

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General



FISCAL YEAR 2008

ANNUAL PERFORMANCE PLAN

The Department of Homeland Security

Office of Inspector General

Fiscal Year 2008 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 2008 Annual Performance Plan* for the Department of Homeland Security's (DHS) Office of Inspector General (OIG). This plan, which is our sixth, outlines the projects that we intend to undertake this fiscal year to evaluate DHS' 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 manmade attacks and natural disasters that may occur. To better align our disaster oversight efforts with DHS' post-Hurricane Katrina realignment, our Office of Disaster Assistance Oversight was renamed the Office of Emergency Management Oversight.

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 audits, inspections, and investigations to promote economy, efficiency, and effectiveness in DHS' programs and operations, and to prevent and detect fraud, waste, abuse, and mismanagement.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents

Chapter	Page
1. OIG Mission and Responsibilities	1
2. OIG Organizational Structure	2
3. FY 2008 Planning Approach	5
4. Allocation of Resources	7
5. FY 2008 Performance Goals and Measures.....	8
6. Project Narratives.....	9
• Directorate for Management.....	9
• Directorate for National Protection and Programs.....	21
• Directorate for Science and Technology.....	24
• Domestic Nuclear Detection Office.....	27
• Federal Emergency Management Agency.....	28
• Office of Intelligence and Analysis.....	51
• Transportation Security Administration.....	54
• United States Citizenship and Immigration Services.....	62
• United States Coast Guard.....	64
• United States Customs and Border Protection.....	71
• United States Immigration Customs Enforcement.....	80
• Multiple Components.....	83
Appendix A - OIG Headquarters and Field Office Contacts	88
Appendix B - Table of Acronyms	91
Appendix C - FY 2007 Performance Goals, Measures, and Accomplishments...	93

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 audit, inspect, 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, the OIG's key legislated responsibilities are as follows:

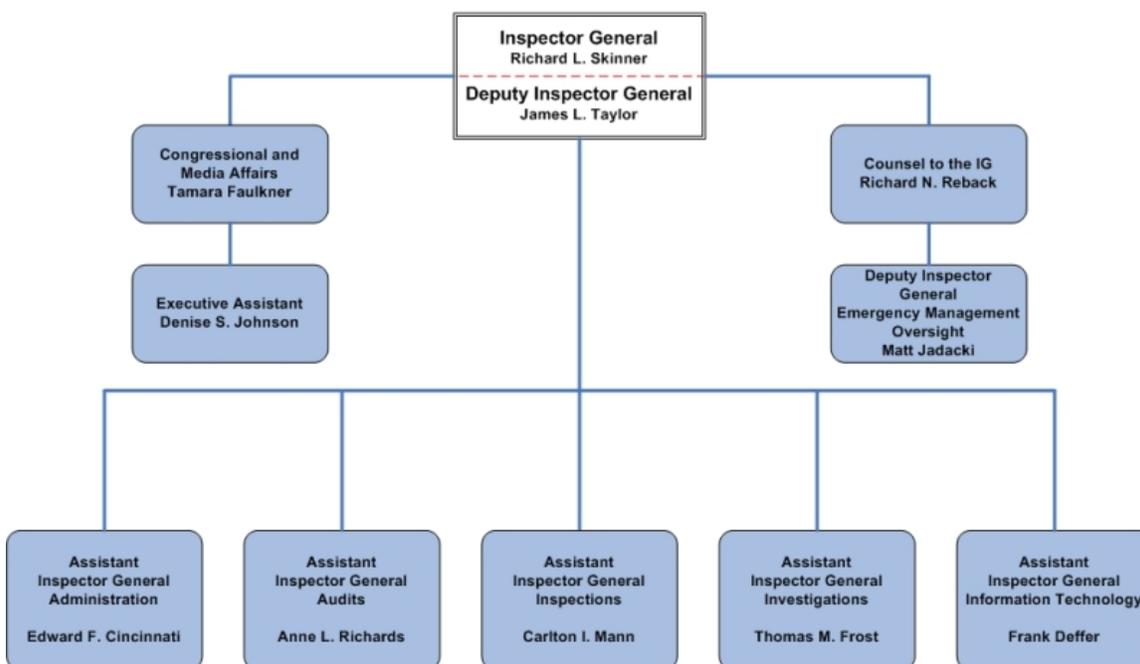
- Conduct and supervise independent and objective audits and investigations relating to the department's programs and operations;
- Promote economy, effectiveness, and efficiency within the department;
- Prevent and detect fraud, waste, and abuse in department programs and operations;
- Review recommendations regarding existing and proposed legislation and regulations relating to department programs and operations;
- Maintain effective working relationships with other federal, state, and local governmental agencies, and non-governmental entities regarding the mandated duties of the OIG; and
- Keep the Secretary and the Congress fully and currently informed of problems in agency programs and operations.

Chapter 2 – OIG Organizational Structure

We are composed of an Executive Office and 7 functional components that are based in Washington, D.C. We also have field offices throughout the country.

The OIG Management Team is reflected below.

Department of Homeland Security Office of Inspector General Management Team



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 and other management officials; 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;

furnishes attorney services for the issuance and enforcement of OIG subpoenas; and provides legal advice on OIG operations. 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 146 FTEs.

The Office of Emergency Management Oversight (EMO) 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 is an independent and objective means of keeping the Congress, the Secretary of Homeland Security, the Administrator of the Federal Emergency Management Agency, and other federal disaster relief agencies fully informed on problems and deficiencies relating to disaster operations and assistance programs, and progress regarding corrective actions. Our focus is weighted heavily toward prevention, including reviewing internal controls, and monitoring and advising DHS and FEMA officials on contracts, grants, and purchase transactions before they are approved. This approach allows the office to stay current on all disaster relief operations and provide on-the-spot advice on internal controls and precedent setting decisions. EMO has 75 FTEs including temporary employees dedicated to Gulf Coast Hurricane recovery operations.

The Office of Inspections provides the IG with a means to analyze programs quickly and to evaluate operational efficiency and vulnerability. This work includes special reviews of sensitive issues that arise suddenly and congressional requests for studies that require immediate attention. Inspectors may examine any area of the department, plus it is the lead OIG unit for reporting on DHS intelligence, international affairs, civil rights and civil liberties, and science and technology. Inspections reports use a variety of study methods and evaluate techniques to develop recommendations for DHS and the reports are released to DHS, Congress, and the public. The office has 41 FTEs.

The Office of Information Technology conducts audits and evaluations of DHS' 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' information security program as mandated by the Federal Information Security Management Act (FISMA). In addition, this office provides technical forensics assistance to OIG offices in support of OIG's fraud prevention and detection program. 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' various internal affairs offices. This office has 188 FTEs and has assigned staff to the Office of Emergency Management Oversight to work on 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 semiannual reports to the Congress. This office has 41 FTEs.

Chapter 3 – FY 2008 Planning Approach

The Annual Performance Plan is our “roadmap” for the inspections and audits that we plan to conduct each year to evaluate DHS programs and operations. In devising the plan, we endeavor to assess DHS’ progress in meeting what it considers to be the major management challenges and the Secretary’s goals and priorities.

This plan describes more projects than may be completed in Fiscal Year (FY) 2008, 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 as the year progresses. The plan includes projects that were initiated, but not completed, during FY 2007. Finally, the plan lists some jobs that will start during FY 2008, but will carry over into FY 2009.

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

DHS’ near-term priority goals are divided into five areas:

- Protect Our Nation From Dangerous People,
- Protect Our Nation From Dangerous Goods,
- Protect Critical Infrastructure,
- Build a Nimble, Effective Emergency Response System and a Culture Preparedness, and
- Strengthen and Unify DHS Operations and Management.

The President’s Management Agenda addresses the following:

- Strategic Management of Human Capital,
- Competitive Sourcing,
- Improved Financial Performance,
- Expanded Electronic Government, and
- Budget and Performance Integration.

In our report titled *Management Challenges Facing the Department of Homeland Security*, we identified the following as the most serious FY 2007 management challenges facing DHS:

- Catastrophic Disaster Response and Recovery,
- Acquisition and Contract Management,
- Grants Management,
- Financial Management,
- Information Technology (IT) Management,
- Infrastructure Protection,
- Border Security,
- Transportation Security, and
- Trade Operations and Security.

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

We will strive to have a consultative and collaborative working relationship with senior management of DHS while at the same time providing, constructive and objective information to promote DHS management decision-making and accountability.

Chapter 4 – Allocation of Resources

The President has requested an appropriation of \$99,111,000 for the OIG in FY 2008.

STANDARD OBJECT CLASSIFICATION SCHEDULE

Object Classifications		FY 2007 Enacted ¹	President's Budget	FY 2008 Change
11.1	Perm Positions	\$ 42,044	\$ 43,671	\$ 1,627
11.3	Other than perm	\$ -	\$ 4,119	\$ 4,119
11.5	Other per comp	\$ 3,587	\$ 3,767	\$ 180
11.8	Spec Srvc Pay	\$ -	\$ -	\$ -
12.1	Benefits	\$ 13,545	\$ 15,054	\$ 1,509
21.0	Travel	\$ 4,176	\$ 5,411	\$ 1,235
22.0	Transportation of things	\$ 66	\$ 86	\$ 20
23.1	GSA rent	\$ 8,308	\$ 8,343	\$ 35
23.2	Other rent	\$ 510	\$ 510	\$ -
23.3	Communication, Utilities, and misc charges	\$ 2,982	\$ 3,011	\$ 29
24.0	Printing	\$ 41	\$ 41	\$ -
25.1	Advisory & Assistance Services	\$ 1,102	\$ 5,454	\$ 4,352
25.2	Other Services	\$ 943	\$ 1,154	\$ 211
25.3	Purchase from Govt. Accts.	\$ 5,796	\$ 5,934	\$ 138
25.7	Operation & maintenance of equipment	\$ 319	\$ 320	\$ 1
26.0	Supplies & materials	\$ 767	\$ 900	\$ 133
31.0	Equipment	\$ 899	\$ 989	\$ 90
32.0	Land & Structures	\$ -	\$ 247	\$ 247
42.0	Indemnity	\$ -	\$ -	\$ -
91.0	Unvouchered	\$ 100	\$ 100	\$ -
Total, Audits, Inspections & Investigations Program		\$ 85,185	\$ 99,111	\$ 13,926
Full Time Equivalents		545	551	6

¹ Does not include the \$13.5M or \$4M transfers from the Disaster Relief Fund.

Chapter 5 – FY 2008 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, our performance goals and measures will be updated annually for maximum effectiveness in meeting the changing needs of DHS, consistent with OIG's statutory responsibilities. In addition to the mandatory requirements, performance measures identified serve as a basis to determine the overall effectiveness of our work.

Goal 1. Add value to DHS programs and operations.

- 1.1 Provide audit and inspection coverage of 75% of DHS' strategic objectives, the President's Management Agenda, and major management challenges facing DHS.
- 1.2 Achieve at least 85% concurrence with recommendations contained in OIG audit and inspection reports.
- 1.3 Complete draft reports for at least 75% 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% of substantiated investigations are accepted for criminal, civil, or administrative action.
- 2.2 At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.
- 2.3 Provide audit coverage of \$1 billion of DHS' grant programs.
- 2.4 Achieve at least 85% concurrence from DHS management with OIG recommendations on grant audits.

Goal 3. Deliver quality products and services.

- 3.1 Establish and implement an internal quality control review program covering all elements of DHS OIG. In particular, conduct peer reviews to ensure that applicable audit, inspection, and investigation standards and policies are being followed.
- 3.2 Ensure that 100% of DHS OIG employees have an annual Individual Development Plan. *(new)*
- 3.3 Ensure that 100% of all eligible DHS OIG employees have an Individual Performance Plan and receive an annual Rating of Record. *(new)*

Chapter 6 – Project Narratives

DIRECTORATE FOR MANAGEMENT

FY 2008 Audit of DHS' Consolidated Financial Statements (Mandatory)

The Chief Financial Officers Act requires that an annual financial statement audit be performed at DHS. We will contract with an independent public accounting (IPA) firm to conduct the audit of the DHS consolidated financial statements, including roll-up of the U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), and Federal Law Enforcement Training Center (FLETC) standalone audits into the consolidated financial statements. Additionally, as part of the financial statement audit the IPA will perform an auditability assessment of USCG.

Objectives: Ascertain and report on the fairness of presentations of DHS' FY 2008 financial statements; obtain an understanding of internal control 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 to identify noncompliance that 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. *Office of Audits*

Individual Audits of CBP's, FLETC's, and TSA's Financial Statements (Mandatory)

The Chief Financial Officers Act requires that an annual financial statement audit be performed at DHS. We will contract with IPA firms to conduct standalone audits of CBP, FLETC, and TSA in conjunction with the consolidated statement audit.

Objectives: Ascertain and report on the fairness of presentations of CBP's, FLETC's, and TSA's FY 2008 financial statements; obtain an understanding of internal control 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 to identify noncompliance that 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. *Office of Audits*

FY 2008 Audit of DHS' Internal Control Over Financial Reporting (Mandatory)

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

The Office of Management and Budget (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, which addresses financial performance in the President's Management Agenda.

Objective: Ascertain and report on the effectiveness of DHS' internal control over financial reporting in conjunction with the FY 2008 DHS consolidated financial statement audit. *Office of Audits*

Office of National Drug Control Policy (ONDCP) Reviews at CBP, USCG, and Immigration and Customs Enforcement (ICE) (Mandatory)

Under 21 U.S.C. 1704 (d) and the ONDCP Circular, *Drug Control Accounting*, our office is required to perform a review of assertions made by management related to FY 2007 obligations for the National Drug Control Program. We will contract with independent public accounting firms to review CBP's, USCG's, and ICE's ONDCP assertions. This review addresses in part financial performance in the President's Management Agenda.

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

DHS' Corrective Action Plan Process and Implementation of OMB Circular A-123 at the Office of Chief Financial Officer (OCFO), the Federal Emergency Management Agency (FEMA), TSA, and ICE

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.

Objectives: Determine the adequacy of and the process for developing competent, corrective action plans and how this process is integrated into DHS' plan to fully implement OMB Circular A-123 to assess remediation action between FY 2007 and FY 2008 at the OCFO, FEMA, TSA, and ICE. Additionally, this audit will address management's self-assessment of internal control and related corrective action plans. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

USCG's Progress in Improving Financial Management

Since becoming part of DHS in 2003, USCG has struggled with severe weaknesses in its financial management and reporting. USCG contributes to the DHS Disclaimer of Opinion and all of the Material Weaknesses. In FY 2007, USCG contracted with public accounting firms to begin addressing those weaknesses, starting with the development of corrective action plans.

Objectives: Determine the adequacy of and the process for developing competent, corrective action plans and how this process is integrated into DHS' plan to fully implement OMB Circular A-123 at USCG including the progress made between FY 2007 and FY 2008 in implementing its corrective action plans and moving to a more stable, long-term financial management organization and capability. Additionally, this audit will address management's self-assessment of internal control and related corrective action plans. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

Small and Disadvantaged Business Utilization (Congressional)

The U.S. House of Representatives adopted an amendment to the *Department of Homeland Security Appropriations Bill, 2008*, requiring OIG to examine DHS' use of procurement authorities to assist small and disadvantaged businesses. The 8(a) Business Development Program enables federal agencies to award sole source contracts without preparing the written justifications and approvals normally required for sole source contracts. Moreover, an agency may limit competition for certain solicitations to participants in the 8(a) Business Development Program or Historically Underutilized Business Zone Program.

Objective: Assess the extent to which DHS is effectively and properly using small and disadvantaged businesses in DHS procurements. *Office of Audits*

Control of Accountable Property

Several DHS components have large, armed workforces, such as the United States Secret Service, Federal Air Marshals, CBP, and ICE agents. In addition, several components

have internal affairs agents who carry weapons. Federal property regulations deem the weapons, along with their ammunition and protective clothing, as sensitive property from several perspectives—security, safety, and high value. Specific inventory control requirements apply to sensitive property to limit accessibility to authorized individuals and ensure accountability.

Objectives: Assess the extent to which DHS is complying with applicable federal and DHS policies, procedures, and internal controls over weapons, ammunition, and protective clothing. For selected offices, evaluate implementation of applicable policies, procedures, and internal controls. *Office of Audits*

Suspension and Debarment

Suspension and debarment are intended to prevent poor performance, waste, fraud, and abuse in federal procurement. Suspension temporarily excludes a person or company from bidding on, receiving, or participating in federally funded contracts and grants, pending completion of an investigative, legal, or administrative proceeding. The General Services Administration (GSA), on behalf of the federal government, operates an Internet-accessible database that includes names and addresses of contractors who are excluded from federal contracts, for names involved in a single action. As part of the responsibility determination that agencies make before soliciting contractors, they are to check the GSA database. When an agency becomes aware of a contractor's poor performance, it should take action that may lead to suspension and debarment. While DHS spends more than one-third of its budget through contracts and billions more in grants, it took not one suspension or debarment action in FYs 2005 and 2006.

Objectives: Assess the extent to which DHS is complying with applicable federal and DHS policies, procedures, and internal controls to ensure that selected vendors are not debarred, suspended, or otherwise ineligible for new federal contracts and that DHS takes appropriate measures to address performance or conduct problems with contractors, up to and including debarment. *Office of Audits*

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.

Objectives: Determine the progress of the DHS 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) clearance processing in a timely manner and the impact the process is having on program performance. *Office of Inspections*

Oversight of Contracted IT-Related Testing Performed as Part of DHS' FY 2008 Audited Financial Statements *(Mandatory)*

We contracted with an IPA firm to conduct DHS' annual financial statement audit. Individual audits of CBP's, FLETC's, and TSA's financial statements will be performed in conjunction with the consolidated statement audit. As a part of this annual audit, the IPA firm's IT auditors perform a review of general and application controls in place over critical financial systems.

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

Annual Evaluation of DHS' Information Security Program for FY 2008 *(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 OMB, requires an annual review and reporting of agencies' compliance with the requirements under 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.

Objectives: Determine what progress DHS has made in resolving weaknesses cited in prior OIG reviews. *Office of IT Audit*

FY 2008 Audit of DHS' Internal Control Over Financial Reporting Relating to IT *(Mandatory)*

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

Objective: Assess the effectiveness of DHS' internal control over financial reporting relating to IT in conjunction with the FY 2008 DHS consolidated financial statement audit. *Office of IT Audit*

DHS' IT Plans of Action and Milestones 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. Plans of action and milestones are an integral part of implementing OMB Circular A-123 because they identify needed improvements and corresponding remedial actions.

Objectives: Determine the adequacy of DHS' process for developing competent IT plans of action and milestones and how this process is integrated into DHS' plan to fully implement OMB Circular A-123. This audit addresses financial performance in the President's Management Agenda. *Office of IT Audit*

Followup Review of DHS' IT Disaster Recovery Programs

In May 2005, we reported that DHS did not have a comprehensive IT disaster recovery program, leaving its programs and operations at risk. For example, 15 of the 19 (79%) facilities reviewed did not have a recovery site, or the recovery site was not fully operational. DHS agreed with our findings and recommendations, and initiated efforts to establish a comprehensive program.

Objective: Determine what improvements DHS has made in its disaster recovery capabilities since our May 2005 report. *Office of IT Audit*

DHS IT Management Structure

Creating a single infrastructure for effective communications and information exchange remains a major management challenge for the DHS Chief Information Officer (CIO). However, as we reported in July 2004, the DHS CIO is not well positioned with the authority, reporting relationships, resources, and investment control needed to meet the department's IT objectives. Recently, the department has taken steps to strengthen its

CIO position, in line with Clinger-Cohen Act requirements as well as the successful examples of other federal and industry CIO organizations.

Objectives: Assess the effectiveness of recent DHS actions to strengthen its CIO position and whether these changes have helped further progress toward creating a single department-wide infrastructure for effective communications and information exchange.
Office of IT Audit

DHS' Web Server Security

Web servers are listed in the top 20 Internet security vulnerabilities by the SysAdmin, Audit, Network, Security (SANS) Institute. Public websites are hacked on an almost daily basis, and the threat that DHS web servers could be compromised is real. Damage can be anything from a denial-of-service attack, the placement of pornographic material, the posting of political messages, or the deletion of files or the placement of malicious software.

Objective: Determine whether DHS has adequate security controls over its web servers to protect against unauthorized access from internal and external threats. *Office of IT Audit*

DHS Networks' Vulnerability to External Threats and Penetration

With the Nation's critical infrastructures' increasing reliance on computers and networks, government officials are increasingly concerned about attacks from individuals and groups with malicious intent—such as crime, terrorism, foreign intelligence gathering, and acts of war. Further, government agencies are becoming increasingly concerned about the prospect of combined physical and cyber attacks, which could have devastating consequences. Therefore, performing penetration tests is essential for evaluating the security posture of DHS' networks and for determining the possible level of damage that can occur if DHS' network is compromised.

The purposes of penetration testing are to (1) identify methods of gaining access to a system by using common tools and techniques used by attackers, and (2) discover and mitigate security vulnerabilities before they can be exploited.

Objective: Determine, through the use of penetration testing, whether DHS has implemented effective controls over its networks. *Office of IT Audit*

Portable Storage Device Security

The proliferation of portable electronic storage devices increases the risk of unauthorized access to sensitive data. Examples of portable storage devices are flash drives, jump drives, pen drives, and thumb drives, and portable music players that can also be used to

store data. These devices are small enough to fit into a shirt pocket, relatively inexpensive, and can be used to store a large amount of data. However, these very features can introduce new security risks and amplify risks that already existed with floppy disks.

Objective: Determine whether DHS has implemented effective controls over the use of portable storage devices. *Office of IT Audit*

Technical Security Evaluation of the National Center for Critical Information Processing and Storage

Information security is an important goal for any organization that depends on information systems and computer networks to carry out its mission. 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 at their respective work sites. Toward that end, we have developed an agency-wide information system security program.

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

DHS OneNet

OneNet is a single network that is to use dual carriers to support interoperability and data sharing, in all DHS mission areas, among all DHS components. DHS is deploying OneNet to DHS components. DHS has deployed the initial core of the DHS OneNet and has built a primary Network Operation Center to monitor OneNet performance.

Objective: Determine DHS' progress in consolidating its networks onto OneNet to achieve operational efficiencies and cost savings. *Office of IT Audit*

Oversight of Contracted IT-Related Testing Performed as Part of DHS' FY 2007 Audited Financial Statements (Mandatory)

We contracted with an IPA firm to conduct the annual financial statement audit. Individual audits of CBP's, FLETC's, and TSA's financial statements will be performed in conjunction with the consolidated statement audit. As a part of this annual audit, the IPA firm's IT auditors perform a review of general and application controls in place over critical financial systems.

Objectives: Determine whether contract auditors performed sufficient testing to evaluate DHS' general and application controls over critical financial systems and data to reduce the risk of loss due to errors, fraud, or other illegal acts and disasters, and to effectively

protect the information infrastructure from security threats or other incidents that cause the systems to be unavailable. *Office of IT Audit*

Directorate for Management Carryover Projects From FY 2007

DHS' Corrective Action Plan Process and Implementation of OMB Circular A-123 at OCFO, TSA, ICE and FEMA

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.

Objectives: Determine the adequacy of and the process for developing competent corrective action plans and how this process is integrated into DHS' plan to fully implement OMB Circular A-123 and to assess remediation action between FY 2006 and FY 2007 at OCFO, FEMA, TSA, and ICE. Additionally, this audit will address management's self-assessment of internal control and related corrective action plans. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

USCG Progress in Improving Financial Management

Since becoming part of DHS in 2003, USCG has struggled with severe weaknesses in its financial management and reporting. USCG contributes to the DHS Disclaimer of Opinion and all of the Material Weaknesses. In FY 2007, USCG contracted with public accounting firms to help it begin addressing those weaknesses, starting with the development of corrective action plans.

Objectives: Determine the adequacy of and the process for developing competent corrective action plans and how this process is integrated into DHS' plan to fully implement OMB Circular A-123 at USCG including the progress made between FY 2006 and FY 2007 in implementing its corrective action plans and moving to a more stable, long-term financial management organization and capability. Additionally, this audit will address management's self-assessment of internal control and related corrective action plans. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

FY 2007 Audit of DHS' Consolidated Financial Statements (Mandatory)

The Chief Financial Officers Act requires that an annual financial statement audit be performed at DHS. We contracted with an IPA 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.

Objectives: Ascertain and report on the fairness of presentations of DHS' FY 2007 financial statements; obtain an understanding of internal control 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 to identify noncompliance that 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. *Office of Audits*

FY 2007 Audit of DHS' Internal Control Over Financial Reporting (Mandatory)

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

OMB Circular A-123, *Management's Responsibility for Internal Control* (Revised), requires agency 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, which addresses financial performance in the President's Management Agenda.

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

Training and Qualifications of Acquisition Workforce

DHS purchased almost \$10 billion of goods and services in FY 2004 through almost 60,000 procurement actions such as contracts, delivery orders, and interagency agreements. DHS, according to 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 OMB) 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.

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. *Office of Audits*

Status of DHS Acquisition Function

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 will 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 use.

Objective: Determine how well DHS manages and supports complex procurement programs. *Office of Audits*

DHS' Financial Systems Consolidation

The DHS Financial Systems Consolidation Project will bring together the financial, budget, and asset control activities of the 22 DHS component agencies. As part of this effort, DHS is making plans to consolidate all DHS components on financial systems currently run at the USCG.

Objective: Determine whether DHS has properly justified its approach to consolidating financial systems under the financial systems consolidation project. *Office of IT Audit*

Internet Protocol Version 6 (IPv6)

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. IPv6 is replete with new features and functions such as expanded address space, improved flexibility and functionality, improved information routing, enhanced mobility features, simplified activation, configuration and operation of networks and services, and once fully implemented, improved security.

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 (EA) assessment in February 2006.

Objective: Assess the progress DHS has made in developing and implementing its IPv6 transition plan. *Office of IT Audit*

FY 2007 Audit of DHS' Internal Control Over Financial Reporting Relating to IT
(Mandatory)

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

Objectives: Ascertain and report on the effectiveness of DHS' internal control over financial reporting relating to IT in conjunction with the FY 2007 DHS consolidated financial statement audit. *Office of IT Audit*

DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS

Petroleum and Natural Gas Subsectors

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 subsector 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 subsector also poses public safety and economic risks, as natural gas meets one-fifth of the Nation's electrical needs.

Objective: Determine the scope and effectiveness of DHS efforts to support the Department of Energy's protection of the petroleum and natural gas subsectors. *Office of Inspections*

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, to support its risk management framework. A maturing database 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 decisionmaking. 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 database. However, that review did not fully assess the extent that the database is used to inform programmatic analyses.

Objective: Determine the extent that DHS is using the National Asset Database to support its risk management framework. *Office of Inspections*

Vulnerability Assessment Methodologies

There is a wide variety of vulnerability assessment methodologies in use by public and private entities. The Office of Infrastructure Protection is attempting to establish output standards for vulnerability assessments; assist entities in evaluating, modifying, or developing vulnerability assessment methodologies; and participate in vulnerability assessments of critical sites, operational systems, states, and regions. The Office of Infrastructure Protection 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.

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

Followup Review of National Cyber Security

The Director, National Cyber Security Division (NCSA), formerly part of the DHS Information Analysis and Infrastructure Protection (IAIP) 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 serves 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.

Objective: Determine whether NCSA has managed effectively the implementation of the National Strategy to Secure Cyberspace and the department's cyber security program. *Office of IT Audit*

Directorate for National Protection and Programs Carryover Projects From FY 2007

The Office of Infrastructure Protection's Resource Requirements (Congressional)

The Office of Infrastructure Protection 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 for FY 2007 \$549,140,000 and 445 FTEs.

Objectives: Determine whether (1) the physical space and number of full-time permanent staff assigned to the Office of Infrastructure Protection is adequate to meet its broad

responsibilities, and (2) what particular challenges the office faces in the use of contractors or temporary employees. *Office of Inspections*

Administering Lessons Learned From Exercises (Congressional)

The 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 compounded tragedy if a real disaster should occur.

Objectives: Determine, in the aftermath of large TOPOFF exercises, (1) how 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. *Office of Inspections*

DIRECTORATE FOR SCIENCE AND TECHNOLOGY

Research and Development in Aviation *(Congressional)*

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

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

Office of Inspections

Homeland Security Institute *(Congressional)*

Established by the Homeland Security Act of 2002, the Homeland Security Institute is a congressionally chartered, federally funded research and development center. The institute provides scientific, technical, and analytical expertise in assessing homeland security issues. The Homeland Security Institute draws on the expertise of partners from the academic, nonprofit, policy, and private sectors to frame the debate, discuss policy implications and alternatives, and recommend solutions to issues facing homeland security policymakers. The Under Secretary for Science and Technology serves as the primary DHS sponsor of the Homeland Security Institute.

Objectives: Determine (1) the effectiveness of DHS and S&T oversight of the Homeland Security Institute and (2) the extent that DHS components use the work of the institute.

Office of Inspections

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 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 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.

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 in comparison with other research, development, test, and evaluation organizations. *Office of Inspections*

Directorate for Science and Technology Carryover Projects From FY 2007

Homeland Security Advanced Research Projects Agency: Funding Research Projects (Congressional)

The Homeland Security Advanced Research Projects Agency (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 it accelerates the prototyping and deployment of technologies intended to reduce homeland vulnerabilities.

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. *Office of Inspections*

S&T's Research, Development, and Funding Priorities (Congressional)

S&T 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.

Objectives: Determine (1) the process S&T uses to set its research and development priorities and investments; (2) the decisionmaking process S&T uses to balance short- 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 decisionmaking process are resolved and documented. *Office of Inspections*

Support Antiterrorism by Fostering Effective Technologies Act *(Department Request)*

In 2002, Congress enacted the Support Antiterrorism 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 consequences. The Undersecretary of S&T currently manages the SAFETY program.

Objectives: Determine the efficacy of the SAFETY Program by reviewing (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 quantitative—executed in determining liability caps; and (4) the coordination between the S&T and other DHS departments in determining what technologies are needed in the field. *Office of Inspections*

DOMESTIC NUCLEAR DETECTION OFFICE

Carryover Projects From FY 2007

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.

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.
Office of Inspections

FEDERAL EMERGENCY MANAGEMENT AGENCY

In order to focus on and establish a continuous oversight presence in disaster-related activities, we created the Office of Disaster Assistance Oversight (DAO) on October 1, 2006. The establishment of this office has strengthened our ability to react quickly and efficiently to a variety of disasters and further advance our collaborative efforts with the federal Inspector General community, through the President's Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency's (PCIE/ECIE) Homeland Security Round Table, to achieve a holistic approach to federal disaster response and recovery oversight. Beginning in FY 2008, DAO was renamed the Office of Emergency Management Oversight (EMO), in keeping with DHS' post-Hurricane Katrina realignment.

Recurring Disaster Operations and Oversight

EMO will deploy experienced staff to FEMA Headquarters, Joint Field Offices (JFOs), National Processing Service Centers, and other FEMA field locations to provide on-the-spot advice, assistance, and oversight to DHS, FEMA, state, and local officials after major natural or manmade events that are, or will likely become, federally declared disaster declarations. Principal oversight activities include the following:

- Attending senior-level meetings at FEMA Headquarters and providing continuous, onsite 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;
- Reviewing mission assignments and supporting documentation, and coordinating and meeting with OIG officials from other federal organizations to devise plans to provide appropriate oversight of mission assignment costs;
- 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 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 (PA) repairs and restorations, and hazard mitigation, as well as other support areas (e.g., property management);
- Participating in PA applicant briefings and kick-off meetings with FEMA, state, and local officials; overseeing the development of larger PA projects to ensure work eligibility and reasonableness; performing interim reviews of subgrantees'

claims; and following up on specific issues and complaints about subgrantee 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 oversight strategies;
- Responding to congressional requests/inquiries, briefing interested parties on the results of our oversight, and coordinating with our Office of Investigations as to known or suspected fraud, waste, or abuse; and
- Coordinating with state and local government audit and investigative organizations.

In addition, EMO regional staff will maintain effective relationships with FEMA regional personnel by (1) meeting with executive and senior FEMA regional office personnel to explain EMO's mission, priorities, and capabilities; and (2) attending or participating in meetings, workshops, exercises, and conferences between FEMA and other federal agencies, regional states, and nongovernmental or volunteer organizations.

Objectives: Our focus will be on staying current on all disaster relief operations and activities and evaluating (1) FEMA's implementation of existing disaster operations and assistance policies and procedures, (2) development of new policies and procedures based on the magnitude of the disaster event, and (3) federal, state, and local internal controls over the disaster relief funding provided for disaster operations and assistance activities.
Office of Emergency Management Oversight

Disaster Assistance Grants (Nationwide)

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 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 20 audits of grantees and subgrantees, 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 PA grants, but may include hazard mitigation grants and grant assistance provided to individuals and households.

Objectives: Determine (1) the eligibility of the grantee or subgrantee and of the work funded by the grant, and (2) whether grantees or subgrantees accounted for and expended FEMA funds according to federal regulations. *Office of Emergency Management Oversight*

FEMA Disaster Acquisition Workforce

Well-managed acquisitions enable FEMA to respond effectively to disasters. A properly trained and staffed acquisition workforce is key to managing acquisitions effectively. At the time Hurricane Katrina struck, FEMA did not have sufficient numbers of trained contracting staff and contracting officer's technical representatives to meet mission requirements. In addition, an assessment process was not in place to monitor planning efforts for disaster-related procurement needs and to monitor and maintain surge capacity for disaster contracting. Funding for acquisition oversight of disaster contracts was inadequate. While FEMA has made some progress resolving staffing shortfalls, it may not be enough to be ready for the next catastrophic disaster.

Objectives: Determine whether (1) FEMA has a disaster acquisition workforce strategy whether it is adequate to satisfy the requirements of a catastrophic disaster; (2) there is an up-to-date disaster acquisition policy that includes workforce requirements for procurement, contract monitoring, and contract management; and (3) acquisition staff is properly trained. *Office of Emergency Management Oversight*

FEMA Acquisition Process

Since Hurricane Katrina, FEMA has awarded approximately 4,000 contracts totaling more than \$7 billion. With this volume of contracting for goods and services, it is essential that all agency acquisitions be handled in an efficient, effective, and accountable manner. FEMA needs to have in place sound policies and procedures to make and communicate good business practices. FEMA has committed to modernizing its acquisition function and to developing a team that will operate efficiently and effectively in support of FEMA's mission.

Objectives: (1) Determine the strengths and weaknesses of FEMA's current acquisition process from requirements identification through closeout of the final contract action; and (2) the extent to which best practices and lessons learned from disaster operations have been used to improve FEMA's acquisition process. *Office of Emergency Management Oversight*

Selected 2007 Disaster Contracts

As of June 7, 2007, the President had declared 34 major disasters in 2007 across the United States, with 30 of those disasters in states other than the Gulf Coast states. Also in June 2007, FEMA had 17 open JFOs and spent hundreds of millions of dollars responding to these disasters. Since Hurricane Katrina, the focus has been on contracting in the Gulf Coast states with limited audit attention on other disaster activities. Because of the many lessons learned and reported during 2006 and new legislation enacted since Hurricane Katrina, FEMA has implemented a number of significant changes in the

acquisitions area. However, there are concerns whether the significant policy changes have been properly documented, and if staff has been informed and trained so that there is effective and efficient implementation of these policies in the field.

Objectives: Audit ten select 2007 non-Gulf-Coast disaster contracts to: (1) determine the extent FEMA has improved its ability to track, manage, and monitor disaster contracts; (2) what internal control changes have been made to reduce and deter the level of fraud, waste, and abuse regarding disaster contracts; and (3) what impact, if any, new acquisition-related legislation has had on the state of FEMA disaster acquisitions. *Office of Emergency Management Oversight*

Acquisition Management Review/Scorecard

The success of disaster relief efforts 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. In May 2007, our office published an acquisition scorecard identifying the progress made in selected functions and activities within FEMA. The scorecard assessed the current status of the acquisition programs against key interrelated elements essential to an efficient, effective, and accountable acquisition process. This work provided a baseline for conducting further acquisition reviews, which we have incorporated into our 2008 performance plan. We will conduct another FEMA acquisition scorecard in the fall of 2008.

Objectives: Assess the current status of the acquisition programs against the following key interrelated elements essential to an efficient, effective, and accountable acquisition process: (1) organizational alignment and leadership, (2) policies and processes, (3) financial accountability, (4) acquisition workforce, and (5) knowledge management and information systems. *Office of Emergency Management Oversight*

FEMA's Non-Disaster-Specific Support Accounts

Based on survey work on the Disaster Relief Fund (DRF) in FY 2007, additional review is needed on internal controls over the use of disaster support accounts to fund disaster-related activities that are not attributable or easily allocated to a specific disaster. The control environment poses a risk of misuse or abuse of these funds but, more immediately, does not allow for the transparency and accurate reporting of these funds. With the exception of reporting on direct disaster cost associated with the three 2005 hurricanes, Katrina, Rita, and Wilma, FEMA is only required to report on the DRF as a whole. FEMA is not required to report on DRF subaccounts. Although disaster support accounts make up a small percentage of the overall DRF fund, these accounts averaged nearly \$338 million in annual expenditures over the last 5 fiscal years; nearly tripling within this timeframe. Finally, the criteria for using DRF funding is extremely flexible,

allowing wide latitude in its use, making it difficult to discern whether DRF expenditures should be more appropriately charged to other FEMA appropriations.

Objectives: Determine whether DRF obligations and expenditures: (1) are accurately tracked and whether management controls are in place to prevent and detect misuse; and (2) are made according to appropriate rules and regulations, including OMB approvals and internal guidance. *Office of Emergency Management Oversight*

Disaster Closeout Process

Once disasters are declared, obligations are made in the DRF based on estimates of expenses. With a major disaster, it can be years before the programs are completed and the disaster closed out. There are currently more than 400 open disasters. If disasters are not closed in a timely manner, the obligations may be no longer valid thus distorting the unobligated balance available in the DRF.

Objective: Determine whether open disaster declarations should be closed and funds deobligated. *Office of Emergency Management Oversight*

FEMA's National Process Service Center Operations

FEMA's National Processing Service Centers are central to successfully maintaining the FEMA helpline and registering and processing applications from disaster victims. During Hurricane Katrina recovery efforts, FEMA experienced problems meeting staffing requirements for these operations and ensuring that personnel were trained to implement appropriate business processes to assist disaster victims.

Objectives: Determine to what extent FEMA is prepared to meet staffing requirements and address the increased volume of inquiries and applications during large-scale disasters. *Office of Emergency Management Oversight*

FEMA's Housing Strategy for Future Disasters

Despite the availability of housing units in other federal agencies' inventories, FEMA purchased more than 140,000 emergency housing units, including travel trailers, mobile homes, and modular housing kits in response to Hurricanes Katrina, Rita, and Wilma. Many of the purchased units were never used, some were inappropriate and could not be used in the intended areas, and most of the modular kits were never assembled and have since deteriorated in unprotected storage. FEMA extended its disaster housing mission past the 18 months authorized in the Robert T. Stafford Act, as amended. The President requested that FEMA and the Department of Housing and Urban Development (HUD)

create a process to transition long-term disaster housing to HUD. Legal concerns about Stafford Act restrictions have delayed the process for transition.

In response to the National Disaster Housing Strategy that was mandated in the Department of Homeland Security Appropriations Act, 2007, FEMA has promised a different approach in the future to avoid such problems

Objectives: Determine the efficacy of FEMA’s (1) interagency housing coordination; (2) strategic plans for providing emergency housing to future disaster victims; and (3) strategy for addressing the persistent transitional housing issues.

Office of Emergency Management Oversight

Federal Disaster Assistance Application Process

FEMA is leading the effort to improve the promptness and efficiency with which disaster victims obtain access to eligible federal disaster assistance. A key element of this effort involves the implementation of a consolidated and unified disaster application capability to deliver timely disaster assistance and safeguard against improper payments.

Objectives: Determine to what extent FEMA’s revised disaster application process: (1) registers disaster victims in a “one-stop” manner; (2) safeguards against waste, fraud, and abuse; and, (3) is coordinated with state and local governments and voluntary organizations such as the American Red Cross.

Office of Emergency Management Oversight

FEMA’s Management of Mission Assignments

FEMA uses mission assignments to coordinate the deployment of resources from other federal agencies and is responsible for administering expenditures from the DRF. Key elements of the successful execution and management of mission assignments involve establishing mission assignment requirements, identifying what entity or entities can best fulfill those requirements, coordinating and monitoring mission assignment implementation, verifying expenditures and accounting for procured property, and administratively closing mission assignments according to established procedures.

Objectives: Determine to what extent FEMA is: (1) establishing mission assignment requirements and identifying appropriate capabilities to fulfill those assignments; (2) coordinating and monitoring the implementation of mission assignments; (3) ensuring that expenditures from the DRF are verified and procured property is accounted for; and, (4) closing mission assignments in a timely manner according to established procedures.

Office of Emergency Management Oversight

FEMA's Use of Interagency Agreements

FEMA executes interagency agreements with other federal agencies to obtain goods and services for disaster work that is expected to last longer than the 60 days defined in regulations for mission assignments. As with any acquisition, FEMA is responsible for ensuring that the procurement is appropriate and controls are in place, sufficient oversight is performed and expenditures are verified, and work is completed according to the terms of the agreement and administratively closed following established procedures.

Objectives: Determine to what extent FEMA is: (1) following established policies and procedures in initiating and administering interagency agreements; (2) appropriately monitoring implementation; (3) ensuring that expenditures from the DRF are verified and procured property is accounted for; and, (4) closing interagency agreements in a timely manner according to established procedures. *Office of Emergency Management Oversight*

FEMA's Compliance With the Flood Insurance Reform Act of 2004

The Bunning-Bereuter-Blumenauer Flood Insurance Reform Act of 2004, Public Law 108-264, included a number of provisions aimed at producing savings for flood insurance policyholders and federal taxpayers through reduced flood insurance losses and reduced federal disaster assistance. Specifically, the Act created a pilot program under the Flood Mitigation Assistance Program to focus on "severe" repetitive loss properties and established procedures for increasing flood insurance premiums for policyholders who decline mitigation offers under the pilot program.

Objectives: Determine to what extent FEMA's compliance with provisions in the Flood Insurance Reform Act of 2004 have realized savings and identified opportunities for improving mitigation outcomes. *Office of Emergency Management Oversight*

FEMA's Implementation of Federal Regulations Applying to Government Furnished Equipment

In the Federal Acquisition Regulations (FAR) Part 45 - Government Property - government agencies are given guidance on providing government property to contractors, contractor use and rental of government property, management of government property in the possession of contractors, and reporting, reuse, and disposal.

Objectives: Determine FEMA's compliance with the FAR and its controls over government-furnished equipment. *Office of Emergency Management Oversight*

FEMA's PA Project Management Process

PA grants are awarded to subgrantees of states to repair infrastructure, such as buildings and highways, damaged by disasters. FEMA's primary tool for authorizing and monitoring PA projects is the project worksheet. It is used to document the scope of work and cost estimates and to authorize payments for individual projects. Incomplete, inaccurate, untimely, or out-of-date project worksheets significantly increase the risk that grantees and subgrantees will not effectively manage projects. Poor project management leads to cost overruns, completion delays, and numerous other problems. FEMA has been criticized, particularly since Hurricane Katrina, for not having an effective method of authorizing and monitoring PA projects and for making project management more difficult for grantees and subgrantees.

Objectives: Determine the effectiveness of FEMA's process for monitoring PA projects, including the use of project worksheets, and to identify opportunities for improving the current process, as applicable. *Office of Emergency Management Oversight*

FEMA's Management and Oversight of PA Technical Assistance Contractors

FEMA awards nationwide, stand-by technical assistance contracts (TAC) to meet PA program needs that typically cannot be met by FEMA staff. PA TAC employees are specialists that provide services such as assessing and estimating disaster damages to complex facilities, and providing insurance adjustment services and historical and environmental reviews. For disasters occurring in FYs 2004, 2005, and 2006, FEMA spent \$228.3 million, \$1.4 billion, and \$94.9 million, through November 2006, respectively, for PA TACs. A contracting officer technical representative located at FEMA Headquarters oversees the master contracts and task monitors at field and regional offices provide site monitoring for TAC employees.

Objectives: Determine the efficacy of FEMA's management of PA technical assistance contractors, including processes and procedures for awarding individual task orders, evaluating contractor performance, and certifying contractor billings. *Office of Emergency Management Oversight*

Readiness – FEMA's Logistics Management Process for Responding to Catastrophic Disasters

FEMA provided record levels of support to victims and emergency responders during its response to Hurricane Katrina. However, a number of logistics failures make it clear that improvements are needed before the next major disaster. Areas needing improvement include:

- Planning, i.e., how FEMA will determine what is needed and where it is needed;

- Coordinating requirements with state and local governments;
- Coordinating with federal agencies and other response organizations;
- Identifying the best sources for needed resources;
- Tracking and timing deliveries;
- Adequate logistics staffing;
- Communication throughout the logistics process; and
- Evaluating and reporting on performance.

Objectives: Determine to what extent FEMA has improved its logistics management since Hurricane Katrina and what additional changes are needed. *Office of Emergency Management Oversight*

Readiness – Effectiveness of FEMA’s Remedial Action Management Program

FEMA has used after-action reports, facilitator-led discussions called “hot washes,” and third party reviews following disasters to identify “lessons learned” and solutions to problems that occurred during disaster response and recovery operations. However, corrective actions were not always implemented or tracked. In 2003, FEMA implemented the Remedial Action Management Program designed to consolidate, assign, track, and monitor the remediation of problems that were identified following disasters.

Objective: Determine to what extent FEMA is using its Remedial Action Management Program to implement lessons learned from Hurricane Katrina and other disasters to improve its readiness for the next catastrophic disaster. *Office of Emergency Management Oversight*

State Administration of FEMA’s PA Projects

States, as grantees, are responsible for ensuring that FEMA subgrantees are aware of requirements imposed on them by federal statutes and regulations and are required to monitor subgrantee activities to ensure compliance with applicable federal requirements. Under FEMA’s PA program, states are provided an allowance to cover the extraordinary costs incurred by state employees in managing PA projects. Such management activities include preparing project applications, formulating project worksheets, validating small projects, and conducting final inspections. Eligible costs include overtime pay and per diem and travel expenses but not regular time.

States are required to submit Administrative Plans to FEMA on how they plan to administer grants under the PA program. Each plan must include specific procedures regarding all phases of grant management and must be approved by the appropriate FEMA Regional Office. States are also required to report quarterly to FEMA on the status of all open large PA projects. Progress reports are critical to the states and FEMA in determining the status of projects, including the stage of project completion, incurred

costs, and any problems that could result in delays, cost overruns, or noncompliance with federal grant conditions.

Over the past several years, our reviews of disaster-related costs claimed by FEMA subgrantees have consistently disclosed poor grant accounting, improper contracting practices, and costs charged to the grants that were not eligible for FEMA reimbursement.

Objectives: Determine whether states (grantees) are (1) providing adequate guidance to subgrantees to ensure that they are aware of grant requirements and eligibility of costs; (2) sufficiently monitoring the activities of subgrantees; (3) submitting Administrative Plans and quarterly progress reports that include required procedures and elements for proper grant administration; and (4) using the administrative allowance for authorized purposes. *Office of Emergency Management Oversight*

Tracking PA Insurance Requirements

According to 44 Code of Federal Regulations 206.253, “No assistance shall be provided under Section 406 of the Stafford Act for any facility for which assistance was provided as a result of a previous major disaster unless all insurance required by FEMA as a condition of the previous assistance has been obtained and maintained.” Both FEMA and the states, as grantees, are responsible for tracking facilities that received federal disaster assistance in previous disasters, and for ensuring that funds are not provided a second time to a facility for which insurance coverage was not maintained as required.

Objectives: Determine (1) the extent to which FEMA and the states monitor and track insurance requirements; and (2) whether facilities that were required to maintain insurance, but did not, received assistance a second time. *Office of Emergency Management Oversight*

Eliminating Stove-piped Grant Programs

Over the last 4 years, the DHS has provided \$11.3 billion to state and local governments to prevent, prepare for, and respond to acts of terrorism. An additional \$3.2 billion in grants and other assistance provided by other federal agencies has also gone to state and local responders. These funds are provided through competitive grants either directly to organizations or through formula grants passed through state agencies to local organizations.

Historically, federal grant programs have had problems with “stove piping”—programs that focus on their narrowly defined missions without regard to the greater needs of the government as a whole. Often components support the projects that compete for funding against similar projects in another component. For example, DHS OIG’s report prepared by the Office of Inspections, Evaluations & Special Reviews on the Assistance to Firefighters Grant Program (OIG-ISP-01-03, September 2003) pointed out that many

items authorized for purchase under this program are also authorized for purchase under the State Homeland Security Grant Program. Such significant shortcomings had been identified in the past, and the potential for overlap and duplicate funding has grown as the number of grant programs has grown.

Objectives: Determine the extent to which DHS have developed plans and taken actions to (1) eliminate stove-piped grants management systems, (2) initiate best practices or measures to eliminate duplications and reduce wasteful spending, and (3) enhance coordination among internal components and external agencies to identify grant programs with similar purposes. *Office of Audits*

Effectively Managing Grant Resources

The former Office of Grant Operations, now part of FEMA, is responsible for monitoring financial activities of grant programs. The FEMA financial monitoring policy requires monitoring of all grantees at least once during the life cycle of the grant, through either a desk review or an onsite review. The office had only eight FTEs to perform financial monitoring activities and generally coordinated its site visits with the Preparedness Officer. A Preparedness Officer, assigned to each grant when it was awarded, was responsible for implementing the related programmatic monitoring plan. The Preparedness Directorate employed 24 to 30 Preparedness Officers to cover all U.S. states and territories.

The FY 2005 and FY 2006 DHS Financial Statement Audits indicated that the Office of Grant Operations and the Preparedness Division had limited resources to perform financial and programmatic monitoring over grants. As a result, DHS was exposed to the risk of inadequate monitoring, which may lead to errors in grants accrual calculations and grants that are mismanaged and misused.

Objectives: Determine the extent to which DHS effectively manages grant resources to provide sufficient financial and programmatic monitoring of all grantees. Specifically determine the extent to which DHS: (1) instituted appropriate organizational structures and workforce skill mix to achieve this mission; (2) identified gaps and deficiencies (capabilities) in the skill mix, (3) implemented processes and procedures to monitor all grantees; and (4) identified means to continually improve productivity. *Office of Audits*

Use of State and Local Strategies and Capabilities in Grant Funding Decisions

States and urban areas are required to maintain a Homeland Security Strategy to provide (1) a blueprint for comprehensive, enterprise-wide planning for homeland security efforts; and (2) a plan for the use of related federal, state, local, and private resources before, during, and after threatened or actual domestic terrorist attacks, major disasters, and other emergencies.

FEMA has been tasked with assessing the progress made in achieving the goals and objectives stated in the state or urban area Homeland Security Strategies. FEMA must also assess progress made in accomplishing the national priorities issued under the guidance of the Homeland Security Presidential Directive 8, and the impact and progress that has been made using grant program funding. Ultimately, as these strategies and capabilities are fully implemented, requests for preparedness assistance will be expressed as clearly defined requirements based on existing strategies and capabilities. Requests would answer such questions as why a capability is needed; how the capability will be used and supported; what skills will be required; and how much the capability will cost.

Objectives: Determine the extent to which FEMA used the State and Urban Areas Security Initiative strategies and capabilities in grant funding decisions. Specifically determine how FEMA: (1) captures data regarding strategies and capabilities; (2) monitors the strategies and capabilities; (3) verifies that strategies reflect current capabilities; and (4) uses the information regarding the gaps between strategies and capabilities to award grant funds. *Office of Audits*

Internal Control Review of FEMA Acquisitions

Fraud prevention is the most effective and efficient means of minimizing fraud, waste, and abuse. Internal controls are an integral part of fraud prevention. The extent that FEMA has identified, through self-assessments, and resolved internal control shortcomings is uncertain. At the time of Hurricane Katrina, FEMA disaster acquisitions lacked sufficient program management and oversight resulting in numerous problems. Disaster contract information was not readily available, the accuracy and completeness of unpaid obligations could not be fully supported, and invoices were signed without verification of receipt of goods or services. A comprehensive system of strategic internal controls that is implemented and adhered to would minimize these problems and deter fraud, waste, and abuse. The extent that FEMA has taken steps to improve their system of internal controls is unknown.

Objectives: Determine whether FEMA has: (1) established and implemented sufficient internal controls over its acquisition management program, and (2) implemented compensating controls when internal controls are waived or bypassed in the event of urgent circumstances. *Office of Emergency Management Oversight*

Federal Emergency Management Agency Carryover Projects From FY 2007

FEMA's National Flood Insurance Program

In 1968, the Congress created the National Flood Insurance Program (NFIP) in response to the rising cost of taxpayer-funded disaster relief for flood victims and the increasing amount of damage caused by floods. The NFIP makes federally backed flood insurance available in communities that agree to adopt and enforce floodplain management ordinances to reduce future flood damage. Private insurance companies, known as Write Your Own (WYO) companies, administer more than 90% of the flood insurance policies issued through the NFIP. FEMA's Mitigation Division manages the NFIP program, using the services of two contractors. Covansys is the NFIP direct contractor. Computer Sciences Corporation consolidates flood insurance information from the direct contractor and WYO company activities, compiles financial data, and prepares the financial statements for all insurance activities.

Objective: Determine compliance with laws, regulations, and guidelines governing insurance activities conducted by NFIP Servicing Agents and by WYO insurance companies. *Office of Audits*

FEMA's Pre-Disaster Readiness Contracts

After Hurricane Katrina, agencies scrambled to purchase goods and services to support disaster response efforts from thousands of vendors. Prior to the 2005 storms, the federal government had not properly assessed its disaster contracting requirements. The IG community reported that several federal agencies, including FEMA, did not have adequate acquisition plans for carrying out their assigned responsibilities. Readiness contracts with pre-negotiated prices, quantities, terms and conditions, and specifications could have greatly facilitated post-disaster procurement operations. FEMA has recently reported, and we will review, that it has improved its readiness contract strategy and is prepared.

Objectives: Determine the efficacy of FEMA's strategy for: (1) selecting disaster requirements appropriate for readiness contracts or other similar agreements; (2) planning, awarding, and monitoring these contracts; and (3) communicating and coordinating with federal, state, and local partners so that they have timely knowledge of these resources to maximize efficiency and avoid unnecessary duplicative efforts. *Office of Emergency Management Oversight*

FEMA's Emergency Housing Unit Program

FEMA provides temporary housing, including travel trailers, mobile homes, or other types of modular housing to disaster victims. During Hurricanes Katrina and Rita, FEMA spent more than \$2.5 billion on travel trailers and mobile homes. FEMA's future disaster plan includes maintaining an inventory of housing assets at storage facilities in strategic areas of the country for expedited response to housing needs.

Objectives: Determine: (1) the efficacy of the program, including funding, staffing, contracting, acquisition management, and property accountability; (2) the utility of maintaining FEMA storage facilities; and (3) the effectiveness of the procedures to ensure the proper maintenance of the housing assets. *Office of Emergency Management Oversight*

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 PA 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 initiated a pilot program to retool its debris removal program and implemented new policies and procedures.

Objectives: Determine whether the pilot program will meet the debris removal program's stated goals, and whether program evaluation criteria was established that can be used to adequately evaluate the program at the end of the pilot. *Office of Emergency Management Oversight*

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 Program for the mitigation, management, and control of any fire burning on publicly (nonfederal) or privately owned forest or grassland. Under the program, the state or Indian Tribal Government may request a declaration while a fire is burning uncontrolled and threatens such destruction as would constitute a major disaster. The program's declaration requests are submitted to the appropriate FEMA Regional Administrator for approval.

Objective: Determine whether the state (grantee) accounted for and expended fire management assistance grant funds according to federal regulations and FEMA guidelines. *Office of Emergency Management Oversight*

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 homes 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, that is rental assistance, that FEMA provides are maintained in the National Emergency Management Information System, and hotels, motels, and apartments are maintained in other databases.

Objectives: Determine whether: (1) recipients of FEMA's Disaster Housing home repair grant assistance have also received benefits from the NFIP; and (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. *Office of Emergency Management Oversight*

Use of the DRF Following DHS' Establishment of the Preparedness Directorate

A DHS reorganization that took effect on October 18, 2005, nearly 2 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 DRF, it is critical that the DRF be monitored to ensure that it is being used appropriately.

Objective: To determine whether FEMA is using the DRF for eligible expenses following DHS' establishment of the Preparedness Directorate. *Office of Emergency Management Oversight*

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.

Objective: Determine whether personal property is acquired, received, issued, disposed of, controlled, and tracked by the JFOs, Agency Logistics Centers, Territory Logistics Centers, and Remote Storage Sites in an effective and efficient manner. *Office of Emergency Management Oversight*

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.

Objective: Produce a baseline report that identifies programs and areas within the federal government that are at risk of providing duplication of benefits to disaster victims. *Office of Emergency Management Oversight*

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 has initiated efforts to improve its logistics processes and related systems. Specifically, FEMA has implemented a Total Asset Visibility program to provide enhanced visibility, awareness, and accountability over disaster relief supplies and resources.

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

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 procedures to handle claims against New York City 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. Since the company's inception, more than 8,000 individual claims have been submitted, but no claims have been paid, while the company has spent several million dollars in federal funds on legal fees to defend New York City and other named insured against these claims.

Objectives: Determine (1) why the World Trade Center Captive Insurance Company 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 people who were killed. *Office of Inspections*

States' Management of First Responder Grants Program

DHS 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, DHS awards federal "first responder" grant funds to states to assist local jurisdictions in acquiring specialized training, conducting preparedness exercises, acquiring equipment needed to respond to and manage incidents involving weapons of mass destruction, and planning and administering grants. From 2003 through 2005, the 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 reported that states' efforts for managing grant awards need improvement.

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

Assistance to Firefighters Grant Program

The Assistance to Firefighters Grant Program, 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 program falls under FEMA. FY 2003 Assistance to Firefighters Grant Program applications totaled 20,063 and requested grant awards totaled nearly \$2.5 billion. DHS, through a determination of eligibility and competitive evaluation, awarded 8,745 grants in FY 2003 with award amounts totaling \$705.2 million. OIG contractors will conduct ten grant expenditure audits each in three states, including rural, suburban, and urban fire departments. Those audits will focus on the Program's Firefighting Vehicles Acquisition Program and the Fire Operations and Firefighter Safety Program. We will summarize the results of the audits conducted in each state.

Objectives: Determine whether rural, suburban, and urban fire departments (grant recipients) in California, Illinois, and New York properly accounted for and used Assistance to Firefighters Grant Program funds according to federal requirements and the grant program guidance. *Office of Audits*

Continuing Effort to Evaluate State Management of Homeland Security Grant Funds Provided Through States

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 based on a combination of current threat estimates, critical assets, 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. The recently passed Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 2022, requires us to review this area, which is part of our continuing effort to evaluate state management of homeland security funds.

Objectives: Determine to what extent Arizona, California, Illinois, Missouri, Utah, and Washington are effectively and efficiently managing and expending homeland security grant funds to achieve established goals. *Office of Audits*

Gulf Coast Hurricane Recovery Oversight Carryover Projects From FY 2007

Project H.O.P.E. (Congressional)

At the request of a U.S. Senator, we are reviewing the Crisis Counseling Program (CCP) grant made to Florida's Department of Children and Families for the implementation of Project H.O.P.E. (Helping Our People in Emergencies) in response to Hurricanes Katrina and Wilma. The Senator additionally requested that we review whether funds had been used effectively to benefit disaster victims.

Objectives: Determine whether Project H.O.P.E. was: (1) expending funds according to the scope of the grant award; (2) being properly monitored to ensure that all participants were operating within approved guidelines, as defined by the Department of Health and Human Services Center for Mental Health Services and FEMA; and, (3) carrying out approved activities to meet the intent of the CCP. *Office of Emergency Management Oversight*

Multilayered Disaster Contracts

In the aftermath of Hurricane Katrina, FEMA has awarded more than \$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 multitiered subcontracts except at the very bottom where profitability is very low. Prices paid under contracts, both prime contracts and all their subcontracts, 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.

Objectives: Determine the extent of multilayered disaster contracts regarding Hurricane Katrina and document the various problems associated with them. This work may highlight particular case studies to illustrate the problem. *Office of Emergency Management Oversight*

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.

Objective: Determine adequacy of controls in place for management of housing assets from purchase to final disposition. *Office of Emergency Management Oversight*

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 Alabama, Louisiana, and Mississippi, where FEMA pays for security. According to FEMA's Gulf Coast Recovery Office, 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 need for alternative housing in the Gulf Coast region suggests that these TH sites may be permanent.

Objectives: Determine how well FEMA is managing its TH program transition efforts, what role other federal agencies should have in TH, and whether FEMA has devised a road map for transferring the TH sites to local governments. *Office of Emergency Management Oversight*

FEMA's Section 406 Mitigation

FEMA provides PA 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 PA grant program in the Hurricanes Katrina and Rita recovery process.

Objective: Determine how effectively FEMA is managing PA mitigation grants across the hurricane-damaged Gulf Coast. *Office of Emergency Management Oversight*

FEMA's Hazard Mitigation Grant Program

Authorized under Section 404 of the Stafford Act, the Hazard Mitigation Grant Program provides grants to states and local governments to implement long-term hazard mitigation measures after a major disaster declaration. The purpose of the program 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% 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 program funds to states along the Gulf Coast for Hurricanes Katrina and Rita.

Objective: Determine how effectively FEMA and the states are managing the Hazard Mitigation Grant Program after Hurricanes Katrina and Rita. *Office of Emergency Management Oversight*

FEMA's NFIP (Mandatory)

FEMA manages the 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 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 windstorm insurance pools in which such insurers participated.

Objective: Determine whether the NFIP's WYO program was effective in properly attributing the damage from Hurricane Katrina to either flooding or windstorm. *Office of Emergency Management Oversight*

FEMA Recommendation Tracking

Since Hurricane Katrina, our office has issued 82 disaster assistance reports and approximately 160 recommendations to FEMA. We have received no response to 27 of these 82 reports.

Objective: Determine the status of recommendations on disaster assistance reports issued since Hurricane Katrina. *Office of Emergency Management Oversight*

FEMA's Technical Assistance Contracts

In the aftermath of Hurricane 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.

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. *Office of Emergency Management Oversight*

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, CBP, ICE, and the National Communication System. FEMA awarded \$775 million in Hurricane Katrina mission assignments to those five DHS components.

Objectives: Determine whether mission assignment requirements were satisfied, funds were spent effectively and accurately accounted for, contracting followed proper procurement procedures, adequate documentation were maintained, and purchased property was managed according to governing laws and regulations. *Office of Emergency Management Oversight*

FEMA Sheltering and Transitional Housing for Evacuees

Hurricanes Katrina and Rita produced more than 1 million evacuees. Many are still living in TH. We are reviewing FEMA's planning for sheltering evacuees, and implementation of TH 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.

Objectives: Determine to what extent FEMA's TH program met the needs of hurricane victims and identify improvements that need to be addressed for future disasters. *Office of Emergency Management Oversight*

FEMA Readiness: Assessment of FEMA's Disaster Workforce

One of the critical areas that impacted FEMA's ability to effectively respond to the enormous challenges presented by Hurricane Katrina was the limited depth and strength of the FEMA Disaster Workforce. This area was well-examined in the 13 years prior to Hurricane Katrina, with 12 studies being performed by the Agency. And following the 2005 hurricane season, FEMA again initiated a study of this subject. In addition to these

FEMA-initiated actions, DHS-OIG completed an Inspections review that addressed this same issue, and the Post Katrina Emergency Management Reform Act of 2006 called for the rebuilding of FEMA's permanent and reserve workforces through some very specific actions and strategies. With input from these many sources, FEMA has worked to improve its readiness and now claims to be better prepared to response to the next catastrophic disaster.

Objectives: Determine the progress FEMA has made towards enhancing its disaster workforce since Hurricane Katrina, particularly in light of the inputs from the numerous FEMA studies, the DHS-OIG Inspections report and the 2006 Reform Act. *Office of Emergency Management Oversight*

Federal Disaster Relief Assistance Applications and Databases (Mandatory)

Conference Report H.R. 109-699 to H.R. 5441- Department of Homeland Security Appropriations Act, 2007, Title VI - National Emergency Management, Sec 696 states that all programs in DHS that administer federal disaster relief assistance should develop and maintain proper internal management controls to prevent and detect fraud, waste, and abuse. This act requires that the IG determine the existence and implementation of these internal management controls.

Objective: Determine whether DHS has developed and implemented the proper level of internal controls to prevent and detect fraud, waste, and abuse. *Office of IT Audit*

Hurricane Katrina Fraud Task Force

Our investigators continue to be active participants on the Department of Justice Hurricane Katrina Fraud Task Force established by the United States Attorney General on September 8, 2005. As a result of Hurricanes Katrina and Rita, we have established offices in Mobile, Alabama; Baton Rouge, Louisiana; Biloxi, Mississippi; and Hattiesburg, Mississippi; and have staffed these offices primarily with temporary contractor investigators who are a Cadre of On-Response Employees or Disaster Assistance Employees. We will continue to fully participate on the task force during FY 2008. *Office of Emergency Management Oversight*

OFFICE OF INTELLIGENCE AND ANALYSIS

Intelligence Oversight and Quarterly Reporting – Final Report Each Quarter *(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 us to report on a routine basis how well the department has complied with 12333, and whether any violations have occurred. USCG and the Office of Intelligence & Analysis are the only two Intelligence Community members within DHS. This report, which is signed by the IG and DHS General Counsel, is submitted quarterly to the Intelligence Oversight Board, a standing committee of the President's Foreign Intelligence Oversight Board.

Objective: Validate the assertions made by the USCG and Office of Intelligence & Analysis concerning their compliance with Executive Order 12333. *Office of Inspections*

Office of Intelligence & Analysis's Fusion Center Initiative *(Congressional)*

Executive Orders 13311 and 13356 provide guidance that will enhance the federal government'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.

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

Information Sharing at the National Operations Center (Congressional)

The National Operations Center within DHS provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence & Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The center operates 24 hours a day, 7 days a week, 365 days a year to coordinate 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.

Objective: Determine what functional and organizational changes the National Operations Center made to better manage the flow of information following Hurricane Katrina, specifically what new procedures were instituted to ensure that incoming reports are properly reported within the center and to the Secretary. *Office of Inspections*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2008 (Mandatory)

Identifying potential information security threats to DHS' intelligence systems is key in evaluating DHS' intelligence program. The loss or compromise of DHS' intelligence systems or the data contained on those systems can have severe consequences, affecting national security, U.S. citizens, and the department's missions. In response to the increasing threat to information systems and the highly networked nature of the federal computing environment, Congress, in conjunction with the Director National Intelligence, Chief Information Officer, and OMB, requires 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.

Objectives: Perform an independent evaluation of the effectiveness DHS' information security program and practices for its intelligence systems and to also determine what progress DHS has made in resolving weaknesses cited in the prior year's review. *Office of IT Audit*

*Office of Intelligence and Analysis
Carryover Project From FY 2007*

Nominations Process for the Consolidated Terrorist Watchlist

The Intelligence Reform and Terrorism Prevention Act of 2004 requires the Office of the Director of National Intelligence to report to Congress on whether there are consistent standards and adequate processes for maintaining accurate watchlists. As part of a joint review led by the Office of the Director of National Intelligence OIG, we will examine DHS processes for watch list nominations.

Objectives: Determine whether (1) processes and standards for nominating individuals to the consolidated watchlist are articulated, consistent, and understood by nominators; (2) quality control processes help ensure nominations are accurate, understandable, updated, and appropriately inclusive given information available to the components; (3) responsibility for watchlist nominations is effective and understood; (4) nominators receive adequate guidance on the nominations process; (5) agencies maintain sufficient records of their nominations to the National Counterterrorism Center; and (6) components with terrorism information appropriately participate in the nomination process. *Office of Inspections*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2007 (Mandatory)

Identifying potential information security threats to DHS' intelligence systems is key in evaluating DHS' intelligence program. The loss or compromise of DHS' intelligence systems or the data contained on those systems can have severe consequences, affecting national security, U.S. citizens, and the department's missions. In response to the increasing threat to information systems and the highly networked nature of the federal computing environment, Congress, in conjunction with the Director National Intelligence, Chief Information Officer, and OMB, requires 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.

Objective: Perform an independent evaluation of the effectiveness of DHS' information security program and practices for its intelligence systems and to also determine what progress DHS has made in resolving weaknesses cited in the prior year's review. *Office of IT Audit*

TRANSPORTATION SECURITY ADMINISTRATION

TSA's Management of the Surface Transportation Security Inspection Program *(Mandatory)*

The tragic March 11, 2004, rail bombings in Madrid and London starkly illustrate the need to protect rail and other open surface transportation systems. Additionally, derailments of both passenger and freight trains carrying hazardous materials have of the potential for harm. TSA's Surface Transportation Security Inspection Program (STSI) is designed to assist surface transportation carriers, operators, owners, entities, and facilities to enhance their security against terrorist attack and other security threats and enforce applicable surface transportation security regulations and directives. To date, TSA has reportedly deployed approximately 100 STSI Inspectors nationwide, and assigned them to 20 field offices. STSI Inspectors conduct inspections of key facilities for rail and transit systems to assess transit systems' implementation of core transit security fundamentals and comprehensive security action items; conduct examinations of stakeholder operations, including compliance with security directives; identify security gaps; develop effective practices; and gather information on the system, its operations, and its security resources and initiatives.

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 1304, requires our office to submit by September 30, 2008, a report on the performance and effectiveness of STSI Inspectors. Some in Congress are concerned that the STSI inspection force is not large enough to provide adequate oversight of the thousands of miles of railroad tracks and mass transit lines crisscross the nation. It was reported by the GAO that some mass transit and passenger rail operators have expressed confusion and concern about the role of TSA inspectors and the potential that these inspections could duplicate other federal and state rail inspections.

Objectives: Pursuant to the Act, we will: determine the extent to which (1) TSA provides sufficient oversight of the nation's mass transit systems compliance with TSA's security requirements; (2) TSA's overall methodology for conducting and documenting surface transportation inspections effectively ensures compliance with security regulations; (3) TSA has deployed adequate resources, including the number of Inspectors, to meet the program's mission and objectives; (4) TSA inspectors effectively identify stakeholders' security gaps and develop best practices to enhance security for surface transportation; and (5) the program is meeting its stated goals and objectives. *Office of Audits*

TSA On-Screen Alarm Resolution Protocols for Checked Baggage Screening

TSA established the On-Screen Alarm Resolution Protocol (OSARP), which was put into place by TSA in May 2004 to improve the through-put of checked baggage screened by Explosive Detection Systems (EDS) machines. The protocol allows screeners to examine computer-generated images of the inside of a bag to determine whether a suspicious item or items identified by the EDS machines are in fact harmless, allowing the screener to clear the bag. TSA officials believe the OSARP improves the efficiency of baggage screening and allows the agency to reduce staff used to resolve checked baggage alarms using Explosive Trace Detection.

Objective: Determine the extent to which screeners successfully use OSARP to identify and resolve alarms on threat items on the screens of the EDS machines. *Office of Audits*

Transportation Security Administration Representatives Program

Title 49 USC Section 44934 establishes the position of Transportation Security Administration Representative (TSAR). TSA established the TSAR position for each airport outside the United States at which a representative is necessary for air transportation security. Regulations also require the designation of a TSAR at each airport outside the United States where extraordinary security measures are in place. Among other things, TSARs are responsible for serving as the subject matter expert regarding national transportation security activities in their assigned countries, conducting detailed reviews of foreign governments' national transportation security systems, and assessing conditions, security needs, and any training and technical assistance requirements. There are currently 20 TSARs, located both domestically and internationally, responsible for the implementation of U.S. aviation security regulations for at least 151 airports in 120 countries worldwide.

Objective: Determine how effectively TSARs are ensuring compliance with aviation security requirements at “extraordinary locations” serving as the last point of departure for flights to the United States. *Office of Audits*

Evaluation and Deployment of Explosives Trace Portals

The Explosives Trace Portal (ETP) is a walk-through system for rapidly screening personnel for trace amounts of explosives and its deployed by TSA at 34 airports nationwide. The portal uses sample collection and pre-concentration technology to rapidly force air flows around a passenger and collect vapor and particles. If the portal's alarm sounds, the passenger and his or her property are subject to additional screening. Once cleared, the passenger is free to continue boarding. This technology was evaluated by the Transportation Security Laboratory, the lead organization within DHS' Office of Research and Development, responsible for R&D programs related to civil transportation security. Located in Atlantic City, New Jersey, the mission of the Transportation

Security Laboratory is to anticipate future threats to civil transportation security. In so doing, programs are conducted that accelerate and expand promising technologies to the point of operational test and evaluation, which is then performed by TSA's Office of Security Technology. Operational testing and evaluation of Explosives Trace Portals began in June 2004. TSA stated that by the end of 2006, more than 340 ETPs would be in operation throughout the country. In September 2006, TSA suspended the deployment of ETPs, citing "unanticipated problems," and indicated that the agency was exploring whether to modify, upgrade, or scrap the machines.

Objective: Determine the effectiveness of the Transportation Security Laboratory's evaluation of, and the agency's deployment of, ETP technology. *Office of Audits*

Effectiveness of the Federal Trucking Industry Security Grant Program *(Mandatory)*

Since FY 2003, the Trucking Security Program has provided grants worth more than \$62 million to increase vigilance on the Nation's highways in support of homeland security. Eligibility for trucking security grants is restricted to the Highway Watch[®] Program administered by the American Trucking Association. The Highway Watch[®] Program provides a call center and trains commercial drivers and public safety personnel to identify and report security and safety situations on U.S. roads.

Objectives: Determine the efficacy of the federal trucking industry security grant program, and the need for the program, and its impact on motor carrier security. *Office of Inspections*

TSA's Progress in Securing General Aviation Facilities *(Congressional)*

General aviation, which is the operation of civilian aircraft for purposes such as business, personal, and instructional flying but not commercial passenger transport, accounts for approximately 77% of flights in the United States. The 9/11 Commission concluded that "major vulnerabilities" exist in general aviation security, but the Commission did not make specific recommendations in this area. In 2003 and 2004, TSA worked with the Aviation Security Advisory Committee and industry stakeholders to develop voluntary *Security Guidelines for General Aviation Airports*. However, since the publication of the guidelines, media reports have showed that security at some general aviation airports is easily defeated.

Objectives: Determine the steps TSA and industry stakeholders have taken in the past 3 years to strengthen general aviation security, and, if any, challenges TSA faces in strengthening general aviation security. *Office of Inspections*

TSA's Known Shipper Program *(Congressional)*

To reduce the risk associated with shipping cargo on commercial passenger airplanes, TSA implemented the Known Shipper Program. Under this program, each aircraft operator or indirect air carrier determines the shipper's validity and screens or inspects the cargo. Only shippers who are known in this way—an estimated 1.5 million shippers—may send cargo on passenger airplanes. However, anecdotal reports suggest that cargo from unknown shippers also receives transport on passenger airplanes, in violation of the Known Shipper Program.

Objectives: Determine how well TSA enforces its policies and procedures, to prevent cargo from unknown shippers from being shipped on passenger planes, including for indirect air carriers and retail shipping outlets. *Office of Inspections*

Followup Audit of Network Security at TSA

In our August 2005 report, we identified control weaknesses on TSA's wired-based sensitive but unclassified networks. Specifically, we reported that TSA has not developed adequate policies and procedures and fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, the contingency plan for TSA's network had not been finalized and tested to ensure that critical operations could be restored in the event of emergency. TSA agreed with our findings and recommendations and has taken steps to improve network security.

Objective: Determine what progress TSA has made in implementing effective security controls for its networks. *Office of IT Audit*

Transportation Security Administration Carryover Projects From FY 2007

Administration of the Federal Trucking Industry Security Grant Program *(Mandatory)*

The Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 1542, required our office to submit by November 1, 2007, a report on the Federal Trucking Industry Security Grant Program for FYs 2004 and 2005. Between FY 2003 and FY 2005, the trucking security grants 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. Currently, the Trucking Security Program provides funding for the Highway Watch[®] program via a cooperative agreement with the American Trucking Association. The Highway Watch[®] program is

designed to increase vigilance and enhance awareness on the Nation's highways in support of homeland security.

Objectives: Pursuant to the Act, we will: describe the announcement, application, receipt, review, award, monitoring, and closeout processes for trucking security grants and report the amount obligated or expended under the program for FYs 2004 and 2005 for: (1) infrastructure protection; (2) training; (3) equipment; (4) educational materials; (5) program administration; (6) marketing; and (7) other functions. *Office of Inspections*

TSA's Efforts to Address Workplace Issues and Concerns Through the Office of the Ombudsman and Associated Initiatives

Processes and procedures used by employees both in the private and public sectors to report workplace concerns are a critical internal control and key management tool to identify and address illegal and unethical conduct, waste, fraud, and other workplace issues. Since 2004, TSA employees have been officially voicing their concerns through a variety of channels, about how the agency operates by filing complaints that historically were significantly higher than other federal agencies. Some reports suggest that mistreatment of the TSA screener workforce hampers the ability of Transportation Security Officers (screeners) to effectively do their jobs. TSA has established several key components for employees to resolve various problems using a variety of strategies and resolution techniques, including the Office of the Ombudsman, the Model Workplace Program (MWP), and the Integrated Conflict Management System (ICMS). The Office of the Ombudsman was set up to be an advocate for fair process, procedures, and programs for any employee, supervisor, or manager of TSA. TSA's MWP, established within the Office of the Assistant Administrator for Business Transformation and Culture, is described as the creation of a culture where ideas and issues are raised and resolved respectfully through the implementation of an ICMS. TSA's ICMS is designed to be a pro-active system to address employee issues through enhanced communication, cooperative problem solving, and prevention and better management of conflict. The system was established to provide greater support to the various TSA offices that handle complaints and create a broad program that would address conflict before it became problematic.

Objective: Determine the effectiveness of TSA's Office of the Ombudsman and associated initiatives to identify, analyze, address, and minimize workplace issues and concerns. *Office of Audits*

Airport Baggage and Passenger Screening Penetration

The Aviation and Transportation Security Act requires 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 properly screened reduces the opportunity for terrorists to create harm in the air traffic environment. Our testing will consist of

unannounced undercover tests of Transportation Security Officers and security equipment performance at airports nationwide.

Objective: 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 Nation's airports. *Office of Audits*

Controls Over Screener Uniforms, Badges, and Identification Cards

In early 2007, it was widely reported in the press that thousands of TSA uniforms and badges are missing from various airport locations throughout the United States. TSA disclosed that the agency believes that many have been stolen. One media outlet reported that more than 3,700 identification badges and uniform items have been reported lost or stolen from TSA employees since 2003. Security experts fear that individuals could obtain TSA uniforms for terrorist activities or other illegal purposes. The issue has received significant congressional attention, with one congressman proposing fines for TSA employees who lose or do not return their uniforms and badges.

Objective: Determine the effectiveness of TSA internal controls over TSA screener uniforms and identification badges. *Office of Audits*

TSA Sole Source Acquisitions

TSA is exempt from use of the FAR for supplies and services. Instead, the TSA Acquisition Management System, authorized under the Aviation and Transportation Security Act of 2001, established policy and guidance for TSA to acquire the supplies and services needed to achieve its mission.

TSA policy promotes use of competition to award contracts. TSA may contract with a single source when it is in TSA's best interest and the rational basis is documented. *Single source* is TSA's terminology for acquisitions entered into, or proposed to be entered into, after soliciting and negotiating with only one source. The rational basis may be based on emergencies, standardization, or only one source available to satisfy a requirement within the time required. The amount of documentation required to support a single source acquisition depends on the size, scope, and complexity of the proposed action.

Objectives: Determine whether (1) TSA properly justified less than full and open competition for single source contracts awarded during FY 2006, (2) management controls are in place to ensure that TSA awards single source contracts only in circumstances allowed under the TSA Acquisition Management System and that TSA complies with applicable policies and procedures; (3) for FY 2006 single source contracts, official records comply with the TSA Acquisition Management System requirement, including appropriate concurrences and approvals; and (4) TSA's award of selected single source contracts was appropriate. *Office of Audits*

TSA's Use of the National Deployment Force (Congressional)

In October 2003, TSA established the National Deployment Force (NDF). The NDF 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 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 NDF in ways not intended and at great expense to the federal government.

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

TSA's Management of Aviation Security Activities at Jackson Evers International Airport (Congressional)

A media report in September 2006 alleged that TSA employees in Jackson, Mississippi, claim security at Jackson-Evers International Airport is compromised regularly. The Chairman of the House Committee on Homeland Security requested that we review allegations that employees at the airport improperly compromised the integrity of TSA security inspections, that TSA supervisors allowed potentially dangerous passengers to board commercial aircraft, and that TSA managers at Jackson-Evers International Airport ignore safety procedures in order to protect their jobs and appease airlines flying out of Jackson. We will assess whether the integrity of the passenger screening process employed at Jackson-Evers International Airport ensures adherence to established TSA protocols and processes.

Objectives: Determine whether (1) Transportation Security Officers at Jackson-Evers International Airport received advanced notice of any covert testing; (2) Transportation Security Officers report the discovery of firearms and other dangerous prohibited items as required in TSA policy and directives; and (3) existing processes, which authorize certain individuals to fly armed, need strengthening. *Office of Inspections*

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.

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. *Office of Inspections*

TSA's Security Screening Procedures for Employees at Orlando International Airport (Congressional)

On February 7, 2007, a local media report raised concerns that TSA officers at Orlando International Airport were permitted to enter airport sterile areas without undergoing routine screening procedures. On March 5, 2007, without authority, two airline employees at the airport successfully placed 14 guns onto a commercial airliner. Both were later arrested, one at the airliner's destination of Puerto Rico. Our review will focus on the security screening policies and procedures TSA uses for its own and airport employees as well as outside vendors.

Objective: Determine whether policies and procedures cause the Orlando International Airport to be susceptible to security breaches or vulnerable to the introduction of prohibited items on aircraft or in any other secure areas of the airport. *Office of Inspections*

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

The United States Citizenship and Immigration Service (USCIS) Adjudication Process Part 2

USCIS is responsible for administering 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. In Part 1 of this review, we focused on the intake of applications and petitions to the adjudication process. In Part 2 of this review, we will focus on the eligibility determination procedures.

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. *Office of Audits*

United States Citizenship and Immigration Services Carryover Project From FY 2007

USCIS Adjudication Process Part 1

USCIS is responsible for administering immigration and naturalization functions and establishing policies and priorities for immigration services. USCIS is taking steps to improve its processing of immigration benefit applications and reduce its chronic backlog. Increasingly, USCIS is relying on lockboxes, largely a contracted operation, to receive petitions/applications for various immigration benefits and fees paid for these services. The advent of lockbox use improves controls over the fees collected for the services USCIS provides. Also, USCIS is applying IT to automate its processes. However, the adjudication of benefit applications and petitions is often complex and contentious. Delays and rework in processing often occur because of errors or omissions in applications and petitions requiring additional applicant submissions. Our preliminary review indicated that under recent automation and lockbox initiatives applications continue to be rejected or delayed in processing.

In Part 1 of this review, we will focus on intake of applications and petitions to the adjudication process. In Part 2 of this review, we will focus on the eligibility determination procedures.

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

USCIS Management of Benefit Fraud Referrals to ICE

According to USCIS, ICE's benefits fraud unit declines to investigate about 70% of USCIS referrals, including 100% 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 force and go out into the communities to develop cases, which may raise legal issues since USCIS has no enforcement authority.

Objectives: Determine: (1) how well USCIS and ICE are defining and dividing the benefits fraud workload and determining the outcome of referrals; and (2) whether the amount of resources used for this mission matches risks and ICE's enforcement strategy. *Office of Inspections*

UNITED STATES COAST GUARD

Missions FY 2007 (Mandatory)

The Homeland Security Act of 2002 directs the IG to conduct an annual review that assesses the performance of all USCG missions, with a particular emphasis on non-homeland security missions. Homeland security missions include Illegal Drug Interdiction; Undocumented Migrant Interdiction; Foreign Fish Enforcement; Ports, Waterways, and Coastal Security; and Defense Readiness. Non-homeland security missions consists of Search and Rescue, Aids to Navigation, Ice Operations, Living Marine Resources, Marine Safety, and Maritime Environmental Protection.

Many of the non-homeland security missions have been severely tested during the response efforts to Hurricane Katrina, which caused severe devastation and flooding to the Gulf Coast states in August 2005. The effects of Hurricane Katrina on USCG's ability to conduct both homeland security and non-homeland security missions will be assessed during this review.

Objective: Determine the extent to which USCG is maintaining its historical level of effort on non-homeland security missions. *Office of Audits*

Acquisition Challenges, USCG Deepwater Program

USCG recognized that immediate changes were needed in its management of major acquisitions. USCG issued its *Blueprint for Acquisition Reform*, which catalogues many of the challenges and risks that have historically impeded the efficient execution of the Deepwater contract. Additionally, while retaining Integrated Coast Guard Systems as the lead system integrator for some assets already in production from the original Deepwater contract, USCG has now assumed the role of lead systems integrator for future procurements under the 43-month contract extension.

We have concerns with USCG's acquisition reform efforts and their ability to serve as the lead systems integrator due to the timeframe and resources required to successfully implement their acquisition reform efforts and increase management and oversight responsibilities. This review is a follow on to the Acquisition Scorecard that was included in our *Semiannual Report to the Congress* issued in May 2007.

Objective: Provide the status of USCG's acquisition reform efforts and newly acquired lead systems integrator role to include USCG's decisions concerning all Deepwater assets. *Office of Audits*

FY 2008 Deepwater Scorecard

We published the first of what will be a series of scorecards identifying the progress made in selected acquisition functions and activities within DHS, including the USCG Deepwater Program. Our focus was on specific areas within acquisition management, specifically, organizational alignment and leadership, policies and processes, financial accountability, acquisition workforce, and knowledge management and information systems. We plan to update the Deepwater Acquisition Scorecard annually.

Objective: Determine the extent to which USCG has made progress in the acquisition function and has addressed the Deepwater cost, schedule, performance, and oversight issues identified in our recent reports. *Office of Audits*

Acquisition of the Medium Range Patrol Aircraft (HC-144), USCG

The Maritime Patrol Aircraft (MPA) is the first major aviation asset to be procured under the Integrated Deepwater System program. ICGS awarded the contract to European Aeronautic Defense and Space for an original procurement order of 35 Casa aircraft, of which the first eight are on contract for production. Designated as HC-144A in the USCG aviation inventory, this aircraft is a replacement for 21 HU-25 Falcons, which will be retired due to aging and obsolescence issues.

The first two aircraft have been delivered to USCG's Aircraft Repair and Supply Center in Elizabeth City, North Carolina, for mission system pallet integration. Following integration of the pallet, it will enter its operational test and evaluation phase at USCG Aviation Training Center in Mobile, Alabama, and is scheduled to enter operational service in late 2007.

Objective: Determine the extent to which the MPA will meet the cost, schedule, and performance requirements contained in the Deepwater Program contract. *Office of Audits*

Deepwater C4ISR Systems, USCG

We conducted a review of USCG's efforts to design and implement command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to support the Integrated Deepwater System program. The review, which was completed in August 2006, determined that USCG's efforts to oversee the development of its C4ISR systems needed improvement. Specifically, the USCG had done a poor job identifying, implementing, and enforcing C4ISR system requirements. As a result, testing, certification, and accreditation of key Deepwater C4ISR systems was difficult to achieve, thereby placing systems security and operations at risk.

USCG continues to encounter challenges in the development and deployment of key Deepwater C4ISR systems. For example, USCG has identified scores of instances where

C4ISR system components installed aboard its 378', 270', 210' cutters fleets are either obsolete (unsupportable by the original equipment manufacturer) or nearing the end of their service life (support through spares attrition only). Similar issues were also identified (to varying degrees) with the Deepwater Short Range Prosecutor (SRP), the Long Range Interceptor, the 123' patrol boat, and the National Security Cutter (NSC). It is not yet clear the extent to which the problem extends to shoreside C4ISR installations. If this situation is not remedied, USCG could soon experience difficulty meeting and maintaining the readiness and operational capability of its cutter, patrol boat, and small boat fleets. System obsolescence also increases life cycle costs over the service life of these assets.

Objective: Determine the extent to which system obsolescence is impacting the operational readiness and performance of C4ISR systems installed by the Deepwater Program. *Office of Audits*

USCG EA Implementation Process

The DHS EA framework establishes the roadmap to achieve an agency's mission through optimal performance of its core business processes within an efficient IT environment. EAs are blueprints for systematically and completely defining an organization's current and desired environment. EAs are essential for evolving information systems and developing new systems that optimize their mission value. We will evaluate how the USCG's EA framework maps to the DHS EA 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 framework.

Objectives: Determine the level of compliance with established federal guidance and DHS EA policies and procedures, and to determine whether or not the USCG has aligned their strategic plans and individual business priorities within an appropriate EA framework. *Office of IT Audit*

USCG IT Management

USCG is a multi-mission maritime service and one of the Nation's five Armed Services. USCG uses myriad IT capabilities to support its mission of saving lives and property at sea; protecting America's maritime borders and suppressing violations of the law; protecting our maritime environment; providing a safe, efficient marine transportation system; and defending the Nation. With more than 95,000 miles of coastline and more than 350 commercial ports, USCG is the lead federal agency for maritime border security.

Objective: Determine the effectiveness of USCG's research, acquisition, implementation and use of technology to support its maritime mission. *Office of IT Audit*

Followup Audit of Network Security at USCG

In our August 2005 report, we identified weaknesses in USCG's wire-based sensitive but unclassified networks. Specifically, we reported that USCG has not developed policies or procedures and fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, the contingency plan for USCG's network had not been tested. Our vulnerability assessments identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices, and inconsistent configuration and patch management. USCG agreed with our findings and recommendations and has taken steps to improve network security.

Objective: Determine what progress USCG has made in implementing effective security controls for its networks. *Office of IT Audit*

United States Coast Guard Carryover Projects From FY 2007

Maintenance, Rehabilitation, and Upgrading of Shore Facilities in Support of USCG Missions

The USCG occupies more than 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 shoreside 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 (SFRL), 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 SFRL are divided into three categories: major AC&I (projects valued at more than \$1.5M), minor AC&I (projects valued between \$200,000 and \$1.5M), and housing AC&I (any value).

The typical AC&I project requires 5 to 7 years to complete: 3 years to plan, 2 years to obtain funding and complete the design, and another 1 to 2 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.

Objectives: Determine the extent to which (1) the USCG is properly maintaining and rehabilitating shore facilities in support of USCG missions, and (2) the condition of these shore facilities is adversely impacting asset readiness, asset service life, and overall mission performance. *Office of Audits*

USCG Mission Performance FY 2006 (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.

Objective: Determine the extent to which the USCG used its resource hours to perform its homeland security and non-homeland security missions, and met its mission performance goals for FY 2001 through FY 2006. *Office of Audits*

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 decisionmaking 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 whether 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.

Objectives: Determine the extent to which the Coast Guard has: (1) implemented a methodology that is capable of identifying all high interest vessels, cargoes and crews

before they are permitted to enter U.S. ports; (2) accessed and evaluated all available intelligence needed to target high interest vessels in a timely and effective manner; and, (3) incorporated all applicable intelligence into the HIV designation and response process. *Office of Audits*

Marine Casualty Investigation Program, USCG (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.

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. *Office of Audits*

Plan for Improving Accountability, Deepwater Acquisition Program (Congressional)

During hearings conducted during the spring and summer of FY 2007, Congress expressed deep concern regarding the cost, schedule, and performance of key assets to be delivered by the Deepwater Acquisition Program.

Over the past 6 months, USCG has announced that two separate cutters being modernized or acquired under the Deepwater contract were not meeting the structural design and performance requirement outlined in the Deepwater contract. These problems have resulted in the withdrawal of cutters from service and a decision by USCG to temporarily suspend Fast Response Cutter (FRC) design efforts and to seek a commercial off-the-shelf replacement. As of December 31, 2006, USCG had obligated more than \$113 million toward these two acquisitions.

On January 29, 2007, the DHS IG issued a report documenting serious crew safety and structural design issues with the NSC. Specifically, due to design deficiencies, the NSC's structure provides insufficient fatigue strength to be deployed underway for 230 days per year over its 30-year operational service life under Caribbean (General Atlantic) and Gulf of Alaska (North Pacific) sea conditions. The report also indicates that USCG technical experts believe the NSC's design deficiencies could, if left uncorrected, increase the cutter's maintenance costs and reduce its service life.

The structural design and performance issues associated with the 123' patrol boat, the FRC, and the NSC will further undermine USCG's ability to perform its Deepwater and Homeland Security missions as well as cost American taxpayers hundreds of millions of dollars to remedy.

Objectives: Determine what: (1) actions USCG has taken or plans to take to make the ICGS integrator accountable for failures associated with the 110'/123' Modernization Project, the acquisition of the FRC, SRP, and NSC; and (2) plans USCG has developed to address operational gaps resulting from asset failures for these selected assets. *Office of Audits*

Acquisition of the 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 NSC as part of the maritime security cutter "force package." The revised Deepwater plan projects the 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.

Objective: Determine to what extent USCG's oversight role and decisionmaking authority was effective in ensuring VUAVs are completed on time and within budget and achieve established operational capabilities. *Office of Audits*

UNITED STATES CUSTOMS AND BORDER PROTECTION

Secure Border Initiative and SBInet 2008 Program Monitoring *(Mandatory)*

The Secure Border Initiative (SBI) was created in September 2005 to provide a comprehensive approach to border security and illegal immigration. A portion of CBP efforts focus on a major systems acquisition program to modernize border patrol operations, called SBInet. The SBInet program is charged with developing and deploying new technology, infrastructure, and tactics to gain effective control of our Nation's borders. In September 2006, CBP competitively awarded a systems integration contract to the Boeing Company. CBP is planning additional SBInet contract actions. The teams assigned will monitor the program's status and the department's progress in building management capacity and provide oversight of SBInet contracts actions, including interagency agreements.

Objectives: Determine whether CBP has implemented effective cost, schedule, and technical performance controls and appropriate risk management processes. *Office of Audits*

Use of Contractor Support Services *(Mandatory)*

The SBI is a comprehensive effort to secure our borders that includes CBP's program to modernize border patrol operations called SBInet. SBInet 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. In September 2006, CBP competitively awarded a systems integration contract to the Boeing Company. CBP is planning additional SBInet contract actions. 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. The team assigned will monitor the department's progress in building management and oversight capacity of SBInet contracts, focusing on the use of contractors, their roles and responsibilities, and examining the performance of inherently governmental functions within the SBI and SBInet program offices.

Objectives: Determine the extent and risks of CBP's reliance on contractor support services for inherently governmental functions, and its compliance with policy and regulations on use of contractor support services. *Office of Audits*

CBP's SBInet Tactical Infrastructure for Northern Border (Mandatory)

CBP's Office of Border Patrol is responsible for controlling our Nation's borders between the ports of entry. The Border Patrol relies on the use of tactical infrastructure, such as fencing, vehicle barriers, high-intensity lighting and roads to deter and channel illegal entries to areas optimal for detection and apprehension. CBP and its SBInet program are charged with implementing the Secure Fence Act. The Secure Fence Act of 2006 directed DHS to achieve operational control of the entire international border of the United States, specifying tactical infrastructure construction on the southwest border while requiring a feasibility study of an infrastructure security system along the northern land and maritime border of the United States. The study is to cover the necessity, feasibility, and economic impact of implementing an infrastructure security system along the northern border and the study report is due to Congress in early FY 2008. During hearings in March 2007, the Congress also expressed concern about the vulnerability and lack of action on the northern border to prevent the entry of terrorists.

Objectives: Determine whether CBP is (1) properly evaluating the tactical infrastructure needs for the northern United States border as required by the Secure Fence Act, and (2) effectively planning, prioritizing, and coordinating the tactical infrastructure projects for the northern border. *Office of Audits*

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

The Coast Guard and Maritime Transportation Act of 2004, Public Law 108-293, Section 809 (c), 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 Section 70116 of title 46, United States Code. Section 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 the OIG to submit to the Congress, one year after the plan is issued, an evaluation of the progress made by DHS in implementing the plan.

Objective: Determine DHS' progress in implementing its plan to secure systems of international intermodal transportation. *Office of Audits*

Effectiveness of Targeting System for International Cargo Containers (Mandatory)

CBP is developing the Automated Commercial Environment (ACE), a new system to modernize the targeting, inspection, enforcement, border security, revenue collection, and trade statistics processes for all cargo entering and leaving the United States. The system was started in August 2001 and is scheduled for completion in 2011 at an estimated cost of \$3.3 billion.

One portion of the system is a cargo selectivity and targeting module that will modernize and consolidate the legacy targeting systems. CBP's automated targeting capabilities are essential to identify the high-risk cargo that warrants physical screening and inspection. CBP uses the targeting system to identify those containers that pose a higher risk as it screens more than 10 million containers that arrive annually. CBP officers physically inspect the high-risk containers for terrorism-related materials.

The Coast Guard and Maritime Transportation Act of 2004, Public Law 108-293, Section 809 (g), requires the IG to evaluate and report on the effectiveness of the cargo inspection targeting system for detecting international cargo containers potentially being used for acts of terrorism.

Objective: Determine the effectiveness of CBP's targeting system used to identify cargo containers at risk for terrorism. *Office of Audits*

Cash Collections and Deposits

CBP collects \$3.2 billion in cash and checks annually. The remaining 90% of CBP revenue is collected and deposited electronically. CBP is trying to reduce cash collections because of the higher risk and cost associated with handling money. Cash is more susceptible to loss or theft than electronic payments.

The Revenue Division is in the process of installing new electronic cash registers in 76 locations to replace older equipment. The electronic cash registers are integrated with the mainframe revenue system, the Electronic Collection System (ECS). It also provides a tracking mechanism whereby CBP can identify the cash register, employee, transaction amount, and transaction type. CBP collects cash three ways. First, CBP officers process collections using electronic cash registers that are integrated with ECS. Second, locations that do not have electronic cash registers use standalone cash registers. Third, CBP Officers use serially numbered forms as receipts for cash and checks collected from passengers and importers. The Revenue Division monitors the serially numbered forms through Coordinators and Form Control Officers at the ports.

Objective: Determine the effectiveness of CBP's internal controls for receipting, storing, transporting, recording, and depositing cash collections. *Office of Audits*

Small Vessel Security

Small vessels can be used to smuggle narcotics, illegal aliens, and other contraband into the United States, and pose a terrorist threat. On June 19-20, 2007, DHS held a National Small Vessel Security Summit with a select group of small vessel maritime stakeholders and top federal, state, and local government officials to discuss concerns and issues posed by small vessels being used by terrorists in U.S. waters. The Secretary of DHS, the Commandant of the USCG, the Commissioner of the CBP, and the Director of the Domestic Nuclear Detection Office attended the summit. The Summit was intended to compile information to be used in national-level decisions involving the development of small vessel security measures to detect, deter, interdict, and defeat terrorist use of small vessels in U.S. waters.

Operators of small pleasure vessels arriving in the United States from a foreign port or that met another vessel or received merchandise outside U.S. territorial waters, are required to report their arrival to CBP. CBP may direct the vessel to a nearby port of entry to satisfy the face-to-face requirement, or to another location. There are four programs that may exempt participants from the face-to-face inspection at a designated reporting location. CBP tracks these reports using the Pleasure Boat Reporting System.

Objective: Determine the effectiveness of DHS requirements and capabilities to prevent the use of small vessels to smuggle illegal people or goods into the United States. *Office of Audits*

Automated Commercial Environment

The ACE Secure Data Portal is a customized computer screen similar to a website home page that connects CBP, the trade community, and other government agencies by providing a single, centralized, online 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 online access point to ACE, is accessible to more than 1,000 CBP and trade community users. By providing the right information, tools, and foresight, ACE will be a critical element for trade enforcement and in preventing cargo from becoming an instrument of terrorism.

Objectives: Determine whether DHS has implemented proper and effective security controls over ACE to ensure the efficient collection, processing, and analysis of commercial import and export data, including security acceptance testing performed by ACE sites when new technologies, system interfaces, or increments are deployed. *Office of IT Audit*

Treasury Enforcement Communication System Database Security

Treasury Enforcement Communication System (TECS) is a mainframe application that supports customs enforcement, which is comprised of CBP and ICE enforcement and inspection operations. TECS is used to track and process data on suspect individuals, businesses, vehicles, aircraft, and vessels entering the United States by sea, air, or land, and is accessed by Customs Officers through the CBP network while performing their duties at sea, air, and land ports of entry. TECS comprises numerous interrelated CBP applications that provide law enforcement support and data/information storage services for DHS and other external federal agencies that perform law enforcement functions.

Objective: Determine whether CBP has implemented proper and effective controls over sensitive data contained in its mission critical databases. *Office of IT Audit*

Secure Border Initiative IT Approach

In September 2006, DHS announced that it had awarded a 3-year contract to the Boeing Corporation to implement the SBI, a program to safeguard U.S. borders and reduce illegal immigration. Boeing will provide an array of communications systems, sensors, IT, and command and control capabilities to enhance situational awareness. The Boeing solution also will include development of a common operating picture that will provide uniform data, through a command center environment, to all DHS agencies. The common operating picture will support systems interoperability with stakeholders external to DHS.

Objectives: Determine whether DHS is properly planning, acquiring, and managing technology according to federal requirements to accomplish SBI program objectives. *Office of IT Audit*

TECS Modernization

TECS plays an essential role in the screening of travelers entering the United States and in supporting the screening requirements of other federal agencies. DHS is planning to modernize TECS, and develop an updated system that will reduce chances of missing someone on a watch list due to issues associated with transcription from other alphabets; improve information sharing with other agencies, foreign governments, and DHS components resulting in fewer incorrect admission decision; and increase availability of TECS for primary and secondary operations at the border as well as watch list services for all DHS components.

Objective: Determine whether CBP's approach to developing and deploying a modernized replacement for TECS is being carried out in an effective and efficient manner. *Office of IT Audit*

United States Customs and Border Protection Carryover Projects From FY 2007

SBIInet Small Business Opportunities *(Mandatory)*

The SBI is a comprehensive effort to secure our borders that includes CBP's program to modernize border patrol operations called SBIInet. 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. In September 2006, CBP competitively awarded a systems integration contract to the Boeing Company. CBP is planning additional SBIInet contract actions. The teams assigned will assess whether CBP has effectively provided small business opportunities in pursuit of SBIInet contract actions. The FY 2007 Homeland Security Appropriations Conference Report called for the IG to review and report on SBI contract actions. Congressional concerns about SBI acquisitions had been expressed as early as November 2005, with the introduction of the Secure Border Initiative Accountability Act of 2005; specific concerns include compliance with regulation and policy promoting competition and small business opportunities.

Objective: Determine whether SBIInet contracting strategies provide access to small business. *Office of Audits*

Implementation of the Secure Fence Act of 2006 *(Mandatory)*

As part of the tactical infrastructure deployed under SBIInet, CBP is challenged to construct the physical barriers required under the Secure Fence Act of 2006 for specific stretches of the southwest border. The Secure Fence Act of 2006 is driving the extent of infrastructure applied in the SBIInet mix of technology, infrastructure, personnel, and tactics CBP is deploying to control the border. Although a systems integration contract for SBIInet was awarded to the Boeing Company in 2006, CBP retained the option to use traditional sources of supply for its construction needs, including the Army Corps of Engineers, National Guard, and GSA. Such interagency support has not always accomplished expected results as shown in prior audits, as well as, the SBIInet program's lessons learned process. The team assigned will monitor the program's status and provide oversight of SBIInet interagency and intergovernmental support agreements.

Objectives: Determine whether CBP has (1) made progress and is on target to meet the construction requirements as set forth in the Secure Fence Act; (2) properly planned and coordinated tactical infrastructure projects along the southwest border; and, (3) established effective oversight and controls for these projects. *Office of Audits*

Border Patrol Facilities (Mandatory)

In addition to the tactical infrastructure deployed under SBInet, CBP is challenged to provide the facilities to support the expansion of the Border Patrol. Although a systems integration contract for SBInet was awarded to the Boeing Company in 2006, CBP retained option to use traditional sources of supply for its construction needs, including the Army Corps of Engineers, National Guard, and GSA. Such interagency support has not always accomplished expected results as shown in prior audits, as well as, the SBInet program's lessons learned process. The team assigned will monitor the program's status and provide oversight of SBInet interagency and intergovernmental support agreements.

Objectives: Determine whether CBP has (1) properly planned and coordinated Border Patrol facilities construction projects along the southwest border, and (2) established effective oversight and controls for these projects. *Office of Audits*

Recruiting, Hiring, and Training of Border Patrol Agents

The priority mission of the Border Patrol is preventing terrorists and terrorists' weapons, including weapons of mass destruction, from entering the United States. The Border Patrol is responsible for patrolling nearly 6,000 miles of Mexican and Canadian international land borders and more than 2,000 miles of coastal waters surrounding the Florida Peninsula and the island of Puerto Rico. Border Patrol agents work around the clock on assignments, in all types of terrain and weather conditions, often in isolated areas.

In 2006, President Bush announced his commitment to hire an additional 6,000 Border Patrol agents by the end of 2008, bringing Border Patrol's total strength to more than 18,000 agents. Before CBP can hire the additional Border Patrol agents, they must first recruit sufficient numbers of applicants for the position of Border Patrol agent. Before appointment, recruits are screened and must undergo and satisfactorily complete a background investigation. Finally, each Border Patrol agent trainee must complete an 81-day resident course of instruction in integrated law, physical training, firearms instruction, driving, and Spanish. Border Patrol trainees must maintain a passing score in all courses of instruction in order to be retained.

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

CBP's Aircraft Fleet Modernization

CBP protects the American people and critical infrastructure by using an integrated and coordinated air fleet to detect, monitor, intercept, and track suspect conveyances involved with illegal movement of people, illicit drugs, and other contraband thereby preventing

acts of terrorism from arising. CBP has 41 Air Branches and Units, including two P-3 Operations Centers.

In FY 2008, CBP requested more than \$350 million for their strategic objective to modernize the fleet to 220 aircraft of eight different types. This effort has significant impact on safety, maintenance cost, operational readiness, and mission effectiveness. Currently, the CBP air fleet consists of 267 aircraft of 19 different types. The average age of a CBP aircraft is 22 years, while some aircraft in the P-3 fleet are more than 40 years old. The P-3s conduct domestic air security and crisis response missions, as well as, air detection and monitoring missions in drug source and transit zones, including South and Central America, the Eastern Pacific, and the Caribbean, under the aegis of the Joint Interagency Task Force-South, a unit of the U.S. Southern Command.

In 2006, CBP air wings flew more than 90,000 mission hours in support of national border security operations. CBP air assets were directly involved in the apprehension of 204,665 undocumented aliens; 925 criminal arrests; and the seizure of 200,000 pounds of narcotics, 4 aircraft, 26 marine vessels, 140 vehicles, and more than \$105 million in currency.

Objectives: Determine the extent to which CBP has coordinated its air fleet strategy with other components to accomplish the overall DHS mission requirements in a cost effective manner. *Office of Audits*

Strategic Trade Centers

CBP has five Strategic Trade Centers (STCs) throughout the country to provide risk analysis, strategic planning, trade targeting, and import pattern monitoring. The STCs are a critical component of CBP's efforts to collect all of the revenue due to the U.S. government.

The Priority Trade Issues assigned to each STC are:

Location	Priority Trade Issues
Los Angeles, CA	International Property Rights
Dallas, TX	Agriculture
Fort Lauderdale, FL	Anti-Dumping
Chicago, IL	Miscellaneous Revenue
New York, NY	Textile

The Chicago STC is responsible for ensuring that CBP Officers collect the revenues due on goods arriving into the United States. To accomplish its mission, the STC performs various activities including the following:

- Targeting companies and commodities for noncompliance with CBP laws via risk assessment methodologies;

- Initiating and preparing impact assessments on new criteria and recommending modification or deletion of criteria;
- Addressing revenue-related allegations, issues, and concerns that the domestic industry and Congress have raised;
- Conducting periodic risk assessments using revenue gap reports, compliance measurement results, and other information to identify material revenue losses; and
- Preparing periodic reports on outstanding bills and protests.

Objective: Determine whether the STCs are improving CBP's ability to collect all of the revenue legally owed to CBP. *Office of Audits*

CBP's Procurement of Untrained Canines (Congressional)

In February 2006, CBP issued a solicitation seeking vendors to provide untrained canines to train for DHS use. 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 websites 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.

Objectives: Determine whether CBP's dog training program is being carried out in effective, efficient, and economic manner, and has had an impact on CBP's revised border protection strategy. *Office of Inspections*

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

Federal Protective Service (FPS) Contract Guard Procurement Process

The FPS is responsible for policing, securing, and ensuring a safe environment in which federal agencies can conduct business at approximately 9,000 facilities nationwide. To provide for the physical safety of government employees and visitors, FPS uses an estimated 1,200 employees and 15,000 contract guards. Our October 2006 audit of FPS contract guard service operations found that FPS did not pay invoices in a timely manner, thereby violating the Prompt Payment Act. Last year, allegations surfaced about the veracity of one guard contractor's operating and billing practices.

Objective: Determine whether FPS has complied with applicable laws, regulations, and guidelines governing its guard services contracts. *Office of Audits*

FPS Long-term Sustainability

FPS continues to face management challenges from its transition from the GSA to DHS in March 2003. FPS operations are funded solely through security fees that FPS charges federal agencies based on their buildings' security levels and needs. Nevertheless, FPS developed a significant budget shortfall for FY 2006 and 2007. Recently, FPS unveiled a risk-based strategy for providing security services and allocating its resources that will reduce the number of employees from 1,200 to 950 through outplacement and attrition.

Objective: Determine whether the operating model being used by FPS, including the mix of employee and contract security guards and funding projections, represents an effective and sustainable long-term strategy to meet FPS mission requirements. *Office of Audits*

ICE Worksite Enforcement– Review of ICE Worksite Enforcement: The March 2007 New Bedford Apprehensions (Congressional)

As part of its worksite enforcement efforts, ICE conducted a search on March 6, 2007, at Michael Bianco, Inc., a New Bedford, Massachusetts, leather maker. ICE arrested five individuals in connection with alleged hiring of illegal aliens and providing fraudulent identification documents to workers at the factory. In addition, ICE interviewed hundreds of employees to determine their alien and immigration status and to place those unlawfully in the United States in administrative removal proceedings. During this process, ICE detained many aliens out of state.

Objectives: Determine (1) whether ICE considered maintaining custody of detained aliens closer to Massachusetts; (2) the number of children who have one or both parents in a detention center as a result of the March search; (3) the number of detainees released because they were a single parent or sole care giver; (4) the number of detainees who were released for humanitarian reasons and criteria for determining such; and (5) whether the detainees had sufficient access to Massachusetts Department of Social Services representatives. Also, we will determine (6) whether ICE reported its findings from its May 2006 investigation to the Department of Defense or other federal organizations; (7) whether those findings affected Michael Bianco, Inc.'s, contract activities; and (8) whether the type of service or product a company provides for a federal entity has an affect on which companies ICE investigates. *Office of Inspections*

United States Immigration and Customs Enforcement Carryover Projects From FY 2007

Detainee Telephone Services Contract

Federal detention standards require that holding facilities provide detainees reasonable and equitable access to telephones for (1) free calls for legal representation and home country consular services, and (2) paid calls to family, friends, and others. The federal government provides these services through a contract for free access to legal services and consulates and sale of debit cards that detainees use to pay for personal calls. The contract specifies maximum rates that the vendor may charge when detainees place calls with their debit cards. The vendor must provide refunds for improper charges. The contract contains other requirements about connection quality and repair timeliness. The federal government does not pay the vendor. Rather, as compensation for providing free calls to legal and consular services, the vendor has the exclusive right to sell debit cards to the detainees. During FY 2006, the federal government held about 300,000 detainees. Based on concerns about the vendor's compliance with several contract requirements, the Assistant Secretary for ICE requested that we audit this contract.

Objective: Determine whether the contractor complied with contract terms and conditions for detainee telephone services. *Office of Audits*

Removal of a Canadian Citizen to Syria (Congressional)

Our office is evaluating the decision by the Immigration and Naturalization Service (INS) to remove a Canadian and Syrian citizen to Syria, where he alleges that he was tortured. The INS at John F. Kennedy 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.

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.
Office of Inspections

Conditions of Detention for ICE Detainees: Special Review of Two Cases Involving Detainee Deaths

Various reports have criticized whether ICE detention standards and oversight result in sufficient guidance to ensure that ICE detainees with symptoms of serious medical conditions receive appropriate and timely care. Untimely or inappropriate care increases the risk of detainee injury and death, plus the risk of preventable harm to all ICE detainees.

Objectives: Determine whether ICE officials and contractors complied with all relevant detention standards, processes, and procedures, particularly the standard for medical care, in the event of a detainee’s death, including notifications to next-of-kin and disposition of property. *Office of Inspections*

ICE's Visa Security Program

On September 26, 2003, the Departments of State (State) and Homeland Security signed a Memorandum of Understanding (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.

Objectives: Determine (1) the effectiveness of interaction and coordination, as well as the competing authorities and procedures in visa screening that result, when DHS Visa Security Officers and Department of State Diplomatic Security Officers and Consular Affairs Anti-Fraud Officers are present in a single embassy or consulate; (2) how the addition of Visa Security Officers in some locations has affected visa security; (3) the adequacy and relevance of training provided to Visa Security Officers; and (4) how the Visa Security Program will be expanded and implemented at additional international locations. *Office of Inspections*

MULTIPLE COMPONENTS

FY 2008 Secure Border Initiative Financial Accountability (Mandatory)

The FY 2007 Homeland Security Appropriations Conference Report called for the Inspector General to review and report on the SBI contract actions. Congressional concerns expressed about SBI acquisitions include ensuring the accomplishment of program objectives; understanding of program's trade-offs of competing cost, schedule, and performance objectives; and ensuring compliance with regulation and policy promoting competition and small business opportunities. Additionally, Congress has expressed concerns that interagency agreements are not properly managed to efficiently accomplish objectives. The FY 2007 SBI Financial Accountability Review identified and assessed the risks and controls over SBI contract actions to ensure accomplishment of program objectives and compliance with applicable regulations and policies. The FY 2008 review updates that assessment and examines selected contract actions for compliance.

Objectives: Determine the effectiveness of controls over SBI contract actions to ensure accomplishment of program objectives and compliance with applicable regulations and policies. *Office of Audits*

Relationship Between the Directorate for National Protection and Programs and FEMA (Congressional)

In October 2006, the Post-Katrina Emergency Management Reform Act transferred several functions from the Preparedness Directorate to FEMA, including the Office of Grants and Training and the U.S. Fire Administration. Combining FEMA and legacy Preparedness Directorate programs, FEMA organized its new National Preparedness division to focus on policy, contingency planning, exercise coordination and evaluation, emergency management training, and hazard mitigation. Outside FEMA, DHS created the Directorate for National Protection and Programs with the remaining functions of the Preparedness Directorate, including infrastructure protection and risk management and analysis.

Objective: Determine how effectively FEMA and the Directorate for National Protection and Programs coordinate challenges with respect to overlapping or shared responsibilities. *Office of Inspections*

DHS' Administrative Procedures for Handling Allegations of Employee Misconduct

To address allegations of criminal, administrative, and ethical misconduct, DHS maintains an extensive internal investigations community. Currently, DHS components, including the OIG, CBP, ICE, and TSA, conduct employee misconduct investigations. This review will assess administrative procedures used by DHS components for handling allegations of employee misconduct.

Inspection Objectives: (1) Determine the current inventory and source of allegations received by DHS components; (2) Evaluate the process used to determine how allegations are assigned, managed, and disposed of; (3) Determine whether procedures used to refer allegations to the Office of Inspector General are in compliance with Management Directive 0810.1; and, (4) Assess the coordination, collaboration, and information sharing among DHS components. *Office of Inspections*

Operational Structure and Coordination of Overseas Missions and Operations

The DHS 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.

Objectives: Determine the adequacy of (1) processes used to select, train, and deploy overseas employees; (2) human, financial, and capital resources in each country to effectively accomplish the component's program goals; and (3) management oversight and internal controls of its international programs and personnel. *Office of Inspections*

Effectiveness of the DHS Traveler Redress Inquiry Program (TRIP) (Congressional)

In January 2006, DHS and the Department of State announced plans to accelerate creation of a process for government-wide traveler screening redress. The DHS TRIP is a voluntary program to provide a one-stop mechanism for individuals to request redress when they believe watchlists or DHS screening programs have led to their being (1) denied or delayed boarding transportation; (2) denied or delayed entry into or departure from the United States at a port of entry; or (3) identified for additional secondary screening at our Nation's transportation facilities, including airports and seaports. DHS TRIP processes the requests for redress or assistance, in coordination with the TSA, CBP, USCIS, ICE, U.S. Visitor and Immigrant Status Indicator Technology Program, DHS Office for Civil Rights and Civil Liberties, DHS Screening Coordination Office, DHS Privacy Office, Department of State, and Federal Bureau of Investigation's Terrorist Screening Center.

Objectives: Determine whether: (1) information is processed and safeguarded as intended; (2) responses to individual requests are processed in a timely manner; and (3) the program has accelerated the correction of erroneous screening information. *Office of Inspections*

DHS Privacy Management

The DHS Privacy Office works with DHS components to build a culture of privacy within DHS. The DHS Privacy Office reviews Systems of Records Notices and Privacy Impact Assessments during the early stages of IT systems development. However, DHS does not currently have a means to rapidly evaluate the high-level management support of privacy programs and assurance of transparency and accountability for privacy practices once operationalized at each of its components. The Privacy Act of 1974, as amended, and the E-Government Act of 2002 require that DHS management protect sensitive, mission-critical data and personally identifiable information contained in its systems of record.

Objectives: Determine, through a series of audits, how effectively DHS and its components are developing and implementing privacy programs to protect personally identifiable information. *Office of IT Audit*

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 decisionmakers. 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.

Objective: Determine the effectiveness of DHS efforts to manage its various data mining programs in support of the agency's mission. *Office of IT Audit*

Multiple Components Carryover Projects From FY 2007

FY 2007 Secure Border Initiative Financial Accountability (Mandatory)

The FY 2007 Homeland Security Appropriations Conference Report called for the IG to review and report on the SBI contract actions. Congressional concerns about SBI acquisitions had been expressed as early as November 2005 with the introduction of the Secure Border Initiative Accountability Act of 2005. Concerns about accomplishment of program objectives had basis in prior border security initiatives such as the failed Immigration and Naturalization Service Integrated Surveillance Intelligence System. Additionally, compliance with regulation and policy promoting competition and small business opportunities are a continuing concern.

Unlike prior initiatives SBI intends to bring a systems approach to meeting the challenge of border security. SBI seeks to put the right tools in the hands of the men and women on the front lines, facilitate the reduction of administrative and diplomatic obstacles to accomplishing border security missions, ensure that DHS resources are appropriately distributed, and institute systematic efficiencies. For example, ICE and USCIS are two key components of the DHS “layered defense” approach to protecting the Nation and fulfilling the goals of SBI. ICE is responsible for apprehension, detention, and removal of illegal aliens and expansion of worksite enforcement. USCIS leads initiatives for the temporary guest worker program and expanding the employment verification program. Both contribute to a comprehensive solution towards reducing illegal migration, identification of criminal aliens, and increase our Nation’s safety and security from people intent on committing acts of terrorism against the United States. DHS budgets link about \$10 billion a year to SBI. While this includes expanded personnel and operations support, these components, USCG, and the Office of Procurement Operations spend about \$3 billion per year on SBI contracts.

Objective: Determine whether management controls over SBI contract actions are sufficient to ensure accomplishment of program objectives and compliance with applicable regulations and policies. *Office of Audits*

Implementation of OIG Recommendations

As of March 30, 2007, open recommendations from our audit and inspection reports, which require further DHS action, numbered 2,042. Most often, DHS components agree with recommendations and propose actions to implement them, but corrective action occurs over months or years. DHS components are required to provide us with periodic reports of their progress toward closing recommendations.

Objectives: Determine whether OIG and DHS procedures for monitoring and closing recommendations are adequate, and to identify opportunities to increase timely closure of recommendations. *Office of Inspections*

DHS Management of Overseas Operations

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 Security Initiative, 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.

Objectives: Determine the scope and effectiveness of DHS' oversight and policy direction for its overseas authorities and responsibilities, including interagency coordination of operational and resource requirements. *Office of Inspections*

Technical Security Evaluation Program of DHS Work Sites

Information security is an important goal for any organization that depends on information systems and computer networks to carry out its mission. 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 at their respective work sites. Toward that end, we have developed an agency-wide information system security evaluation program.

The Chet Holifield Federal Building, Laguna Niguel, California, was chosen because it is used by several hundred DHS employees from CBP, ICE, and USCIS.

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

Homeland Security Presidential Directive 7 (HSPD-7) Compliance

HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, directs the heads of all federal departments and agencies, by July 2004, to develop and submit to OMB plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans should address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

Objective: Determine the effectiveness of DHS efforts to comply with HSPD-7. *Office of IT Audit*

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

OIG Headquarters Senior Management Team

- Richard L. Skinner** **Inspector General**
- James L. Taylor** **Deputy Inspector General**
- Matt Jadacki** **Deputy Inspector General/Emergency
Management Oversight**
- Richard N. Reback** **Counsel to the Inspector General**
- Anne L. Richards** **Assistant Inspector General/Audits**
- Thomas M. Frost** **Assistant Inspector General/Investigations**
- Carlton I. Mann** **Assistant Inspector General/Inspections**
- Frank Deffer** **Assistant Inspector General/Information
Technology**
- Edward F. Cincinnati** **Assistant Inspector General/Administration**
- Tamara Faulkner** **Congressional Liaison and Media Affairs**
- Denise S. Johnson** **Executive Assistant to the Inspector General**

Locations of Audit Field Offices

Boston, MA

Boston, MA 02222
(617) 565-8700 / Fax (617) 565-8955

Miami, FL

Miramar, FL 33027
(954) 538-7842 / Fax (954) 602-1033

Chicago, IL

Chicago, IL 60603
(312) 886-6300 / Fax (312) 886-6308

Philadelphia, PA

Marlton, NJ 08053-1521
(856) 596-3810 / Fax (856) 810-3412

Houston, TX

Houston, TX 77057
(713) 706-4611 / Fax (713) 706-4625

Locations of Emergency Management Oversight Field Offices

Atlanta, GA

Atlanta, GA 30309
(404) 832-6701 / Fax (404) 832-6645

Oakland, CA

Oakland, CA 94612
(510) 637-4311 / Fax (510) 637-1484

Biloxi, MS

Biloxi, MS 39531
(228) 385-1277 / Fax (228) 385-1714

San Juan, PR

San Juan, PR 00918
(787) 294-2500 / Fax (787) 771-3620

Dallas, TX

Denton, TX 76208
(940) 891-8900 / Fax (940) 891-8948

New Orleans, LA

New Orleans, LA 70114
(504) 762-2164 / Fax (504) 762-2873

Locations of Investigative Field Offices

Arlington, VA

Arlington, VA 22209
(703) 235-0848 / Fax: (703) 235-0854

Atlanta, GA

Atlanta, GA 30341
(404) 832-6730 / Fax: (404) 832-6646

Boston, MA

Boston, MA 02222
(617) 565-8705 / Fax: (617) 565-8995

Buffalo, NY

Buffalo, NY 14202
(716) 551-4231 / Fax: (716) 551-4238

Chicago, IL

Chicago, IL 60603
(312) 886-2800 / Fax: (312) 886-2804

Dallas, TX

Denton, TX 76208
(940) 891-8930 / Fax: (940) 891-8959

Del Rio, TX

Del Rio, TX 78840
(830) 703-7492 / Fax: (830) 703-2065

Detroit, MI

Detroit, MI 48226
(313) 226-2163 / Fax: (313) 226-6405

El Centro, CA

Imperial, CA 92251
(760) 335-3900 / Fax: (760) 335-3726

El Paso, TX

El Paso, TX 79925
(915) 629-1800 / Fax: (915) 594-1330

El Segundo, CA

El Segundo, CA 90245
(310) 665-7320 / Fax: (310) 665-7309

Houston, TX

Houston, TX 77057
(713) 706-4600 / Fax: (713) 706-4622

Laredo, TX

Laredo, TX 78045
(956) 794-2917 / Fax: (956) 717-0395

McAllen, TX

McAllen, TX 78501
(956) 664-8010 / Fax: (956) 618-8151

Miami, FL

Miramar, FL 33027
(954) 538-7555 / Fax: (954) 602-1033

New York City, NY

Jersey City, NJ 07310
(201) 356-1800 / Fax: (201) 356-4038

Oakland, CA

Oakland, CA 94612
(510) 637-4311 / Fax: (510) 637-4327

Orlando, FL

Lake Mary, FL 32746
(407) 804-6399 / Fax: (407) 804-8730

Philadelphia, PA

Marlton, NJ 08053
(856) 596-3800 / Fax: (856) 810-3410

San Diego, CA

San Diego, CA 92101
(619) 235-2501 / Fax: (619) 687-3144

San Juan, PR

San Juan, PR 00918
(787) 294-2500 / Fax: (787) 771-3620

Seattle, WA

Kirkland, WA 98033
(425) 250-1260 / Fax: (425) 576-0898

St. Thomas, VI

(340) 777-1792 / Fax: (340) 777-1803

Tucson, AZ

Tucson, AZ 85741
(520) 229-6420 / Fax: (520) 742-7192

Yuma, AZ

Yuma, AZ 85365
(928) 314-9640 / Fax: (928) 314-9640

Appendix B Acronyms

AC&I	Acquisition Construction and Improvement
ACE	Automated Commercial Environment
CBP	Customs and Border Protection
CCP	Crisis Counseling Program
DAO	Office of Disaster Assistance Oversight
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DNDO	Domestic Nuclear Detection Office
DRF	Disaster Relief Fund
EA	Enterprise Architecture
ECS	Electronic Collection System
EDS	Explosive Detection Systems
EMO	Office of Emergency Management Oversight
ETP	Explosive Detection Personnel Portal
FAR	Federal Acquisition Regulations
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FPS	Federal Protective Service
FRC	Fast Response Cutter
FTE	Full-time equivalent
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HOPE	Helping Our People in Emergencies
HSARPA	Homeland Security Advanced Research Projects Agency
HSIN	Homeland Security Information Network
HSPD-7	Homeland Security Presidential Directive 7
HUD	Department of Housing and Urban Development
IAIP	Information Analysis and Infrastructure Protection
ICE	Immigration and Customs Enforcement
ICMS	Integrated Conflict Management System
IG	Inspector General
INS	Immigration and Naturalization Service
IPA	Independent Public Accounting
IPv6	Internet Protocol version 6
IT	Information Technology
JFO	Joint Field Office
MOU	Memorandum of Understanding
MPA	Maritime Patrol Aircraft
MWP	Model Workplace Program
NCCIPS	National Center for Critical Information Processing and Storage
NCSD	National Cyber Security Division

Appendix B (cont'd)

Acronyms

NDF	National Deployment Force
NEDCTP	National Explosives Detection Canine Team Program
NFIP	National Flood Insurance Program
NSC	National Security Cutter
OCFO	Office of Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OSARP	On-screen Alarm Resolution Protocol
PA	Public Assistance
PCIE/ECIE	President's Council on Integrity and Efficiency
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RAMP	Remedial Action Management Program
S&T	Science and Technology
SAFETY ACT	Support Anti-Terrorism By Fostering Technologies Act
SANS	SysAdmin, Audit, Network, Security Institute
SBI	Secure Border Initiative
SFRL	Shore Facilities Requirements List
SRP	Short Range Prosecutor
STC	Strategic Trade Centers
TAC	Technical Assistance Contract
TECS	Treasury Enforcement Communication System
TH	Transitional Housing
TOI	Targets of Interest
TOPOFF 3	Top Officials Three Exercise
TSA	Transportation Security Administration
TSAR	Transportation Security Administration Representative
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
VUAV	Vertical Take-off and Landing Unmanned Aerial Vehicle
WYO	Write Your Own

Appendix C – FY 2007 Performance Goals, Measures, and Accomplishments

Goal 1. Add value to DHS programs and operations.

- | | | |
|-----|--|------|
| 1.1 | Provide audit and inspection coverage of 75% of DHS' critical mission areas, the President's Management Agenda, and the most serious management challenges facing DHS. | 100% |
| 1.2 | Achieve at least 85% concurrence with recommendations contained in OIG audit and inspection reports (excludes grant audits). | 91% |
| 1.3 | Complete draft reports for at least 75% of inspections and audits within 6 months of the project start date (excludes grant audits). | 55% |

Goal 2. Ensure integrity of DHS programs and operations.

- | | | |
|-----|--|------|
| 2.1 | At least 75% of substantiated investigations are accepted for criminal, civil, or administrative action. | 76% |
| 2.2 | At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions. | 81% |
| 2.3 | Provide audit coverage of \$500 million of DHS' grant programs. | 240% |
| 2.4 | Achieve at least 85% concurrence with recommendations on grant audits. | 62% |

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) 254-4199, fax your request to (202) 254-4305, or visit the OIG website at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse, or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600, Attention:
Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.