPP assets were selected subjectively by DHS.

***Inspection Objectives:*** Determine (1) the adequacy of process used to identify BZPP assets and eligibility criteria for BZPP investments; (2) the utility of BZPP's equipment purchasing plans; (3) whether equipment purchases are unique to this program and the extent that they are available through other programs such as the State Homeland Security Grants, the Urban Area Security Initiative, and first responder grant programs; (4) the extent that purchases are clearly designed to reduce vulnerabilities in areas surrounding critical infrastructure and key resources; and (5) whether DHS has modified its methodology for selecting future BZPP sites.

## SCIENCE AND TECHNOLOGY

### **Review of the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement Program (*Mandatory*)**

The Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) program is designed to extract relationships and correlations from large amounts of data to produce actionable intelligence on terrorists. A prototype is currently available to analysts in Intelligence and Analysis using departmental and other data, including some on U.S. citizens. The conferees for the 2007 DHS Appropriations Act understand that up to \$40,000,000 has been obligated for ADVISE. The ADVISE program plan, total costs, and privacy impacts are unclear and therefore the conferees directed us to

Department of Homeland Security

conduct a comprehensive program review and report within nine months of enactment of this Act.

**Review Objectives:** Determine the effectiveness of DHS' ADVISE program by evaluating (1) strategies, policies, and procedures for conducting data mining to produce actionable intelligence on terrorists; (2) systems and activities to determine and understand potential threats to homeland security using data mining techniques; and (3) communication and coordination with information security partners and the public to help prepare for and counter the potential threats identified.

**Plum Island Animal Disease Center**

The Plum Island Animal Disease Center is responsible for research and diagnosis to protect United States animal industries and exports against catastrophic economic losses caused by foreign animal disease agents accidentally or deliberately introduced into the United States.

In June 2003, the land, buildings, and other facilities of the Plum Island Animal Disease Center were transferred to DHS. The DHS is responsible for the safety and security of the center, but the facility is staffed and operated by USDA personnel. Plum Island is located off the northeastern tip of New York's Long Island.

**Audit Objective:** Determine if Science and Technology (S&T) has established adequate physical and logical security controls for the sensitive systems and data housed in the Plum Island Animal Disease Center.

**Review of the Homeland Security Advanced Research Projects Agency's Efforts to Support Research and Development for Screening Technologies**

TSA's passenger and check-baggage screening efforts must detect and deter the potential explosives, chemical/biological weapons, nuclear devices, and other weapons in transit. To address needs like this, the Homeland Security Advanced Research Projects Agency (HSARPA) was established to provide research, development, and demonstration in cooperation with the end users, private sector, university researchers through the Centers of Excellence, and the Homeland Security and national and federal laboratories. With technology solutions, such as biometrics, portal, wireless, and detection technologies, TSA will be able to improve human performance of airport screeners and overall effectiveness of screening operations.

**Audit Objectives:** Determine the adequacy of the planning and management of HSARPA's efforts for supporting aviation screening operations; how user requirements are identified; and, what challenges HSARPA faces in improving quality and delivery of services.



---

**A Review of the Homeland Security Policy Institute ([Congressional](#))**

The Homeland Security Policy Institute (HSPI) draws on the expertise of its partners from the academic, nonprofit, policy, and private sectors for a common goal of better preparing the Nation for the threat of terrorism. HSPI frames the debate, discusses policy implications and alternatives, and recommends solutions to issues facing America's homeland security policymakers. By linking academicians and scientists to decision-makers at all levels of government, the private sector and the communities we live in, HSPI is working to build a bridge between theory and practice in the homeland security arena.

***Inspection Objectives:*** Determine (1) the extent of the utilization of the HSPI by DHS components; (2) the criteria for selecting partners; and, (3) how recommendations that address emerging security issues are disseminated to key policymakers.

**Homeland Security Advanced Research Projects Agency: Funding Research Projects ([Congressional](#))**

The HSARPA manages a broad portfolio of solicitations and proposals for the development of homeland security technology. HSARPA performs this function in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers, and universities. HSARPA invests in programs offering the potential for revolutionary changes in technologies that promote homeland security and accelerates the prototyping and deployment of technologies intended to reduce homeland vulnerabilities.

***Inspection Objectives:*** Determine (1) the process HSARPA uses to identify, prioritize, and fund research projects relevant to detection, prevention, and recovery from homeland security threats, particularly acts of terrorism; (2) how HSARPA monitors research projects; and, (3) the effectiveness of the S&T Directorate's approach to working with the Department of Defense and adapting military technologies for homeland defense.

**Organizational Structure, Programs, and Human Capital Needs ([Congressional](#))**

The Mission of the S&T Directorate is to protect the homeland by providing federal and local officials with state-of-the-art technology and other resources. The Directorate fulfills its mission through strategic objectives to develop and deploy state-of-the-art, high-performance, low-operating-cost systems to prevent, detect, and mitigate the consequences of chemical, biological, radiological, nuclear, and explosive attacks; develop equipment, protocols, and training procedures for response to and recovery from chemical, biological, radiological, nuclear, and explosive attacks; enhance the technical capabilities of DHS's operational elements and other federal, state, local, and tribal agencies to fulfill their homeland security-related missions; develop methods and capabilities to test and assess threats and vulnerabilities, and prevent technology surprise and anticipate emerging threats; and, develop technical standards and establish certified laboratories to evaluate homeland

Department of Homeland Security

security and emergency responder technologies. Scientists, technology experts from a variety of disciplines, and researchers are just a few of the types of staff S&T requires to execute its mission successfully.

**Inspection Objectives:** Determine (1) S&T's initiatives to attract and retain competent employees; (2) how employees' effectiveness is evaluated; and, (3) the turnover rates at all levels of the Directorate by component and compare those statistics with other research, development, test, and evaluation organizations.

**A Review of the Science and Technology Directorate's Research, Development, and Funding Priorities (Congressional)**

The S&T Directorate fulfills its mission by researching, developing, and then funding projects designed to create and deploy state-of-the-art, high-performance, low-operating-cost systems. The systems are designed to prevent, detect, and mitigate the consequences of chemical, biological, radiological, nuclear, and explosive attacks, and to develop equipment, protocols, and training procedures for response to and recovery from chemical, biological, radiological, nuclear, and explosive attacks. The potential threats against the United States are many and varied. S&T must have a strategic plan to develop the appropriate technologies at the appropriate time.

**Inspection Objectives:** Determine (1) the process S&T uses to set its research and development priorities and investments; (2) the decision-making process S&T uses to balance short term and long term research; (3) S&T's methodology for distributing funds for research and development to the national laboratories, academia, and the private sector; and, (4) how conflicts of interest in the decision-making process are resolved and documented.

**Research and Development in Aviation (Congressional)**

S&T's Office of Plans, Programs, and Requirements (PPR) partners with operational end-users to identify requirements, create strategic initiatives to address these requirements, prioritize investments, and ensure both short-term and long-term goals are met in accordance with national policies. Under its border and transportation portfolio, PPR focuses on preventing the entry of terrorists and instruments of terrorism while ensuring an efficient flow of lawful traffic and commerce.

**Inspection Objective:** Determine (1) what challenges S&T has faced in administering aviation research and development programs after those responsibilities were transferred from TSA this fiscal year, and (2) the extent S&T has coordinated with TSA to ensure a smooth transition.



## *Carryover Projects from FY 2006*

### **BioWatch Program**

The mission of the BioWatch Program is to provide 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, 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 Centers for Disease Control 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.

***Audit Objective:*** Determine to what extent BioWatch program management have implemented proper controls for coordinating responsibilities and funding with its partner agencies.

### **Support Anti-terrorism By Fostering Effective Technologies Act**

In 2002, Congress enacted the Support Anti-terrorism By Fostering Effective Technologies Act (SAFETY Act) to encourage the development of new antiterrorism technologies. The Act called for a new system of risk and liability management for manufacturers, specifically creating liability limitations for claims arising out of, relating to, or resulting from an act of terrorism. If a manufacturer implements a SAFETY-approved antiterrorism technology that ultimately fails, the Act provides protection against severe financial and legal consequence. The Undersecretary of S&T currently manages the SAFETY program.

***Inspection Objectives:*** Determine the efficacy of the SAFETY Program, i.e., (1) the complete application process, both pre- and full-process, for participation in the SAFETY program; (2) the technologies currently approved and implemented under the Act; (3) the analytical methods—qualitative and/or quantitative—executed in determining liability caps; and (4) the coordination between the S&T directorate and other DHS departments in determining what technologies are needed in the field.

## TRANSPORTATION SECURITY ADMINISTRATION

### **Airport Passenger and Baggage Screening Penetration**

The Aviation and Transportation Security Act requires the Transportation Security Administration (TSA) to screen or inspect all passengers, goods, and property before entry into the sterile areas of the airport. Ensuring that passengers and their baggage are adequately screened reduces the opportunity for terrorists to create harm in the air traffic environment. Due to the recent London terrorist threat of liquid explosives being introduced into the sterile area, we will focus on TSA's policies, procedures, training, and equipment to prevent these threat items from entering the sterile areas of airports and the checked baggage system.

***Audit Objectives:*** Determine to what extent TSA's policies, procedures, training, equipment, and supervision ensure that screener performance prevents threat items from entry into the sterile area and the checked baggage systems of the nations airports.

### **Transportation Security Administration's On-Screen Alarm Resolution Protocol**

TSA implemented the On-Screen Alarm Resolution Protocol in May 2004. This process allows TSA Screening Officers (TSOs) to resolve alarms from checked bags using the image of the bag contents on the screen of the Explosives Detection System machine. In this process, the TSO determines if an alarm bag contains an (1) obvious threat (2) requires further inspection (a suspect bag) or (3) is clear for transport onto the aircraft. The protocol is designed to expedite checked baggage screening and to develop TSO proficiency in screening images to detect improvised explosive devices and other prohibited items in checked baggage. It is critical that procedures used by the TSO are not modified to expedite baggage movement during peak hours or other time-sensitive operations. In such instances the security process would be compromised and vulnerable to terrorist acts.

***Audit Objective:*** Determine whether TSA's use of the protocol has enhanced the TSO's ability to detect threat items and improved the efficiency of the checked baggage screening process.

### **New Technologies to Screen Passengers and Their Property**

Our office has conducted two audits of screeners' ability to detect threat items on passengers and in their carry-on and checked baggage. We recommended that TSA make better use of technology to improve screeners' ability to detect and prevent prohibited items from being carried on board aircraft. In its official response to our report, TSA agreed with our conclusion that significant improvements in screener performance will only be possible with the introduction of new technology. TSA has several pilot programs at airports

nationwide, such as the explosive trace portal, backscatter systems, and the explosive detection document scanner.

**Audit Objectives:** Determine the status of TSA's evaluation, deployment, and testing of new screening technologies.

### **Transportation Security Administration IT Management**

Within DHS, TSA protects the nation's transportation systems to ensure freedom of movement for people and commerce. In addition to the administrative and other systems it needs to manage its day-to-day operations, TSA has begun implementing a number of technical solutions and high-profile initiatives to better support its transportation security mission.

**Audit Objectives:** Determine the effectiveness of the TSA's efforts to manage the research, acquisition, and implementation of technology to ensure safe and effective movement of people and commerce.

### **The Transportation Security Administration's use of the National Screening Force (Congressional)**

In October 2003, TSA established the National Screening Force (NSF). The NSF consists of full-time passenger and baggage screeners who have a home airport, but have volunteered to travel to other airports to provide screening support during emergencies, seasonal demands, or under other special circumstances that require a greater number of screeners than are regularly available. There are concerns that the TSA is heavily reliant on the NSF in ways not intended and at great expense to the federal government.

**Inspection Objectives:** Determine (1) when, where, and why the NSF has been deployed, (2) the expenses incurred related to maintenance and deployment of the NSF including lodging, travel, and per diem costs, (3) the overtime attributed to the NSF; and, (4) the adequacy of TSA's standard operating procedures for the NSF.

### **Review of Efforts to Enhance Transit and Passenger Rail Security**

Recent bombings of commuter and subway trains in Europe and India attest to the vulnerability of passenger rail systems to terrorist attack. Every day passenger rail systems in the United States carry nearly five times as many passengers as air carriers. DHS has taken several steps to manage risk and strengthen our nation's rail and transit systems. DHS has provided \$374.7 million to 60 different commuter systems; has trained and deployed Security Enhancement Teams, canine teams, and Mass Transit Inspectors to high-risk areas; has developed new detection technologies; and, is performing security assessments of systems across the country. DHS and TSA have also developed additional plans to secure the Nation's commuter rail systems better.

**Inspection Objectives:** Determine (1) the effectiveness of measures taken to date to enhance security throughout the Nation's commuter rail systems, (2) TSA's current and future plans to enhance rail security and evaluate them, and (3) the effectiveness of TSA's coordination with the Office of Infrastructure Protection and the Office of Grants and Training pertaining to commuter rail security enhancement.

### ***Carryover Projects from FY 2006***

#### **TSA's Federal Employment Compensation Act Program**

The Federal Employees' Compensation Act (FECA) provides for wage loss compensation, medical care and survivors' benefits to three million federal and postal workers around the world for employment-related injuries and occupational diseases. Under FECA, Federal agencies are responsible for advising employees on their rights and responsibilities, completing and submitting claim forms to the Office of Workers' Compensation Program in a timely manner and continuing to pay injured employees who have experienced traumatic injuries. Agencies are also responsible for assisting employees in returning to work, challenging questionable claims, keeping in contact with the injured employee, managing compensation costs, and accommodating "light duty" work when able. The TSA has been criticized in the Congress and media for its rising and disproportionately high injury claims, primarily in its screener workforce. Fewer available screeners, reportedly, has resulted in high overtime costs, screening lanes being closed, missed training for screeners, and, potentially, putting security at risk.

**Audit Objectives:** Determine whether TSA is effectively managing the FECA program and taking steps to reduce the number of workplace injuries and lost workdays, and minimizing FECA-related compensation costs.

#### **TSA's Oversight of Air Cargo Security on Passenger Aircraft**

The Aviation and Transportation Security Act of 2001 requires the screening of all passengers and property, including cargo shipped on passenger aircraft. The amount of cargo transported on passenger aircraft is estimated to be about six billion pounds annually. TSA regulations require aircraft operators to inspect all cargo at the time of acceptance for visual signs of tampering, exposed wires, or leaks that may render the cargo unsafe to transport. TSA also requires air carriers to perform more in-depth screening on a certain percentage of cargo. An audit that we conducted in 2004 found physical inspections for screening cargo were ineffective because air carrier employees were not trained to identify explosives nor were they equipped with explosives screening equipment. Our recent work uncovered other deficiencies with cargo screening, including various interpretation and application of the exemption criteria by air carriers, and the lack of standardized training for personnel conducting screening activity, which might leave the air cargo system vulnerable to attack.

**Audit Objective:** Determine whether TSA provides adequate oversight of carriers' compliance with TSA's security programs related to the handling and screening of cargo shipped on passenger aircraft.

### **Implementation of Aviation Security Requirements at Foreign Airports**

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 airports.

**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.

### **Review of Allegations Regarding San Francisco International Airport**

TSA management requested that we review allegations that TSA officials at San Francisco International Airport (SFO) knowingly violated TSA policy and procedures in covering up security breaches at SFO, and whether TSA and officials of the contract screening company at SFO had compromised our covert security testing by broadcasting tester descriptions and methodologies to all screening areas.

**Audit Objective:** Determine whether TSA management at SFO complied with TSA policy and procedures for identifying and reporting security incidents and whether and to what extent covert security testing has been compromised at SFO.

### **Access to Secure Areas at Airports**

Controlling access to secure airport areas, where only authorized airport employees and contractors are allowed, is paramount to ensuring the safety of the flying public. Airports have improved security practices by requiring that only passengers with boarding passes be allowed entry to the security checkpoints. This requirement and others should reduce the opportunity for terrorist activity.

**Audit Objectives:** Determine whether the airline industry complied with federal aviation requirements to allow only authorized personnel access to secure airport areas, and review

Department of Homeland Security

the coordination and authorities of the federal security directors and other stakeholders at airports.

**TSA's Federal Flight Deck Officer Program**

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 pilots of air carriers who volunteer 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 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 requalification 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.

**Follow-up Review of TSA Employee Background Checks**

When TSA rapidly hired over 55,000 passenger and baggage screeners in 2002, it failed to conduct personnel security screening in a timely and thorough manner. In January 2004, we reported several causes for these personnel security weaknesses. The chief cause was an inadequate infrastructure for processing security checks. We issued 12 recommendations, nine of which were resolved and closed by August 2004. Since 2004, various reports to our office have indicated that TSA's personnel security screening continues to have problems with certain aspects of the screener background check process. This follow-up review will assess the effectiveness of TSA's corrective actions and examine issues that have come to our attention since the January 2004 report.

***Inspection Objectives:*** Determine (1) what position risk designations TSA has and what background checks TSA completes for each designation; (2) the extent to which TSA's current adjudication standards permit TSA to retain or hire staff with derogatory background checks; and (3) the effectiveness of TSA's management of the screening process, including staffing levels, use of contractors, and compliance with federal law.

**UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES****Consistent Application of the Citizenship and Immigration Service Adjudication Process**

The United States Citizenship and Immigration Service (USCIS) is responsible for administering the immigration and naturalization functions and establishing policies and priorities for immigration services. USCIS Adjudication Officers at regional centers interpret and apply laws and regulations regarding eligibility for immigration benefits such as naturalization. Adjudication Officers determine eligibility of the applicants for immigration and citizenship benefits, review motions for reconsideration, and make the final determination on cases. Inefficiencies in processing applications have resulted in a large backlog and thousands of Freedom of Information Act requests inquiring about the status of applications. These inefficiencies and fraud have been reported in prior audits, as well as the lack of automation.

***Audit Objective:*** Determine whether the USCIS properly controls adjudication processes to ensure consistent and equitable application of criteria and procedures, and the timely handling of applications.

**Review of Systems to Enable Alien Status Verification**

Since the Immigration Reform and Control Act passed in 1986, employers must view documentation that an applicant is legally in the United States before hiring that person. However, partly because of widespread document fraud, employers continue to employ aliens who are not legally authorized to work. ICE is beginning an employer outreach program called ICE Mutual Agreement between Government and Employers (IMAGE) to encourage self-policing and best hiring practices. USCIS offers related tools that provide independent verification of an alien's legal status: the Basic Pilot Employment Verification Program, whose use IMAGE requires, and the Systematic Alien Verification for Entitlements Program (SAVE) for government benefits and school administrators.

***Inspection Objectives:*** Determine (1) how well the USCIS programs are positioned to support interior enforcement efforts and employer sanctions; and (2) how USCIS manages SAVE and the Basic Pilot Program, ensures compliance with privacy and computer matching laws, provides secondary examination to verify initial "hits," and maintains database accuracy.



## ***Carryover Project from FY 2006***

### **U.S. Citizenship and Immigration Services Information Technology Modernization Follow-up**

In our September 2005 report, *USCIS Faces Challenges in Modernizing Information Technology* (OIG-05-41), we identified several challenges, such as an unfocused improvement approach, as well as DHS reorganization and new security requirements, that are hindering USCIS from achieving its IT modernization objectives and made recommendations for overcoming them. Progress in moving forward with IT modernization plans is critical, given that efficient and effective use of technology will be key to supporting the potentially dramatic increases in immigration benefits processing workloads that could result from recently proposed immigration reform legislation.

***Audit Objectives:*** Determine the adequacy of the progress made in USCIS's approach to improving IT to support immigration benefits processing.

## **UNITED STATES COAST GUARD**

### **Coast Guard Response Capabilities for High-Risk Vessels Entering U.S. Ports**

The USCG is responsible for identifying, detecting, tracking, boarding, inspecting, and escorting high interest vessels that may pose a substantial risk to U.S. ports due to the composition of a vessel's crew, passengers, and cargo. Approximately 8,000 vessels make over 62,000 port visits each year. As a result of The Maritime Transportation Security Act of 2002, the USCG has instituted strict reporting requirements for all vessels arriving and departing U.S. seaports, and has developed a decision-making matrix to target high interest vessels, cargoes, and crews. Designating and responding to high interest vessels requires a substantial commitment of personnel, equipment, and funding.

Local Sector Commanders designate high interest vessels based on the targeting matrix, which includes data from the Intelligence Coordination Centers and local field intelligence support teams. Commandant Instruction mandates that all high interest vessels be boarded. However, the manner in which these boardings are executed is the responsibility of the local Sector Commander. This audit is a follow-on to an audit initiated in June 2006 to assess USCG intelligence-based operations that collect, fuse, analyze, and disseminate intelligence regarding high interest vessels, cargoes, and crews. This audit will focus on the operational capabilities of the USCG to appropriately respond to designated high interest vessels, cargoes, and crews.



***Audit Objective:*** Determine the extent of the USCG's ability to board, inspect, escort, divert, and secure, as necessary, all high interest vessels before they enter a U.S. port, thereby mitigating or eliminating the risks and impacts of catastrophic consequences.

### **U.S. Coast Guard Mission Performance (*Mandatory*)**

The Homeland Security Act of 2002 directs our office to monitor the use of USCG assets on all USCG missions, with a particular emphasis on non-homeland security missions. Homeland security missions include illegal drug interdiction; undocumented migrant interdiction; other law enforcement; ports, waterways, and coastal security; and defense readiness. Non-homeland security missions consist of search and rescue, aids to navigation, ice operations, living marine resources, marine safety, and maritime environmental protection. In the past, emphasis on many of the non-homeland security missions may have been reduced during crisis situations such as the response efforts to Hurricane Katrina, which caused severe devastation and flooding to the Gulf Coast in August 2005.

***Audit Objective:*** Determine the USCG's utilization of assets during FY 2007 and compare the utilization to prior years.

### **Marine Accident Investigations (*Congressional*)**

The House Committee on Transportation and Infrastructure and the Senate Committee on Commerce, Science, and Transportation, requested that we determine the extent to which marine casualty investigations and reports result in information and recommendations that prevent similar casualties, minimize the effect of similar casualties, and maximize lives saved in similar casualties. The final report is due to Congress on June 30, 2007.

***Audit Objective:*** Determine the extent to which marine casualty investigations and reports result in information and recommendations that prevent and minimize similar casualties, and maximize lives saved.

### **Procurement, Testing, and Deployment of Vertical Take-off and Landing Unmanned Aerial Vehicles**

The Vertical Take-off and Landing Unmanned Aerial Vehicle (VUAV) is a short-range, shipboard deployable unmanned aircraft. The primary role of the VUAV system is to provide the USCG with the capability to survey, detect, classify, and identify targets of interest (TOI) that are operating beyond the visual range of the cutter or the range of its sensors. The VUAV's endurance and payload capability will allow the USCG to conduct short or long-range surveillance missions, classify and identify targets from the air, covertly track and monitor TOIs, and establish long-range voice communications. This asset will be used to support maritime homeland security missions, as well as search and rescue, illegal drug interdiction, marine environmental protection, and military preparedness. The VUAV will be deployed aboard the National Security Cutter as part of the maritime security cutter "force package." The revised Deepwater plan projects the

Department of Homeland Security

acquisition of 45 Bell Helicopter-Textron “Eagle Eye” tilt-rotor vertical takeoff-and-landing VUAVs. Delivery of the first production prototype and initial flight-testing are anticipated for fall 2008, with initial deployment expected in 2011.

Technical and contractual problems have hindered the VUAV program and delayed the implementation schedule. The VUAVs do not have the kind of detection and collision avoidance technology required to operate within the National Air Space, and would therefore be limited to fly outside of zones used by manned aircraft. In April 2006, a VUAV demonstrator built by Bell crashed after an unexpected loss of engine power while hovering. Also, the performance-based contract that is being used to procure the VUAVs can result in errors in “translation” between government needs and the requirements that are included in the contract, possibly resulting in additional costs and reduced capabilities.

**Audit Objective:** Determine to what extent USCG’s oversight role and decision-making authority was effective in ensuring VUAVs are completed on time and within budget and achieve established operational capabilities.

**Review of U.S. Coast Guard Enterprise Architecture Implementation Process**

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. 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. We will evaluate how the USCG’s enterprise architecture framework maps to the DHS enterprise architecture framework. The audit will identify any voids in the transition planning from the USCG’s legacy (C4ISR) “As Is” to the DHS “To Be” enterprise architecture framework.

**Audit Objectives:** To determine the level of compliance with established federal guidance and DHS enterprise architecture policies and procedures, and to determine whether the USCG has aligned their strategic plans and individual business priorities within an appropriate enterprise architecture framework.

***Carryover Projects from FY 2006***

**Maintenance, Rehabilitation, and Upgrading of Shore Facilities in Support of U.S. Coast Guard Missions**

The USCG occupies over 33 million square feet of building space, located at more than 1,600 sites, and owns 65,000 acres. The USCG estimates it has more than 21,000 buildings and structures. The estimated replacement value for these shore side assets is \$7.5 billion. Based on this value, and recent and projected shore infrastructure acquisition, construction, and improvement (AC&I) funding levels, USCG’s re-capitalization rate hovers around 200

years. To put this into perspective, the Department of Defense's target recapitalization rate for its facilities is 67 years.

Twice each year the USCG updates its Shore Facilities Requirements List, which is the planning document used to "ensure that planning, development, and execution of shore construction provides maximum benefit from USCG's limited AC&I resources." Projects on the list are divided into three categories: major AC&I (projects valued at over \$1.5M), minor AC&I (projects valued between \$200k and \$1.5M), and housing AC&I (any value).

The typical AC&I project requires five to seven years to complete: three years to plan, two years to obtain funding and complete the design, and another one to two years to construct. Under their respective Maintenance and Logistics Command, USCG's Facilities Design and Construction Centers Atlantic Area and Pacific Area typically manage the larger AC&I projects. USCG Civil Engineering Units handle some minor AC&I projects, as well as nonrecurring maintenance projects.

***Audit Objective:*** To determine the extent to which the USCG is adequately maintaining and rehabilitating shore facilities in support of USCG missions. The audit will also determine the extent to which the condition of these shore facilities is adversely impacting asset readiness, asset service life, and overall mission performance.

### **Maritime Intelligence Operations Involving High-Risk Vessels Entering U.S. Ports**

The USCG is responsible for identifying, detecting, tracking, boarding, inspecting, and escorting high interest vessels that may pose a substantial risk to U.S. ports due to the composition of a vessel's crew, passengers, or cargo. More than 8,000 vessels make 51,000 port visits each year. As a result of The Maritime Transportation Security Act of 2002, the USCG has instituted strict reporting requirements for all vessels arriving and departing U.S. seaports, and has developed a sophisticated decision-making matrix to target high interest vessels, cargoes, and crews. Responding to high interest vessels requires a substantial commitment of personnel, equipment, and funding.

Local sector commanders designate high interest vessels based on the targeting matrix, which includes data from the Intelligence Coordination Center and the local field intelligence support teams. For example, analysts at the Intelligence Coordination Center conduct automated analyses that match crew lists, provided under 96-hour notice of arrival regulations, with law enforcement (criminal and immigration) and anti-terrorism databases to determine if there is a threat. Commandant instruction mandates that all high interest vessels be boarded. However, the manner in which these boardings are executed is the responsibility of the local sector commander.

***Audit Objectives:*** Determine the extent of the USCG's ability, through intelligence-based operations, to collect, fuse, analyze, and disseminate intelligence regarding high interest vessels, cargoes, and crews attempting to enter U.S. seaports.

### **Acquisition of the National Security Cutter, USCG Deepwater Program**

The Maritime Security Cutter, Large is the first major surface asset to be produced under the IDS program. It will be the largest and most technically advanced of the three new classes of cutters designed and built by ICGS, the partnership between Northrop Grumman and Lockheed Martin. Not a direct one-for-one asset replacement, the eight planned cutters will replace the 12 existing 378-foot High Endurance Cutters (WHEC), which entered the USCG inventory in the 1960s under the Deepwater concept of a “system-of-systems.” USCG’s legacy Deepwater assets, the WHECs and medium endurance cutters, exhibit rapidly decreasing operational readiness and associated increases in maintenance costs due to the age of the fleet and increased operations tempo.

From 1999 to 2004, the number of unscheduled maintenance days has increased 400 percent from 85 to 358. The limited performance capabilities of the WHECs severely impact USCG’s ability to meet current mission requirements, especially with its increased role in homeland security operations. The eight cutters will be delivered over a 10-year period with the first scheduled for delivery in May 2007. The lead national security cutter is projected to cost \$480M under a cost-plus-incentive contract; the cost of the follow-on cutters is estimated to be \$350M per ship under a fixed-price contract. Certain design elements of the national security cutter have yet to be finalized. USCG has identified some of these design elements as top program risks and is working to mitigate and eliminate them.

***Audit Objectives:*** Determine to what extent the oversight roles and decision-making authorities held by ICGS and USCG during the design and construction of the national security cutters are effective in ensuring (1) the structural integrity of the vessel, (2) the vessel is completed on time and within budget, and (3) the vessel achieves established operational capabilities.

### **Safety and Security Vulnerabilities Associated with the 123-foot Maritime Patrol Boat and the Short Range Prosecutor**

In February 2006, we received a hotline complaint that USCG’s 123-foot Island Class Patrol Boats (WPBs) contain safety and security vulnerabilities. The complaint asserts that the vulnerabilities were incorporated during the conversion of the 110-foot WPB to the 123-foot WPB. The complaint alleges that the contractor failed to comply with the design standards established for the design and integration of electronic equipment into the 123-foot WPB.

***Review Objective:*** Determine whether the allegations concerning the 123-foot WPB conversion are valid.

## UNITED STATES SECRET SERVICE

### Review of the Electronic Crimes Task Forces

With the passage of the USA PATRIOT Act in October 2001, the United States Secret Service (USSS) was authorized to establish a nationwide network of electronic crimes task forces, based on the agency's New York City model. Recently, the USSS announced nine new task forces in addition to existing operations in 15 U.S. cities. For FY 2006, the USSS received \$39.6 million to support investigations of electronic crimes.

**Inspection Objective:** Determine the progress the USSS has made in stemming electronic crime, given the funding and creation of the task forces.

## MULTI-COMPONENTS

### DHS Disaster Communications

After Hurricane Katrina struck the Gulf Coast in September 2005, questions were raised as to the adequacy of telecommunications among law enforcement and emergency personnel at all levels of government. Problems with telecommunications operability, as well as interoperability within and among jurisdictions hindered rescue and response effort at all levels. Massive destruction to the telecommunications infrastructure disclosed severe gaps and weaknesses in network planning, protocols, and standards. DHS can benefit from examining and potentially applying the successful disaster telecommunications strategies and technologies of other government and industry organizations to better prepare for future disaster coordination.

**Audit Objectives:** Identify and research leading practices for effective disaster telecommunications, and examine the potential to apply these approaches and technology for use in DHS.

### DHS Counter-Terrorist Information Sharing for Critical Infrastructure Protection

There is concern about whether the federal government is effectively communicating and sharing information with private industry to help ensure rapid and effective response to failures of, or potential attacks on, critical sector operations. Sector disruptions or denial of service for an extended period of time can cause a dangerous ripple effect of death and destruction across the Nation's infrastructure. For example, as highlighted by the Thursday, 8/14/03, blackouts in the northeastern United States and Canada, and the wide-spread power outages pursuant to Hurricane Isabel the following month, massive regional electrical failures may be a potential goal of our terrorist enemies, raising concerns about the vulnerability of U.S. public sector operations to possible enemy attack. DHS is

Department of Homeland Security

responsible for analyzing, prioritizing, and sharing information with sector organizations to help safeguard or address potential disruptions to critical sector operations.

***Audit Objectives:*** Determine the effectiveness of DHS's strategies and tools for communicating and collaborating with private industry to ensure rapid response to potential failures of or attacks on critical sector operations.

**Relationship Between the Preparedness Directorate and the FEMA Directorate (Congressional)**

The Preparedness Directorate works with state, local, and private sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest, thereby safeguarding our borders, seaports, bridges and highways, and critical information systems. The FEMA Directorate prepares the nation for hazards, manages Federal response and recovery efforts following any national incident, and administers the NFIP.

***Inspection Objectives:*** Determine how effectively these directorates coordinate challenges with respect to overlapping or shared responsibilities.

**Operational Structure and Coordination of Overseas Missions and Operations**

DHS's Office of International Affairs, within the Office of Policy, does not have supervisory authority over the individual components' myriad international programs. This review will examine DHS international activities on a component-by-component basis and evaluate the quality of management direction and internal control exercised by the component.

***Inspection Objectives:*** Determine each component's international mission and operations, including what operations are conducted overseas, where the component has personnel stationed overseas, and the component's plans for expanding overseas operations. Evaluate the processes used by the component to select, train, and deploy its overseas employees. Evaluate the sufficiency of the human, financial and capital resources in each country to effectively accomplish the component's program goals. Assess the effectiveness of the component's management oversight and internal controls of its international programs and personnel.

**Intelligence Oversight & Quarterly Reporting (Mandatory)**

Executive Order 12333 describes the limited specific cases when a member of the Intelligence Community may collect, retain, or disseminate information on U.S. persons. Another Executive Order, 12863 requires the OIG to report, on a routine basis, how well the department has complied with 12333, and whether any violations have occurred. This report is submitted quarterly to the Intelligence Oversight Board, a standing committee of the President's Foreign Intelligence Oversight Board.



**Inspection Objectives:** A letter report generated from United States Coast Guard and Office of Intelligence & Analysis input. These are the only two Intelligence Community members with DHS. The DHS IG signs the letter report and forwards it to DHS' General Counsel, who then countersigns the report before it is officially submitted to the Intelligence Oversight Board.

### **ICE and USCIS Processing of Benefit Fraud Referrals**

According to USCIS, ICE's benefits fraud unit declines to investigate about 70 percent of USCIS referrals, including 100 percent of single scope marriage fraud. Marriage fraud is a known tool for terrorists to embed in U.S. society. ICE's inability to pursue more USCIS leads has led USCIS to create its own fraud task forces and go out into the communities to develop cases, which may raise legal issues since USCIS has no enforcement authority.

**Inspection Objectives:** Examine how USCIS and ICE are defining and dividing the benefits fraud workload and determine the outcome of referrals; determine what law enforcement and administrative resources the components use for benefits fraud cases, including what role USCIS fraud task forces perform; and assess whether the amount of resources used for this mission match risks and ICE's enforcement strategy.

## ***Carryover Projects from FY 2006***

### **DHS Data Mining**

Data mining refers to the process of knowledge discovery, predictive modeling, and analytics. Data mining includes evolving technologies that assist in the discovery of patterns and relationships from vast quantities of data. It employs techniques from statistics, machine learning, database management, and visualization to aid the work of analysts, agents, and investigators and provides knowledge in a manner that aids and informs decision-makers. The Homeland Security Act authorizes DHS to use data mining tools and other advanced analytics to access, receive, and analyze information.

Our June 2006 report identified and described 12 systems and capabilities that DHS personnel use to perform data mining activities to support DHS' mission of counterterrorism. For DHS, in particular, improving current capabilities in data mining will aid DHS in targeting high-risk cargo for further examination, assisting analysts in evaluating whether a document is counterfeit, collecting tactical information related to suspicious activities, and detecting anomalies and relationships indicative of criminal activity.

**Audit Objectives:** Determine the adequacy of the level of management oversight over data-mining activities, and determine whether it complies with security and privacy requirements.



## **Review of DHS's Maritime Alien Interdiction Operations and Processing of Aliens Who Have Been Interdicted at Sea**

Thousands of people try to enter this country illegally every year using maritime routes, many via smuggling operations. Interdicting migrants at sea means they can be quickly returned to their countries of origin without the costly processes required if they successfully enter the United States, its territory, or its possessions.

The USCG, CBP, and CE are all responsible for interdiction of illegal aliens attempting to enter the United States by sea. The USCG conducts patrols and coordinates with other federal agencies and foreign countries to interdict undocumented migrants at sea. CBP and ICE also enforce and administer immigration and nationality laws in conjunction with the inspection of all persons seeking admission into the United States, and identify and counter drug-related criminal activity. CBP and ICE have small boats close to shore that may interdict migrants during their patrols. Any other agency that interdicts migrants at sea, such as the U.S. Navy, will turn them over to the USCG, which detains them until their disposition is determined by USCIS.

***Inspection Objectives:*** Determine (1) how DHS agencies interdict illegal aliens attempting to enter the United States by sea, (2) how DHS agencies coordinate interdiction efforts with other agencies, (3) how interdicted aliens are detained or repatriated, and (4) whether DHS is allocating the necessary resources to effectively complete their mission with regard to maritime interdiction.

### **DHS Intelligence Collection and Dissemination**

DHS is responsible for guarding our borders and preventing illegal aliens, narcotics, and other contraband from entering the country. Since September 11, 2001, securing our borders has taken on a new emphasis of preventing terrorists from entering the country. DHS must secure 95,000 miles of coastline and 7,000 miles of land border with limited resources. To maximize the effectiveness of those resources, DHS uses intelligence as a force multiplier. DHS must collect, analyze, and disseminate intelligence not only within its internal components, but also with agencies outside of DHS such as the Department of Defense, Department of Justice, and the intelligence community.

There are a number of offices within DHS component agencies that are involved with intelligence activities, such as the Transportation Security Intelligence Service, the CBP Office of Intelligence, the USCG Intelligence Coordination Center, the ICE Office of Intelligence, and the Office of Intelligence and Analysis.

***Inspection Objectives:*** Determine: (1) what intelligence activities exist within DHS; (2) the specific functions of each; (3) whether there are areas of redundancy and the potential for cost savings and improved operational effectiveness by consolidating some functions; and (4) whether there is a cohesive, DHS-wide structure for directing and providing oversight of the various intelligence activities.

---

**DHS Progress in Addressing Challenges in the Relationship Between CBP and ICE**

DHS has acknowledged that there are challenges in the relationship between CBP and ICE. DHS indicated that organizational changes contemplated as a result of the Secretary's Second Stage Review and initiatives undertaken under its Secure Border Initiative will resolve these challenges, and that it will develop performance metrics related to its objectives. In addition, our report on the possible merger of ICE and CBP contains recommendations for corrective action that we will monitor. To evaluate progress in these areas, we will review DHS's plans for implementing our recommendations, the Secure Border Initiative, and changes resulting from the Secretary's Second Stage Review.

***Inspection Objectives:*** Determine DHS progress in addressing difficulties in the relationship between CBP and ICE; in particular, the progress of DHS initiatives to improve: (1) coordination between apprehension and detention and removal operations; (2) coordination between interdiction and investigation operations; and (3) intelligence and information sharing.

## Appendix A OIG Headquarters and Field Office Contacts

**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](http://www.dhs.gov)**

### OIG Headquarters Senior Management Team

|                             |       |   |
|-----------------------------|-------|---|
| <b>Richard L. Skinner</b>   | ..... | <b>Inspector General</b>  |
| <b>James L. Taylor</b>      | ..... | <b>Deputy Inspector General</b>                                   |
| <b>Matt Jadacki</b>         | ..... | <b>Deputy Inspector General/Disaster<br/>Assistance Oversight</b> |
| <b>Richard N. Reback</b>    | ..... | <b>Counsel to the Inspector General</b>                           |
| <b>David M. Zavada</b>      | ..... | <b>Assistant Inspector General/Audits</b>                         |
| <b>Elizabeth Redman</b>     | ..... | <b>Assistant Inspector General/Investigations</b>                 |
| <b>Carlton I. Mann</b>      | ..... | <b>Acting Assistant Inspector<br/>General/Inspections</b>         |
| <b>Frank Deffer</b>         | ..... | <b>Assistant Inspector General/Information<br/>Technology</b>     |
| <b>Edward F. Cincinnati</b> | ..... | <b>Assistant Inspector General/Administration</b>                 |
| <b>Tamara Faulkner</b>      | ..... | <b>Congressional Liaison and Media Affairs</b>                    |
| <b>Denise S. Johnson</b>    | ..... | <b>Executive Assistant to the Inspector General</b>               |

**Appendix A**  
**OIG Headquarters/Field Office Contacts and Locations**  
**Locations of Audit Field Offices**

**Boston, MA**

10 Causeway Street  
Suite 465  
Boston, MA 02222  
(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

**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, Suite 470  
Kansas City, MO 64106  
(816) 329-3880 / Fax: (816) 329-3888

**Miami, FL**

3401 SW 160th Ave., Suite 320  
Miramar, FL 33027  
(954) 538-7842 / Fax: (954) 602-1034

**Philadelphia, PA**

Greentree Executive Campus  
5002 D Lincoln Drive West  
Marlton, NJ 08053-1521  
(856) 968-4907 / Fax (856) 968-4914

\*Scheduled to close by December 31, 2006.

**Appendix A**  
**OIG Headquarters/Field Office Contacts and Locations**  
**Locations of Investigative Field Offices**

**Atlanta, GA**

The Millennium in Midtown  
10 Tenth St., NE, Suite 750  
Atlanta, GA 30309  
(404) 832-6730 / Fax (404) 832-6646

**Baton Rouge, LA**

Louisiana State University  
402 Johnston Hall (Attn: DHS OIG-Inv)  
Baton Rouge, LA 70803  
(225) 334-4900 / Fax: (225) 334-4707

**Biloxi, MS**

FEMA/JFO  
2350 Beach Blvd. (Attn: OIG Inv)  
Biloxi, MS 39531  
(228) 385-4933 / Fax: (228) 385-7148

**Boston, MA**

10 Causeway Street, Suite 465  
Boston, MA 02222  
(617) 565-8705 / Fax (617) 565-8995

**Buffalo, NY**

130 S. Elmwood Ave., Room 501  
Buffalo, NY 14202  
(716) 551-4231 / Fax (716) 551-4238

**Chicago, IL**

55 W. Monroe St., Suite 1050  
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**

290 Town Center Dr., Suite 604  
Dearborn, MI 48126  
(313) 226-2163 / Fax (313) 226-6405

**El Centro, CA**

516 Industry Way, Suite B  
Imperial, CA 92251  
(760) 335-3900 / Fax (760) 335-3726

**El Paso, TX**

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

**Hattiesburg, MS**

6068 US Hwy 98 W, Suite 1258  
Hattiesburg, MS 39402-8881  
(601) 264-8220 / Fax: (601) 264-9088

## Appendix A

### OIG Headquarters/Field Office Contacts and Locations

#### Locations of Investigative Field Offices

**Houston, TX**

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

**Laredo, TX**

901 Victoria St., Suite G  
Laredo, TX 78045  
(956) 796-2917 / Fax (956) 717-0395

**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, Suite 250  
McAllen, TX 78501  
(956) 664-8010 / Fax (956) 618-8151

**Miami, FL**

3401 SW 160th Ave., Suite 401  
Miramar, FL 33027  
(954) 538-7555 / Fax (954) 602-1033

**Mobile, AL**

DHS-OIG Alabama JFO  
1141 Montlimar Dr., Suite 2500  
Mobile, AL 36609  
(251) 344-1487 / Fax: (251) 343-9779

**New York City, NY**

111 Pavonia Ave., Suite 630  
Jersey City, NJ 07310  
(201) 356-1800 / Fax (201) 356-4038

**Oakland, CA**

300 Frank H. Ogawa Plaza, Suite 275  
Oakland, CA 94612  
(510) 637-4311 / Fax (510) 637-4327

**Orlando, FL**

FEMA Long Term Recovery Office  
100 Sunport Lane  
Attn.: SA James DePalma  
Orlando, FL 32809-7892

**Philadelphia, PA**

Greentree Executive Campus  
5002 B Lincoln Drive West  
Marlton, NJ 08053  
(856) 596-3800 / Fax (856) 810-3410

**San Diego, CA**

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

**San Juan, PR**

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

**Appendix A**  
**OIG Headquarters/Field Office Contacts and Locations**  
**Locations of Investigative Field Offices**

**Seattle, WA**

2350 Carillon Point  
Suite 2360  
Kirkland, WA 98033  
(425) 250-1260 / Fax (425) 576-0898

**St. Thomas, VI**

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

**Tucson, AZ**

2120 West Ina Rd., Suite 201  
Tucson, AZ 85741  
(520) 229-6421 / Fax (520) 742-7192

**Washington, DC**

**(Washington Field Office)**  
1300 North 17<sup>th</sup> St., Suite 510  
Arlington, VA 22209  
(703) 235-0848 / Fax (703) 235-0854

**Yuma, AZ**

775 E. 39<sup>th</sup> St., Room 216  
Yuma, AZ 85365  
(928) 314-9640 / Fax (928) 314-9640



**Appendix A**  
**OIG Headquarters/Field Office Contacts and Locations**  
**Locations of Disaster Assistance Oversight Field Offices**

**Atlanta, GA**

The Millennium in Midtown  
10 Tenth St., N.E., Suite 750  
Atlanta, GA 30309  
(404) 832-6700 / Fax: (404) 832-6645

**Biloxi, MS**

2350 Beach Blvd. (Attn: DHS-OIG)  
Biloxi, MS 39531  
(228) 385-5605 / Fax: (228) 385-7149

**Dallas, TX**

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

**New Orleans, LA**

One Seine Court, Room 516  
New Orleans, LA 70114  
(504) 762-2151 / Fax (504) 762-2873

**Oakland, CA**

300 Frank H. Ogawa Plaza, Suite 275  
Oakland, CA 94612  
(510) 637-1482 / Fax: (510) 637-1484

**Orlando, FL**

FEMA Long Term Recovery Office  
100 Sunport Lane  
Orlando, FL 32809-7892  
(407) 856-3204

**San Juan, PR**

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

**St. Thomas, VI**

Federal Building  
5500 Veterans Dr., Room 207  
St. Thomas, VI 00802  
(340) 774-0190 / Fax (340) 774-0191

## Appendix B Acronyms

|         |   |
|---------|---|
| AC&I    | acquisition, construction, and improvement  |
| ACE     | Automated Commercial Environment  |
| ADVISE  | Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement                           |
| AFGP    | Assistance to Firefighters Grant Program  |
| ATS     | Automated Targeting System  |
| BPA     | blanket purchase agreement  |
| BZPP    | Buffer Zone Protection Plan   |
| CBP     | Customs and Border Protection   |
| CS&T    | cargo selectivity and targeting   |
| DHS     | Department of Homeland Security   |
| DNDO    | Domestic Nuclear Detection Office   |
| DRF     | Disaster Relief Fund  |
| e-Gov   | Electronic Government   |
| eMerge2 | Electronically Managing Enterprise Resources for Government<br>Effectiveness and Efficiency project |
| EPA     | Environmental Protection Agency   |
| ECIE    | Executive Council on Integrity and Efficiency   |
| FBI     | Federal Bureau of Investigation   |
| FECA    | Federal Employees' Compensation Act   |
| FEMA    | Federal Emergency Management Agency   |
| FISMA   | Federal Information Security Management Act   |
| FLETC   | Federal Law Enforcement Training Center   |
| FMAG    | Fire Management Assistance Grant  |
| FPS     | Federal Protective Service  |
| FTE     | full-time equivalent  |
| FY      | fiscal year   |
| GAO     | Government Accountability Office  |
| GSA     | General Services Administration   |
| HSARPA  | Homeland Security Advanced Research Projects Agency   |
| HSPI    | Homeland Security Policy Institute  |
| HITRAC  | Homeland Infrastructure Threat and Risk Analysis Center   |

---

|         |  |
|---------|--|
| HMGP    | Hazard Mitigation Grant Program                                |
| HUBZone | Historically Underutilized Business Zone                       |
| I&A     | intelligence and analysis                                      |
| ICE     | Immigration and Customs Enforcement                            |
| IG      | Inspector General  |
| IHP     | Individuals and Households Program                             |
| IMAGE   | ICE Mutual Agreement between Government and Employers          |
| INS     | Immigration and Naturalization Service                         |
| IP      | Infrastructure Protection                                      |
| IPv6    | Internet Protocol Version 6                                    |
| IT      | Information Technology   |
| JFO     | Joint Field Offices  |
| MOU     | Memorandum of Understanding                                    |
| NADB    | National Asset Database  |
| NBIS    | National Biosurveillance Integration System                    |
| NCSD    | National Cyber Security Division                               |
| NEMIS   | National Emergency Management Information System               |
| NFIP    | National Flood Insurance Program                               |
| NOC     | National Operations Center                                     |
| NSF     | National Screening Force                                       |
| OES     | Office of Emergency Services                                   |
| OGT     | Office of Grants and Training                                  |
| OIG     | Office of Inspector General                                    |
| OMB     | Office of Management and Budget                                |
| ONDCP   | Office of National Drug Control Policy                         |
| PCIE    | President's Council on Integrity and Efficiency                |
| PDA     | personal digital assistant                                     |
| PDM     | Pre-Disaster Mitigation  |
| PPR     | Plans, Programs, and Requirements                              |
| RAMCAP  | Risk Analysis and Management for Critical Asset Protection     |
| S&T     | Science and Technology   |
| SAFETY  | Support Anti-terrorism By Fostering Effective Technologies Act |
| SAVE    | Systematic Alien Verification for Entitlements Program         |
| SBI     | Secure Border Initiative                                       |

*Department of Homeland Security*

|          |   |
|----------|---|
| SFO      | San Francisco International Airport                   |
| TH       | Transitional Housing                                  |
| TOI      | targets of interest                                   |
| TOPOFF 3 | Top Officials Three Exercise                          |
| TSA      | Transportation Security Administration                |
| TSO      | TSA Screening Officers                                |
| UASI     | Urban Area Security Initiative                        |
| USCG     | United States Coast Guard                             |
| USCIS    | United States Citizenship and Immigration Service     |
| USDA     | U.S. Department of Agriculture                        |
| USSS     | United States Secret Service                          |
| VUAV     | Vertical Take-off and Landing Unmanned Aerial Vehicle |
| WPB      | 123-foot Island Class Patrol Boats                    |
| WHEC     | High Endurance Cutters                                |
| WTCCIC   | World Trade Center Captive Insurance Company          |
| WYO      | Write Your Own (program)                              |

## Appendix C – Performance Goals, Measures, and Accomplishments

| <b>FY 2006</b>           |  |
|--------------------------|--|
| <b>Performance Goals</b> | <b>Fiscal Year 2006 Actual Performance</b> |

### Goal 1. Add value to DHS programs and operations.

|  |      |
|--|------|
| 1.1 Provide audit and inspection coverage of 75 percent of DHS's critical mission areas, the President's Management Agenda, and the most serious management challenges facing DHS. | 100% |
| 1.2 Achieve at least 79 percent concurrence with recommendations contained in OIG audit and inspection reports (excludes grant audits).  | 91%  |
| 1.3 Complete draft reports for at least 75 percent of inspections and audits within 6 months of the project start date (excludes grant audits).                                    | 64%  |

### Goal 2. Ensure integrity of DHS programs and operations.

|   |     |
|---|-----|
| 2.1 At least 75 percent of substantiated investigations are accepted for criminal, civil, or administrative action.                 | 95% |
| 2.2 At least 75 percent of investigations referred resulted in indictments, convictions, civil findings, or administrative actions. | 75% |
| 2.3 Provide audit coverage of \$500 million of DHS's grant programs.  | 52% |
| 2.4 Achieve at least 75 percent concurrence with 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. | Being Implemented |
| 3.2 | Establish and implement an employee training program for DHS-OIG.                                    | Being Developed   |





## **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](http://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, write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292 or email [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov). The OIG seeks to protect the identity of each writer.