DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

FISCAL YEAR 2009

ANNUAL PERFORMANCE PLAN

The Department of Homeland Security

Office of Inspector General

Fiscal Year 2009
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 that 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 2009 Annual Performance Plan* for the Department of Homeland Security's (DHS) Office of Inspector General. This plan, which is our seventh, 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.

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. 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.

Richard L. Skinner
Inspector General

Table of Contents

Chapter **Page**

Chapter 1 – OIG Mission and Responsibilities

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

An Inspector General (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 & Resources

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

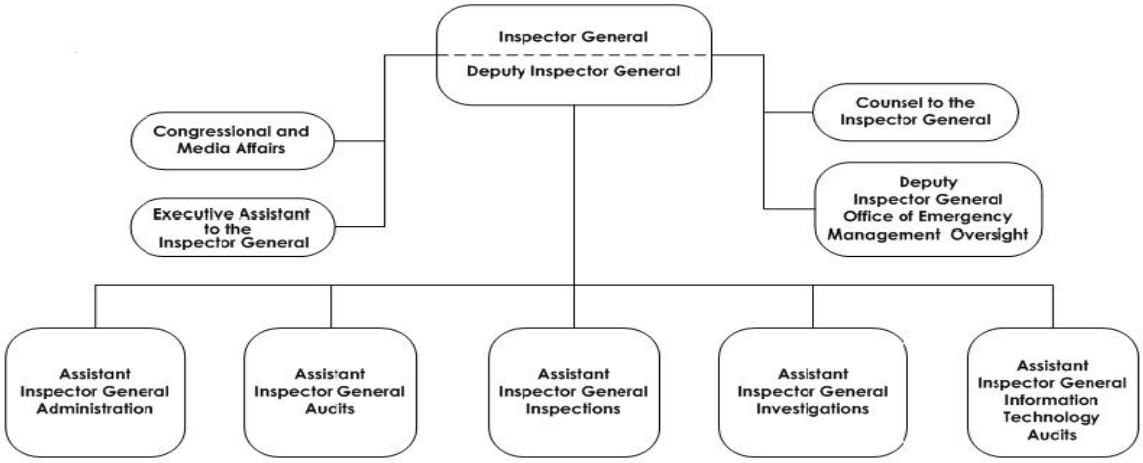

Chart 1: OIG Organization Chart

The OIG consists of the following components:

The Executive Office consists of the IG, the Deputy IG, an executive assistant, and support staff. It provides executive leadership to the OIG.

The Office of Congressional and Media Affairs serves as primary liaison to members of Congress and their staffs, the White House and Executive Branch, the media, and to other federal agencies and governmental entities involved in securing the Nation. The office's staff responds to inquiries from the Congress, the White House, and the media; notifies Congress about OIG initiatives, policies, and programs; and informs other governmental entities about OIG measures that affect their operations and activities. It also provides advice to the IG and supports OIG staff as they address congressional, White House, and media inquiries.

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; serves as 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 determine whether financial accountability is achieved and the final statements are not materially misstated. The office has 171 FTEs.

The Office of Emergency Management Oversight is responsible for providing an aggressive and ongoing audit effort designed to ensure that disaster relief funds (DRF) 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 DHS, the Administrator of the Federal Emergency Management Agency (FEMA), 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. The office has 75 FTEs and temporary employees.

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. Inspections may examine any area of the department, plus it is the lead OIG office 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 Audits 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. The office has 42 FTEs.

The Office of Investigations conducts investigations into allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and programs. These investigations can result in criminal prosecutions, fines, civil monetary

penalties, administrative sanctions, and personnel actions. Additionally, the Office of Investigations provides oversight and monitors the investigative activity of DHS' various internal affairs offices. The office has 189 FTEs, including investigative staff working 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. The office has 41 FTEs.

The President requested an appropriation of $101 million for the OIG in fiscal year (FY) 2009.

Standard Object Classifications		FY 2008 Enacted	FY 2009 President's Budget	FY 2009 Change
11.1	Permanent positions	$ 40,267	$ 45,120	$ 4,853
11.3	Other than permanent	$ 876	$ 1,858	$ 982
11.5	Other personnel compensation	$ 4,787	$ 5,061	$ 274
12.1	Benefits	$ 14,262	$ 15,586	$ 1,324
21.0	Travel	$ 2,995	$ 3,258	$ 263
22.0	Transportation of things	$ 60	$ 65	$ 5
23.1	General Services Administration rent	$ 8,760	$ 8,945	$ 185
23.2	Other rent	$ 337	$ 144	$ (193)
23.3	Communication, utilities, and misc charges	$ 2,477	$ 2,629	$ 152
24.0	Printing	$ 194	$ 204	$ 10
25.1	Advisory & assistance services	$ 5,023	$ 5,277	$ 254
25.2	Other services	$ 989	$ 1,044	$ 55
25.3	Purchase from government accounts	$ 7,431	$ 7,089	$ (342)
25.4	Operation & maintenance of facilities	$ 128	$ 135	$ 7
25.7	Operation & maintenance of equipment	$ 309	$ 324	$ 15
26.0	Supplies & materials	$ 439	$ 469	$ 30
31.0	Equipment	$ 3,227	$ 3,655	$ 428
32.0	Land & structures	$ -	$ -	$ -
42.0	Indemnity	$ -	$ -	$ -
91.0	Unvouchered	$ 150	$ 150	$ -
	Total	**$ 92,711**	**$ 101,013**	**$ 8,302**
Full Time Equivalents		**551**	**577**	**26**

Chapter 3 – FY 2009 Planning Approach

The Annual Performance Plan is our "roadmap" for the audits and the inspections 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 department's stated goals and priorities.

This plan describes more projects than may be completed in FY 2009, 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 2008. Finally, the plan lists some projects that will start during FY 2009, but will carry over into FY 2010.

In establishing priorities, we placed particular emphasis on legislative mandates, such as the *Chief Financial Officers Act* and the *Federal Information Security Management Act of 2002* (FISMA), DHS' strategic goals, the President's Management Agenda, DHS' goals and priorities, congressional priorities, and the most serious management challenges facing the department.

DHS' five goals are:

- Protect Our Nation From Dangerous People,
- Protect Our Nation From Dangerous Goods,
- Protect Critical Infrastructure,
- Strengthen Our Nation's Preparedness and Emergency Response Capabilities, and
- Strengthen and Unify DHS Operations and Management.

In our report titled *Management Challenges Facing the Department of Homeland Security*, we identified the following as the most serious FY 2008 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) nonhomeland 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 – FY 2009 Performance Goals & Measures

We are committed to excellence and to improving DHS and OIG programs and operations. To do this, we establish OIG performance goals, measures, and targets. 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 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. In addition to the mandatory requirements, performance measures identified serve as a basis to assess 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 (excludes grant audits).

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 each 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, and implement 100% of peer review recommendations.

3.2 Ensure that 100% of DHS OIG employees have an annual Individual Development Plan.

3.3 Ensure that 100% of all eligible DHS OIG employees have an Individual Performance Plan and receive an annual Rating of Record.

Chapter 5 – Aligning OIG FY 2009 Projects with DHS' Goals

In the following table, we list DHS' five goals. Underneath each goal, we list our allied FY 2009 projects. The projects and the resulting reports should serve to aid the department in assessing its progress toward achieving its goals. We provide a description of each project and its objectives in Chapter 6.

DHS Goal 1: Protect Our Nation From Dangerous People	
Responsible Directorate/ Component	**Project Title**
CBP	Western Hemisphere Travel Initiative
	FY 2008 Secure Border Initiative Financial Accountability
	The Enforcement Communications Systems Modernization
ICE	ICE's Review of Medical Treatment Requests
Multiple	Intelligence and Information Sharing Among DHS Immigration Components
	Treatment of Unaccompanied Alien Minors
	DHS Employment Verification Programs
	DHS Counterintelligence Activities
TSA	Ability to Communicate With Federal Air Marshals While in Mission Status
USCIS	USCIS Adjudication Process Part 2
	Management Controls to Deter Adjudicator Fraud
Carryover Projects from FY 2008	
CBP	CBP's Northern Border Security Efforts
ICE	Detentions and Deportations Involving the Parents of U.S. Citizen Children
	Transfer of Detainees in ICE Custody
Multiple	Effectiveness of the DHS Traveler Redress Inquiry Program (TRIP)
TSA	Potential Vulnerabilities in TSA's Secure Flight Watchlist Screening

DHS Goal 2: Protect Our Nation From Dangerous Goods

Responsible Directorate/ Component	Project Title
Counter-narcotics	Implementation of the DHS Interagency Statement of Intent for Counternarcotics Enforcement
CBP	CBP's Use of Container Security Initiative Information to Identify and Detect High-Risk Containers Prior to Lading
	Automated Targeting System (ATS) Use in Foreign Ports
TSA	Whole Body Imaging Testing (Red Team)
	Security of Air Cargo During Ground Movement
	Penetration Testing of Law Enforcement Credentials Accepted to Bypass Screening
	TSA's Clear Registered Traveler's Program
Carryover Projects from FY 2008	
CBP	DHS Plan for Implementation of Secure Systems of Transportation
	Progress Report on CBP's Automated Targeting System
TSA	TSA On-Screen Alarm Resolution Protocols for Checked Baggage Screening
	TSA Known Shipper Program

DHS Goal 3: Protect Critical Infrastructure

Responsible Directorate/ Component	Project Title
NPPD	The National Cyber Security Division's Strategy for Control Systems Security
	NCSD's Role in the Trusted Internet Connections Initiative
	The United States Computer Emergency Readiness Team
	Protection of Petroleum and Natural Gas Subsectors
TSA	TSA's Preparedness for Handling Mass Transit Emergencies
USCG	Annual Review of the United States Coast Guard's Mission Performance (FY 2008)
	United States Coast Guard's Acquisition Reorganization
Carryover Projects from FY 2008	
CBP	Small Vessel Security
NPPD	Use and Maintenance of Critical Infrastructure Databases
TSA	TSA Security Regulations Governing General Aviation

DHS Goal 4: Strengthen Our Nation's Preparedness and Emergency Response Capabilities

Responsible Directorate/ Component	Project Title
FEMA	Disaster Assistance Grants (Nationwide)
	Public Assistance Pilot Program
	Public Assistance Appeals Process
	Implementation of Emergency Support Function 6 - Mass Care, Emergency Assistance, Housing and Human Services
	State, Tribal, and Community Level Incident Management Planning Efforts
	FEMA's Strategy to Measure the Effectiveness of Emergency Management Performance Grants
	FEMA's Management, Coordination, and Delivery of Disaster Response Assistance
	FEMA's Incident Management Assistance Teams
	All-Hazards Mitigation Efforts
	FEMA's Progress Implementing Disaster Responders' Credentials
	FEMA's Management of the Emergency Management Performance Grants Program
	Infrastructure Protection Activities Grants Awards
	Flood Map Modernization Followup
Carryover Projects from FY 2008	
FEMA	FEMA's Compliance with the *Flood Insurance Reform Act of 2004*
	FEMA's Public Assistance Pilot Program
	Data Mining to Identify Duplication of Benefits
	Compendium of Federal Disaster Assistance Programs
	FEMA's Exit Strategy for Temporary Housing in the Gulf Coast Region
	FEMA's Hazard Mitigation Grant Program
	Hurricane Katrina: Wind Versus Flood Issues
	FEMA Mission Assignments

DHS Goal 4: Strengthen Our Nation's Preparedness and Emergency Response Capabilities

Responsible Directorate/ Component	Project Title
FEMA	FEMA's Management of Mission Assignments
	Formaldehyde Issues Related to FEMA's Emergency Housing Program
	FEMA's Public Assistance Project Management Process
	FEMA's Disaster Workforce
	FEMA's Public Assistance Program Funding for Hazard Mitigation Measures
	FEMA's Housing Strategy for Future Disasters
	Effectiveness of FEMA's Remedial Action Management Program
	FEMA's Acquisition and Sourcing Strategies for Goods and Services Necessary for Disaster Response
	Federal Incident Management Planning Efforts
	Disaster Closeout Process
	Tracking Public Assistance Insurance Requirements
	FEMA's National Processing Service Center Operations
	State Administration of FEMA's Public Assistance Projects
	FEMA's Temporary Housing Unit Program
	Fire Management Assistance Grant Program
	Federal Disaster Assistance Application Process
	FEMA's Logistics Management Process for Responding to Catastrophic Disasters
	FEMA's Management and Oversight of Public Assistance Technical Assistance Contractors
	States Management of State Homeland Security Grant Program and Urban Areas Security Initiatives Program, Six States to be Determined
	Federal Disaster Relief Assistance Applications and Databases
Intelligence & Analysis	Office of Intelligence and Analysis's Fusion Center Initiative
NPPD	TOPOFF 4 Full-Scale Exercise
Operations Coordination	Information Sharing at the National Operations Center

DHS Goal 5: Strengthen and Unify DHS Operations and Management

Responsible Directorate/ Component	Project Title
CBP	CBP IT Management
	CBP's Actions in Response to Los Angeles International Airport Network Outage
	Information Technology Matters Related to the FY 2008 Financial Statement Audit of CBP
	CBP's Compliance with the *Buy American Act* for Border Fencing
FEMA	Contracting Officer's Technical Representative Program
	FEMA's Enterprise Architecture Implementation Process
	Information Technology Matters Related to the FY 2008 Financial Statement Audit of FEMA
	Eliminating Stove-piped Grant Programs
	Continuing Effort to Evaluate State Management of State Homeland Security Grant Program and Urban Area Security Initiative Programs, States to be Determined
	Automated Deployment Database
	Selected Personnel Practices at FEMA's Maryland National Processing Center
FLETC	Information Technology Matters Related to the FY 2008 Financial Statement Audit of FLETC
Intelligence & Analysis	Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2009 (Two Projects)
	Intelligence Oversight and Quarterly Reporting
Management	FY 2009 Chief Financial Officer Act Audits
	FY 2009 Audit of DHS' Internal Controls over Financial Reporting
	DHS' Internal Controls over Statement of Budgetary Resources (FY 2009)
	Office of National Drug Control Policy Review at CBP, ICE, and USCG
	DHS' Mission Action Plan at OCFO, FEMA, TSA, and USCG
	Acquisition Data Management
	DHS Award Fees
	Annual Evaluation of DHS' Information Security Program for FY 2009
	DHS' IT Plans of Action of Milestones and Implementation of OMB Circular A-123

DHS Goal 5: Strengthen and Unify DHS Operations and Management

Responsible Directorate/ Component	Project Title
Management	Information Technology Matters Related to the FY 2008 Financial Statement Audit
	Plan to Mitigate Components to Standard DHS Financial Systems
	DHS Web Server Security
	DHS Networks' Vulnerability to External Threats and Penetration
	Integrated Wireless Network
	DHS Financial Services Center Security
	Technical Security Evaluation Program for the Port of Buffalo, NY/Canadian Border Crossing
	Followup Review of DHS' Implementation of Homeland Security Presidential Directive 12 (HSPD-12)
Multiple	DHS User Fees
	Protection of Personally Identifiable Information (PII) in DHS Data Mining Programs
	Effectiveness of Contracting Support for S&T
	DHS Spending on Conferences
	Position Management in Selected DHS Internal Affairs Offices
S&T	S&T Management of Contracts with a Small Business
TSA	Information Technology Matters Related to the FY 2008 Financial Statement Audit of TSA
USCG	USCG IT Management
	Information Technology Matters Related to the FY 2008 Financial Statement Audit of USCG
Carryover Projects from FY 2008	
CBP	Refund and Drawback Processes for CBP
	CBP Cash Collections and Deposits Revenue FY 2008
FEMA	FEMA Disaster Acquisition Workforce
	FEMA Acquisition Process
	Internal Control Review of FEMA Acquisitions

DHS Goal 5: Strengthen and Unify DHS Operations and Management

Responsible Directorate/ Component	Project Title
FEMA	FEMA's Property Management
	Contracts Awarded by the Mississippi Transitional Recovery Office
	FEMA's Disaster Relief Fund's Support Accounts
	Selected 2007 Disaster Contracts
	FEMA's Use of Interagency Agreements
	FEMA's Implementation of Federal Regulations Applying to Government Furnished Equipment
ICE	Federal Protective Service Contract Guard Procurement Process
	ICE Contracting and Procurement Overseas
Intelligence & Analysis	Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2008
Management	FY 2008 Chief Financial Officer Act Audits
	FY 2008 Audit of DHS' Internal Controls over Financial Reporting
	DHS' Internal Controls over Statement of Budgetary Resources (FY 2008)
	Office of National Drug Control Policy Reviews at CBP, USCG, and ICE
	DHS' Mission Action Plan Process at OCFO, FEMA, TSA, and USCG
	FEMA's Working Capital Fund
	DHS' Methodology for Cyclical Testing of Internal Controls
	Suspension and Debarment
	Other Than Full and Open Competition Procurements
	LAN A Security and Management Issues
	DHS OneNet
	DHS' IT Disaster Recovery Programs Followup
	Technical Security Evaluation of the National Center for Critical Information Processing and Storage
	The DHS Personnel Security Clearance Program

DHS Goal 5: Strengthen and Unify DHS Operations and Management

Responsible Directorate/ Component	Project Title
Multiple	DHS Component Coordination of Overseas Operations
	Investigative Operations Within the DHS
S&T	S&T's Processes for Funding Research and Development Programs
TSA	TSA Privacy Management

Chapter 6 – Project Narratives

DIRECTORATE FOR MANAGEMENT

FY 2009 Chief Financial Officer Act Audits – Audits of the Consolidated Financial Statements of DHS and the Individual Financial Statements of the United States Custom and Border Protection (CBP), the Federal Law Enforcement Training Center (FLETC), and the Transportation Security Administration (TSA)
(Mandatory)

The *Chief Financial Officers Act* (CFO 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 individual stand-alone audits of CBP, TSA, and FLETC into the consolidated financial statements. Specifically, we will complete the required CFO Act audits related to the consolidated and individual component financial statements:

- DHS Consolidated Audit Report – Opinion on DHS FY 2009 Consolidated Financial Statements – Final Report November 2009
- DHS Consolidated Audit Report – Management Comments Letter – Final Report January 2010
- FEMA Audit Report – Management Comments Letter – Final Report January 2010
- USCG Audit Report – Management Comments Letter – Final Report January 2010
- CBP Audit Report – Opinion on DHS FY 2009 Financial Statements – Final Report December 2009
- FLETC Audit Report – Opinion on DHS FY 2009 Financial Statements – Final Report December 2009
- TSA Audit Report – Opinion on DHS FY 2009 Financial Statements – Final Report December 2009

***Objectives*:** Ascertain and report on the fairness of presentations of DHS' FY 2009 financial statements and FY 2009 financial statements at the individual component level of materiality; obtain an understanding of internal controls over financial reporting, perform tests of those controls to determine audit procedures, and report on weaknesses identified during the audit; perform tests of compliance with certain laws, regulations, and provisions of contracts or grant agreements, noncompliance with which could have a material effect on the financial statements; and, report on noncompliance disclosed by the audit. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

FY 2009 Audit of DHS' Internal Controls over Financial Reporting *(Mandatory)*

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

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 efforts to implement the Circular, and addresses financial performance in the President's Management Agenda.

Objective: Ascertain and report on the effectiveness of DHS' internal controls over financial reporting in conjunction with the FY 2009 DHS consolidated financial statement audit. *Office of Audits*

DHS' Internal Controls over Statement of Budgetary Resources (FY 2009)

Due to the fact that DHS has not been able to obtain an opinion on the balance sheet as part of the financial statement audit, the budgetary accounts receive only limited audit coverage during the financial statement audit. In FY 2008, OIG implemented an additional performance audit to improve internal controls over financial reporting and the auditability of budgetary accounts at the FEMA, Immigration and Customs Enforcement (ICE), Citizenship and Immigration Service (USCIS), the TSA, and USCG.

Objective: Identify where potential internal control improvements can be made that would enhance DHS' ability to provide an assertion on budgetary accounts in the future, i.e., after FY 2008. This assessment will be conducted as a performance audit according to Government Auditing Standards. The audit addresses financial performance in the President's Management Agenda. *Office of Audits*

Office of National Drug Control Policy Review at CBP, ICE, and USCG *(Mandatory)*

Under 21 U.S.C. 1704 (d) and the Office of National Drug Control Policy (ONDCP) Circular, *Drug Control Accounting*, our office is required to perform a review of assertions made by management related to FY 2008 obligations for the National Drug Control Program. We will contract out the ONDCP review of CBP's, ICE's, and USCG's management assertions. This review addresses, in part, financial performance in the President's Management Agenda. We will oversee the reviews of the ONDCP Management Assertions for the following components:

- CBP Audit Report – Review of FY 2009 ONDCP Management Assertions
- CBP Audit Report – Review of FY 2009 ONDCP Performance Summary Report

- ICE Audit Report – Review of FY 2009 ONDCP Management Assertions
- ICE Audit Report – Review of FY 2009 ONDCP Performance Summary Report
- USCG Audit Report – Review of FY 2009 ONDCP Management Assertions
- USCG Audit Report – Review of FY 2009 ONDCP Performance Summary Report

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

DHS' Mission Action Plans at Office of Chief Financial Officer, FEMA, TSA, and USCG

In FY 2006, DHS began a concerted effort to develop management 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. Management action plans are an integral part of implementing OMB Circular A-123 because they identify needed improvements and corresponding remedial actions. We will audit the adequacy of mission action plans for the following components:

- OCFO Audit Report – FY 2010 Mission Action Plans
- FEMA Audit Report – FY 2010 Mission Action Plans
- TSA Audit Report – FY 2010 Mission Action Plans
- USCG Audit Report – FY 2010 of Mission Action Plans
- OCFO Audit Report – Management's implementation of OMB Circular A-123

Objective: Determine the adequacy of and the process for developing competent mission action plans and how this process is integrated into DHS' plan to fully implement OMB Circular A-123 at the Office of the Chief Financial Officer, FEMA, TSA, and USCG. Additionally, this audit will address Management's self-assessment of internal controls and related corrective action plans. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

Acquisition Data Management

DHS has not yet fully deployed a department-wide (enterprise) contract management system that is interfaced with the financial system. Although DHS has begun deployment of Enterprise PRISM Instance, a federalized contract management system, many procurement offices continue to operate using legacy systems that do not interface with financial systems or stand alone versions of PRISM. With eight procurement offices and more than $17 billion in annual acquisitions, the deployment of a consolidated acquisition system would help improve data integrity, reporting, performance measurement, and financial accountability.

Objectives: Determine the extent to which DHS has implemented common systems for managing and reporting acquisition data. Determine the effectiveness of implementation of quality and security controls over acquisition data. *Office of Audits*

DHS Award Fees *(Congressional)*

In response to a request from a member of Congress, we plan to review the practice of award fees by DHS. The requester noted concern about the disconnect between performance and award fees paid to contractors. The requester indicated that DHS appears to be awarding bonuses despite poor performance or without properly evaluating work. This audit will include a review of DHS' use of award fees and compliance with statutory requirements.

Objectives: Determine the extent to which DHS award fee provisions are properly constructed to attain a high caliber of contractor performance. *Office of Audits*

Annual Evaluation of DHS' Information Security Program for Fiscal Year 2009 *(Mandatory)*

In response to the increasing threat to information systems and the highly networked nature of the federal computing environment, Congress, in conjunction with the Office of Management and Budget, requires an annual review and reporting of agencies' compliance with the requirements under 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.

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

DHS' IT Plans of Action of Milestones and Implementation of OMB Circular A-123 *(Mandatory)*

DHS has developed corrective action plans to address numerous material weaknesses in internal control that were identified by the DHS financial statement audit. DHS also has implemented OMB Circular A-123, *Management's Responsibility for Internal Control* (Revised), which requires management to assess and document internal control over financial reporting; identifying needed improvements; taking corresponding corrective action; and making 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 Audits*

IT Matters Related to the FY 2008 Financial Statement Audit – DHS Consolidated ***(Mandatory)***

We contracted with an IPA firm to conduct DHS' annual financial 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 DHS' critical financial systems.

Objective: 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 Audits*

Plan to Migrate Components to Standard DHS Financial Systems

DHS' Transformation and Systems Consolidation program will consolidate 22 component financial systems down to one or two financial solutions. This consolidation effort will include a plan to migrate all DHS components to the new environment.

Objective: Determine the effectiveness of the process that will be used by DHS to migrate DHS components to the new financial systems solutions and determine that security and data transfer issues are properly addressed to ensure that the integrity of the financial information is maintained. *Office of IT Audits*

DHS Web Server Security

Web servers are listed in the top 20 Internet security vulnerabilities by the SysAdmin, Audit, Network, Security Institute. Public websites are hacked on an almost daily basis; and the threat that DHS web servers could be compromised is real. Public web servers continue to be attractive targets for hackers seeking to embarrass organizations or promote a political agenda. Good security practices can protect your site from the risks such compromises create. 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 and applications to protect against unauthorized access. *Office of IT Audits*

DHS Networks' Vulnerability to External Threats and Penetration

The National Institute of Standards and Technology recommends federal agencies to evaluate the effectiveness of security controls implemented on its networks and systems by performing penetration testing annually. A penetration test is the authorized, scheduled, and systematic process of using known vulnerabilities in an attempt to perform an intrusion into host, network, or application resources. The purposes of penetration testing are to identify methods of gaining access to a system by using common tools and techniques used by attackers, and discover and mitigate security vulnerabilities before they can be exploited.

Objective: Determine whether DHS has implemented effective controls over its networks. *Office of IT Audits*

Integrated Wireless Network

Integrated Wireless Network is a secure, wireless, communications network, intended to address federal requirements for ensuring interoperability across federal, state, and local law enforcement partners, at a cost over $5 billion through 2021. Although the Department of Justice is the mandated lead in its development, DHS currently is the largest potential federal user of the system, constituting 64% of all potential users. However, concerns have been raised that DHS flexibility in allocating resources to upgrade its components' legacy communications systems, while still participating in the system, may hinder interagency efforts to create a truly integrated network.

Objectives: Determine the effectiveness of DHS activities to institute an integrated communications network with compliant technology and determine how these efforts relate to the Integrated Wireless Network project jointly conducted with the Departments of Justice and Treasury. *Office of IT Audits*

DHS Financial Services Center Security

The Charleston Regional Center (data center) consists of four multistory buildings formerly owned by the Department of the Navy. They provide space for the Charleston Financial Service Center of the Bureau of Resource Management Global Financial Services (G-FSC) and the Charleston Passport Center. In November 2005, the Phoenix system was hosted at the Financial Services Center under a mutually agreed upon service level agreement designed to implement complete satisfaction of DHS financial and reporting needs. Implementation of this financial management system has allowed for the identification of potential redundancies and plans for better financial management efficiency.

Objective: Determine whether a secure computing environment and platform exists, especially for financial systems, designed to ensure that data confidentiality, integrity, and availability are maintained. *Office of IT Audits*

Technical Security Evaluation Program for the Port of Buffalo, NY/Canadian Border Crossing

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 a program to evaluate information security compliance at DHS work sites.

Objective: Determine whether DHS facilities at the Port of Buffalo, New York, have effective safeguards and comply with technical security standards, controls, and requirements. *Office of IT Audits*

Follow-up Review of DHS' Implementation of Homeland Security Presidential Directive 12

In October 2007, we issued a report entitled *Progress Has Been Made But More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements* (OIG-08-01). In that report, we made recommendations addressing the need for the Program Management Office to implement the following actions:

- Evaluate its implementation plan and take necessary steps to ensure that milestones are met and that further delays are avoided;
- Develop department-wide cost estimates to implement Homeland Security Presidential Directive (HSPD)-12;
- Identify facilities access points and information systems where cards will be required;
- Ensure the proper accreditation of the Personal Identity Verification processes and re-accredit the headquarters PIV Card Issuer services; and
- Certify and accredit information systems used for implementation of HSPD-12 and Federal Information Processing Standards 201 requirements.

As of August 2008, many of the recommendations remain open.

Objective: Determine whether DHS is meeting HSPD-12 implementation requirements and that corrective actions to past recommendations have been completed. *Office of IT Audits*

Directorate for Management
Carryover Projects from FY 2008

FY 2008 Chief Financial Officer Act Audits – Audits of DHS' Consolidated Financial Statements and of CBP's, FLETC's and TSA's Individual Financial Statements ***(Mandatory)***

The *Chief Financial Officers Act* (CFO Act) requires that an annual financial statement audit be performed at DHS. We will contract with an IPA firm to conduct the audit of the DHS consolidated financial statements, including roll-up of the individual stand-alone audits of CBP, TSA, and FLETC into the consolidated financial statements. Specifically, we will complete the required CFO Act audits related to the consolidated and individual component financial statements:

- DHS Consolidated Audit Report – Opinion on DHS FY 2008 Consolidated Financial Statements – Final Report November 2008
- DHS Consolidated Audit Report – Management Comments Letter – Final Report January 2009
- FEMA Audit Report – Management Comments Letter – Final Report January 2009
- USCG Audit Report – Management Comments Letter – Final Report January 2009
- CBP Audit Report – Opinion on DHS FY 2008 Financial Statements – Final Report December 2008
- FLETC Audit Report – Opinion on DHS FY 2008 Financial Statements – Final Report – December 2008
- TSA Audit Report – Opinion on DHS FY 2008 Financial Statements – Final Report December 2008

***Objectives*:** Ascertain and report on the fairness of presentations of DHS' FY 2009 financial statements and FY 2008 financial statements at the individual component level of materiality; 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 Controls 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.

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*

DHS Internal Controls over Statement of Budgetary Resources (FY 2008)

Due to the fact that DHS has not been able to obtain an opinion on the balance sheet as part of the financial statement audit, the budgetary accounts receive only limited audit coverage during the financial statement audit. In FY 2008, OIG implemented an additional performance audit to improve internal controls over financial reporting and the auditability of budgetary accounts at FEMA, ICE, CIS, TSA, and USCG.

Objective: Identify where potential internal control improvements can be made that would enhance DHS' ability to provide an assertion on budgetary accounts in the future, i.e., after FY 2008. This assessment will be conducted as a performance audit according to Government Auditing Standards. The audit addresses financial performance in the President's Management Agenda. *Office of Audits*

ONDCP Reviews at CBP, USCG, and 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 2008 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. We will perform ONDCP reviews for the following operating components:

- CBP Audit Report – Review of FY 2008 ONDCP Management Assertions
- CBP Audit Report – Review of FY 2008 ONDCP Performance Summary Report
- ICE Audit Report – Review of FY 2008 ONDCP Management Assertions
- ICE Audit Report – Review of FY 2008 ONDCP Performance Summary Report
- USCG Audit Report – Review of FY 2008 ONDCP Management Assertions
- USCG Audit Report – Review of FY 2008 ONDCP Performance Summary Report

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

DHS' Mission Action Plan Process at OCFO, FEMA, TSA & USCG

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. We will perform audits of the mission action plan processes at the following operating components:

- OCFO Audit Report – FY 2009 Mission Action Plans
- FEMA Audit Report – FY 2009 Mission Action Plans
- TSA Audit Report – FY 2009 Mission Action Plans
- USCG Audit Report – FY 2009 Mission Action Plans
- OCFO Audit Report – Management's Implementation of OMB Circular A-123

Objectives: Determine the adequacy of and the process for developing competent corrective action plans with detailed and measurable remediation actions. Additionally, provide recommendations to the department on improving Mission Action Plans for the FY 2009 ICOFR playbook. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

FEMA's Working Capital Fund

FEMA uses the Working Capital Fund to support the centralized services provided through selected facilities. The primary customers for the facilities include both FEMA organizations and Other Federal Agencies.

Objectives: Determine the appropriateness of the budget and related WCF costs; and validate the algorithm to determine whether customers are appropriately charged. *Office of Audits*

DHS' Methodology for Cyclical Testing of Internal Controls

DHS' *Internal Control Playbook* for FY 2008 indicates that the Department will implement a multiyear approach to fulfill the OMB Circular A-123 requirements. DHS plans to use materiality calculations and risk-based prioritization to determine which internal control component to address first.

Objectives: Determine whether the methodology used to develop the A-123 implementation plan complies with the OMB Circular A-123 requirements. *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, 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 General Services Administration 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 no suspension or debarment action in FYs 2005 and 2006.

Objectives: Assess the effectiveness of DHS' debarment and suspension procedures for contractors with performance or conduct problems. *Office of Audits*

Other Than Full and Open Competition Procurements ***(Mandatory)***

Competition is presumed to provide the government the best value in obtaining needed supplies and services. Without proper competition, the government may be unable to ensure reasonable cost and performance. Federal regulations provide for noncompetitive acquisitions under certain conditions. Allowable justifications for sole source awards include special programs, such as the 8(a) Business Development Program for small and disadvantaged businesses. When the federal government awards contracts with other than full and open competition, the procuring agency must document its justification in writing and obtain the concurrence and approval of appropriate designated officials.

The House of Representatives included a general provision in the *Department of Homeland Security Appropriations Bill, 2008*, that would limit obligation of funds for contracts and grants unless they are competitively awarded, except during national emergencies. Moreover, past Government Accountability Office and OIG audits identified both improper use of sole source awards and poor cost controls for legitimate sole source awards throughout the government.

We are currently auditing TSA single source awards during FY 2006. *Single source* is TSA's terminology for acquisitions entered into, or proposed to be entered into, after soliciting and negotiating with only one source. During FY 2008, we plan to audit further DHS use of other than full and open competition.

Objectives: Determine whether adequate controls are in place to ensure that DHS uses other than full and open competition only in circumstances allowed under federal regulations and properly justifies its use. *Office of Audits*

LAN A Security and Management Issues

LAN A is the local area network used by DHS headquarters elements in the Washington, DC area. In support of LAN A, the department has entered into a contract agreement to provide information technology support services to DHS headquarters, the department's associate components, select field offices of the department's major components and to other federal, state, and local level government organizations. This agreement consolidates the support services previously provided by multiple vendors. In addition, the DHS SOC has assumed security monitoring and oversight for LAN A.

Objectives: Determine whether contractor performance for LAN A is meeting contract standards and metrics; realizing economies of scale; increasing efficiency and information sharing; generating other administrative and technical benefits resulting in cost savings. In addition, determine whether LAN A security is being ensured through effective monitoring and oversight. *Office of IT Audits*

DHS OneNet

To accomplish their respective missions, DHS and its component organizations rely extensively on IT. For example, in FY 2006, DHS IT funding totaled about $3.64 billion, and in FY 2007 DHS has requested about $4.16 billion. For FY 2006, DHS reported that this funding supported 279 major IT programs. OneNet will replace the fragmented collection component networks merging them into a single infrastructure.

Objective: Determine whether OneNet is providing a secure in-house solution and user driven system to support modern messaging, and secure reliable information sharing. *Office of IT Audits*

DHS' IT Disaster Recovery Programs Follow-up

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 (79%) of the 19 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 Audits*

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: Determine the effectiveness of safeguards and compliance with technical security standards, controls, and requirements. *Office of IT Audits*

The DHS Personnel Security Clearance Program

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, and other employees and contractors; and (4) ensuring agency compliance with its directives, particularly reciprocity. Review DHS' use of investigative authority and how clearance processing time affects program performance. *Office of Inspections*

DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS

The National Cyber Security Division's Strategy for Control Systems Security

One of National Cyber Security Division's (NCSD's) focuses is on securing the Nation's control systems—the virtual and distributed systems that monitor and control sensitive processes and perform vital functions in many of the Nation's critical infrastructures. Because the Nation's controls systems are critical in emergencies and are especially susceptible to cyber security risks and terrorist threats, NCSD, part of DHS' National Protection and Programs Directorate, plays a critical role in helping ensure that these systems are protected. Control systems, for example, are used in providing electric power generation, transmission, and distribution; oil and gas refining; and water treatment and distribution. NCSD helps to secure the cyber systems used in the Nation's critical infrastructures by providing cyber expertise to critical infrastructure sectors, working with vendors to identify critical infrastructure vulnerabilities, sharing information with

infrastructure owners, and providing guidance for securing the critical infrastructure. NCSD plans to release its *Strategy for Control Systems Security* in the summer of 2008.

During FY 2008, NCSD allocated a significant part of its budget to supporting the National Protection and Programs Directorate's mission, including $5 million for its Critical Infrastructure Protection Cyber Security program and $12 million for its Control Systems Security program. Those numbers increase to $6 million and $18 million, respectively, in FY 2009, and $9 million and $28 million, respectively, in FY 2010.

Objective: Determine whether NCSD is ensuring that critical infrastructure sectors adequately assess and address cyber risks on the systems used to run the Nation's critical infrastructures and programs. *Office of IT Audits*

NCSD's Role in the Trusted Internet Connections Initiative

OMB announced the Trusted Internet Connections (TIC) Initiative in November 2007, with the objective of reducing the current number of external federal government connections to internet gateways and portals from thousands to approximately 50. These standardized and optimized external internet connections are called Trusted Internet Connections. By consolidating its connections, the federal government's internet points of presence can be better controlled. NCSD is supporting the implementation of the TIC Initiative. NCSD developed the physical, operational, and technical security requirements an agency must fulfill to serve as a TIC Access Provider, and is responsible, along with OMB, for selecting the agencies to serve as TIC Access Providers. NCSD has allocated $5.7 million to the TIC Initiative for FY 2008, with requests for increased funding in subsequent FYs.

Objective: Evaluate NCSD's role in the TIC Initiative to ensure TICs are securely designed, implemented, and maintained to effectively protect federal networks. *Office of IT Audits*

The United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) was created as a watch and warning mechanism for the federal government's infrastructure by maintaining an awareness of government-wide information security threats and vulnerabilities, and is charged with protecting the Nation's internet infrastructure by coordinating the defense against and response to cyber attacks. Along with supporting its 24x7 incident response mission operations, US-CERT's network physically houses the hardware and software that support the Einstein intrusion detection mechanism and analyses used by federal agency networks, US-CERT's public website, and US-CERT's Secure Portal. US-CERT's public website serves as a source of cyber security information for citizens, private enterprises, information technology professionals, and federal agencies. The Secure Portal provides access to sensitive but unclassified cyber security information used by Information Sharing and Analysis Centers, the government incident response community, and other key vetted stakeholders.

A large portion of NCSD's budget is focused on improving US-CERT facilities and operations. NCSD has allocated $42.9 million toward the US-CERT facility for FY 2008, and an additional $4.9 million in FY 2009. NCSD has also allocated $18 million to support a new backup/redundant US-CERT data center in FY 2008 and dedicated another $14 million in FY 2009.

Objective: Determine the effectiveness of US-CERT operations and whether adequate security controls are in place to secure the US-CERT network and the services it supports, including the US-CERT public website and Secure Portal. *Office of IT Audits*

Protection of Petroleum and Natural Gas Sub-sectors

DHS is responsible for leading, integrating, and coordinating efforts to protect critical infrastructure sectors, eight of which are primarily overseen by other federal departments. The petroleum 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*

Directorate for National Protection and Programs Carryover Projects from FY 2008

Use and Maintenance of Critical Infrastructure Databases ***(Mandatory)***

The National Infrastructure Protection Plan envisions a comprehensive, national inventory of assets to support its risk management framework. A maturing database of national assets is essential to develop a comprehensive picture of the Nation's critical infrastructure and key resources. Furthermore, it can inform DHS decisions about allocating resources to improve homeland security. Our June 2006 report *Progress in Developing the National Asset Database* recommended four improvements to the development and quality of the database. The *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law 110-53, Section 1001, sets additional standards for the database's organization and maintenance. The act requires our office to submit to Congress by August 3, 2009, a report evaluating DHS compliance with its provisions. We also will build on our previous review by assessing the extent to which DHS uses the database to inform programmatic analyses.

Objectives: Determine whether DHS is complying with statutory requirements for the organization and maintenance of the database of national assets and the extent to which

DHS is using the database to support its risk management framework. *Office of Inspections*

TOPOFF 4 Full-Scale Exercise

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. Identifying lessons learned clearly and addressing deficiencies through corrective action plans for local, state, and federal response entities is a vital part of the exercise. These exercises are costly and time-consuming, and they serve as the primary preparation for addressing a real disaster.

Objectives: Determine, in the aftermath of large TOPOFF exercises, whether DHS has an effective process to determine, formulate, and distribute lessons learned and to address remedial needs where deficiencies have been determined to exist. *Office of Inspections*

DIRECTORATE FOR SCIENCE AND TECHNOLOGY

S&T Management of Contracts with a Small Business

Since 1982, the *Small Business Innovation Development Act* requires federal agencies to award 5% of research and development budgets to small businesses. Those small business innovative research (SBIR) awards are designed to assist small businesses to grow their federal research projects into commercial products. To encourage this growth, the Act and federal regulations provide special intellectual property, or data rights, to technology developed under the SBIR funding awards. Under these rights, the government has only restricted data rights to SBIR products for 5 years, limiting its ability to give the technology away.

Objectives: For a selected project, determine whether the Directorate for Science and Technology (S&T) (1) properly followed procurement regulations, SBIR program provisions, and federal ethics rules; and (2) provided appropriate management oversight. *Office of Inspections*

Directorate for Science and Technology Carryover Projects from FY 2008

S&T's Processes for Funding Research and Development Programs

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

Objectives: Determine whether (1) S&T properly defined a process to set its research and development priorities and investments; (2) S&T's decision-making process balances short-term and long-term research; (3) S&T's methodology is fair and equitable for distributing funds for research and development to the national laboratories, academia, and the private sector; and (4) conflicts of interest in the decision-making process are resolved and documented. *Office of Inspections*

FEDERAL EMERGENCY MANAGEMENT AGENCY

Disaster Assistance Grants (Nationwide) – Multiple

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 audits of grantees and subgrantees focusing on grants with the potential for 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 grants awarded under FEMA's Public Assistance (PA) Program, but may include other grant types, such as Hazard Mitigation. FEMA's PA Program provides assistance to states, local governments, and certain nonprofit organizations to repair damages resulting from major disasters or emergencies declared by the President. The PA Program is administered through a coordinated effort between FEMA, the state (grantee), and the subgrantees.

Objective: Determine whether grantees or subgrantees accounted for and expended FEMA funds according to Federal Regulations. *Office of Emergency Management Oversight*

Public Assistance Pilot Program

As a result of the *Post Katrina Emergency Management Reform Act of 2006*, FEMA was authorized to develop a Public Assistance Pilot Program. The Post Katrina Act sets forth three goals for the Public Assistance Pilot Program: (1) reducing the costs to the Federal government of providing assistance to State and local governments; (2) increasing flexibility in grant administration; and (3) expediting the provision of assistance to States and local governments. The Public Assistance Pilot Program specifically addresses the provision of assistance under sections 403(a)(3)(A), 406 and 407 of *The Robert T. Stafford Disaster Relief and Emergency Assistance Act*, 42 U.S.C. 5170b(a)(3)(A), 5172, 5173 (*Stafford Act*). These sections relate to debris removal and the repair, restoration, and replacement of damaged facilities.

Additionally, the legislation recommended new procedures for the administration of public assistance grants and gave FEMA the authority to waive regulations and rules applicable to the provision of assistance. State and local governments may participate in the Public Assistance Pilot Program on a voluntary basis. FEMA's Disaster Assistance Directorate began this pilot program on June 1, 2007, and requested an independent review and opinion on the program as they prepare to evaluate and report to Congress on the results of the program.

Objective: To review the implementation of the pilot program to determine (1) how well the program was executed, (2) whether the pilot program is adequately and equitably implemented across FEMA regions and fair to applicants, and (3) best practices and improvements for program execution in the future. *Office of Emergency Management Oversight*

Public Assistance Appeals Process

Public assistance applicants, subgrantees, or grantees may appeal determinations related to an application for or the provision of federal assistance. The regulations are intended to give applicants, subgrantees, or grantees fair, impartial, and timely consideration of appeals that result from disagreements regarding the scope and cost of disaster-related work. Appeals can be indicative of:

- Incomplete or inadequate inspection of disaster damage,
- Poor project cost estimating,
- Lack of project monitoring as the scope and cost of work increase during project execution, or
- A lack of applicant, subgrantee, or grantee understanding of work eligibility regulations and the allowability and allocability of project costs.

Objectives: (1) Evaluate the causes and cost of adjudicating applicant, subgrantee, or grantee appeals, (2) determine whether FEMA appeal determinations are impartial, comply with public assistance regulations and guidelines, and completed in a timely manner, (3) determine whether the process is cost effective, and (4) identify

improvements FEMA can make to the current process. *Office of Emergency Management Oversight*

Implementation of Emergency Support Function 6 - Mass Care, Emergency Assistance, Housing and Human Services

The Emergency Support Function (ESF) Annexes provide the structure for emergency activity groupings that are most frequently used to provide federal support to states and other federal government agencies during declared disasters and emergencies.

As a result of the *Post Katrina Emergency Management Reform Act of 2006*, the Federal Emergency Management Agency (FEMA) is authorized to lead and coordinate ESF-6 - Mass Care, Emergency Assistance, Housing and Human Services. The legislation requires FEMA to develop and employ a standard operating procedure for ESF-6 that supports the response efforts of federal, state, and local governments and voluntary agencies.

Objectives: Determine (1) to what extent FEMA developed a standard operating procedure for implementing and coordinating each of the four primary functions of ESF-6, (2) to what extent FEMA has coordinated with each of the federal, state, tribal, local and voluntary agencies in developing and implementing its standard operating procedures; and (3) the efficacy of the standard operating procedure of the new ESF-6. *Office of Emergency Management Oversight*

State, Tribal, and Community Level Incident Management Planning Efforts

The premise of the National Response Framework is that incidents begin and end locally and are managed at the lowest possible jurisdiction. As such, it is vital that state, tribal, and local governments have practical, all-hazards plans and supporting procedures, and protocols that address locally identified hazards and risks. The state, tribal, and local planning structure is supported by federal preparedness assistance by FEMA grants such as the Regional Catastrophic Preparedness Grant Program. This structure, in turn, supports the National Response Framework and the federal incident management planning structure by building upon capabilities that augment our national response capacity.

Objectives: Determine whether state, tribal, and local governments have developed plans that align with the 15 planning scenarios and to what extent these plans are integrated and mutually supportive of federal plans. *Office of Emergency Management Oversight*

FEMA's Strategy to Measure the Effectiveness of Emergency Management Performance Grants

Effective, catastrophic all-hazards planning should be of critical importance to state and local jurisdictions. They must engage in comprehensive national and regional planning processes that seek to enhance emergency management and catastrophic capabilities

through strengthened national and regional relationships, and the allocation of resources. Emergency management must be able to coordinate in the context of natural and man-made hazards that threaten the security of the homeland, and the safety and well-being of citizens. An all-hazards approach to preparedness, including the development of a comprehensive program of planning, training, and exercises, sets the stage for an effective and consistent response to any threatened or actual disaster or emergency, regardless of the cause.

As appropriated by the *Fiscal Year 2008 (FY 2008) Department of Homeland Security Appropriations Act* (P.L. 110-161), the FY 2008 Emergency Management Performance Grants (EMPG) will provide $291 million (more than double from 2002) to assist state and local governments to sustain and enhance all-hazards emergency management capabilities. In FY 2008, specific planning focus areas include evacuation planning, logistics and resource management, continuity of operations (COOP)/continuity of government planning, and recovery planning.

Recently, the FEMA Administrator told the Homeland Security Appropriations Subcommittee that FEMA would have a plan to measure the effectiveness of grant funding by August 2008.

Objectives: Determine FEMA's strategy for measuring the effectiveness of EMPG grant funding. Specifically, we will determine whether FEMA has: (1) developed a strategy for evaluating the effectiveness of EMPG grant funding; (2) communicated this strategy to grant recipients; and (3) developed an implementation plan for carrying out the evaluation strategy. We will look at whether the evaluation strategy reflects legislative mandates and goals for the EMPG program, reflects guidance provided by FEMA to grant recipients, and includes verifiable performance measures. *Office of Emergency Management Oversight*

Contracting Officer's Technical Representative Program

Recent OIG and the Government Accountability Office reports indicate that FEMA needs to improve contractor management oversight, including the ability to manage numerous large contracts in major or catastrophic disasters. In the first 3 months of 2008, 15 major disasters have been declared and numerous large initiatives have begun. FEMA has stated that they now have 700 trained Contracting Officer's Technical Representatives (COTRs) to manage these contracts. This review will assess the headquarters COTR program office, and its efforts to establish a structure and train sufficient staff to significantly improve their performance in contractor oversight and contract monitoring.

Objectives: Determine: (1) if policies, procedures, and processes have been established and communicated to all COTRs and are being implemented consistently; (2) if a system of knowledge management and document retention has been implemented and if standardized documentation exists; (3) what training requirements have been established, and how they are being tracked; and (4) if strategies and plans have been developed to staff a catastrophic disaster. *Office of Emergency Management Oversight*

FEMA's Management, Coordination, and Delivery of Disaster Response Assistance

When a disaster occurs, it is essential that FEMA be able to quickly identify, among its prearranged resources, the best source to meet the immediate needs of the affected area and determine whether those resources are efficiently and effectively deployed to the disaster area. Resources may be deployed from a variety of sources including:

- Prepositioned FEMA resources,
- Mission assignments/pre-scripted mission assignments,
- Interagency agreements,
- Advance readiness contracts, and
- State-owned or state-controlled resources.

The mechanisms to activate each of these options should be in place prior to a disaster and must be communicated throughout FEMA so that all stakeholders can act quickly and effectively. Previously we focused on strategy; this audit will focus on implementation.

Objectives: Determine to what extent FEMA has: (1) communicated its strategy for the effective mobilization and deployment of critical resources from a variety of sources to all stakeholders, (2) trained stakeholders in management and coordination of all potential resources, including the use of a reliable and accurate system to determine what resources are available, and which sources they should use to efficiently and effectively deliver needed goods and supplies, (3) developed, tested, and trained staff on systems to track goods and services from requirement definition to delivery, and (4) trained staff on a system to close-out contracts and agreements to ensure billings and payments are accurate, and funds are de-obligated where appropriate. *Office of Emergency Management Oversight*

FEMA's Incident Management Assistance Teams

FEMA is developing the next generation of rapidly deployable interagency emergency response teams to address the requirements of the Post Katrina Emergency Management Reform Act of 2006. The Incident Management Assistance Teams (IMATs) are designed to provide a forward Federal presence to facilitate managing the national response to catastrophic incidents. The primary mission of an IMAT will be to rapidly deploy to an incident or incident-threatened venue, provide leadership in the identification and provision of federal assistance, and coordinate and integrate interjurisdictional response in support of the affected state(s) or United States Territory(ies). The IMATs will support efforts to meet the emergent needs of state and local jurisdictions; possess the capability to provide initial situational awareness for Federal decision-makers; and support the initial establishment of a unified command.

Objectives: To determine (1) the role and capabilities of an IMAT during various types of disasters, (2) when all IMATs will be fully operational, (3) who is responsible for

coordination and management, and (4) their ability to respond within 12 hours, including contingency plans. *Office of Emergency Management Oversight*

All-Hazards Mitigation Efforts

Mitigation means taking actions to reduce the effects of a hazard before it occurs. It includes both the planning and implementation of measures to reduce the risks associated with known natural and human-made hazards, and the process of planning for effective response to disasters that do occur. FEMA's Mitigation Directorate manages a variety of programs designed to reduce future losses to homes, businesses, schools, public buildings and critical facilities from floods, earthquakes, tornadoes, and other natural disasters. The National Response Framework identifies 15 national planning scenarios that represent the gravest dangers facing the United States—ranging from pandemic influenza to terrorist attacks using an improvised explosive device. This review focuses upon FEMA's role, leadership, and contribution to mitigating hazards associated with the 15 national planning scenarios.

Objectives: Determine to what extent FEMA is leading efforts to mitigate all-hazards and evaluate FEMA's role, leadership, and contribution in addressing all necessary tasks and activities to mitigate hazards associated with the 15 national planning scenarios. *Office of Emergency Management Oversight*

FEMA's Progress in Implementing Disaster Responders' Credentials

FEMA, federal, state, and private sector participants continue to express concern over not having a workable identification system. Recent incidents have been cited where responders were denied access to areas where they were needed, as well as truck drivers who were not permitted to deliver emergency supplies because they did not have recognized credentials. Similar situations have occurred prior to, during, and since Hurricane Katrina.

Credentialing is mandated by the National Incident Management System and in accord with Homeland Security Presidential Directive – 5, *Management of Domestic Incidents* to address the needs of federal, state, local, and private sector responders.

Objectives: (1) Determine the status of federal initiatives, (2) determine whether FEMA is actively engaged in implementing a program that facilitates delivery of emergency services, and (3) assess FEMA's plans and timelines for implementing a credentialing program for the emergency management community. *Office of Emergency Management Oversight*

FEMA's Management of the Emergency Management Performance Grants Program

This audit will focus on how FEMA manages the EMPG program, using the grants lifecycle as the framework. We will review FEMA's management regarding program announcement, application receipt and review, award, and post-award oversight.

Objectives: Review FEMA's management of the EMPG program throughout the grant lifecycle, specifically, (1) is the program guidance clear and does it reflect the program's legislative mandate; (2) how are applications reviewed and funding decisions made; (3) does FEMA have the people, processes, and systems in place for making timely and accurate grant awards; and (4) what are FEMA's procedures for monitoring grants post-award. *Office of Emergency Management Oversight*

Infrastructure Protection Activities Grants Awards

In FY 2008 DHS made $844 million dollars available for Infrastructure Protection Activities grants. This grant program includes the Port Security Grant Program, the Transit Security Grant Program (which includes the Freight Rail Security Grant Program and the Intercity Passenger Rail Program), the Trucking Security Grant Program, the Intercity Bus Security Grant Program, and the Buffer Zone Protection Program. The FY 2008 funding level represented a 29% increase in funding over the prior year. Of the grant programs under the Infrastructure Protection Activities, only the Trucking Security Grant Program ($15.5 million) has been audited to date.

These grant programs are at a higher level of risk than many other similar programs because they are not necessarily supported by a state agency. Grant applications can come from private sector owners and funding may be awarded directly to them. Without state involvement, potential Grant recipients may not apply for or be awarded grant funding even though they control a high-risk part of the infrastructure.

Objective: Determine if the FY 2008 grant recipients represent the entities (state, private sector, and multiregional) that are at the highest levels of threat and vulnerability according to current DHS risk assessments. *Office of Audits*

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, our Office of Inspections prepared a report on the Assistance to Firefighters Grant Program (OIG-ISP-01-03, September 2003) and 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 have 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*

Continuing Effort to Evaluate States Management of State Homeland Security Grant Program and Urban Areas Security Initiative Program, States to be Determined ***(Mandatory)***

Public Law 110–53, Implementing Recommendations of the *9/11 Commission Act of 2007*, August 3, 2007, requires us to audit each state that receives State Homeland Security Grant Program and Urban Areas Security Initiative grant funds at least once during the next 7 years. As part of our continuing effort to ensure the effective and appropriate use of grants administered by FEMA, we will evaluate states' and urban areas' management of homeland security funds through the initiation of audits in eight to nine previously unaudited states. Specifically, we will determine whether the funds awarded were used in accordance with the law, program, guidance, and state homeland security plans and other applicable plans. We will also determine the extent to which funds awarded enhanced the ability of a grantee to prevent, prepare for, protect against, and respond to natural disasters, acts of terrorism, and other man-made disasters.

Objectives: Determine the extent that selected states have effectively and efficiently implemented the State Homeland Security Grant Program and, if applicable, the Urban Areas Security Initiative program, achieved the goals of the programs, and spent funds in accordance with grant requirements. *Office of Audits*

FEMA's Enterprise Architecture Implementation Process

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

Objectives: Determine the level of compliance with established Federal guidance and DHS' Enterprise Architecture policies and procedures, and to determine whether FEMA has aligned its strategic plans and individual business priorities within an appropriate Enterprise Architecture framework. *Office of IT Audits*

Information Technology Matters Related to the FY 2008 Financial Statement Audit of FEMA

We contracted with an IPA firm to conduct DHS' annual financial 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 FEMA's critical financial systems.

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

Automated Deployment Database

In September 2005, we reported that FEMA was not able to manage deployment of its disaster response personnel effectively. Specifically, we stated that the automated deployment database lacked integration between other FEMA systems, which prevented FEMA from coordinating people and disaster supplies. Without adequate coordination, personnel arrived at disaster sites and were unable to begin work because the supplies and equipment they needed had not yet arrived, or the supplies arrived without the necessary people to accept and distribute them.

Objectives: Determine the effectiveness of FEMA's efforts to ensure its personnel deployment system can track personnel effectively and integrate with other FEMA IT systems, such as those used for logistics and other disaster management activities. *Office of IT Audits*

Flood Map Modernization Follow-up

In September 2005, we reported FEMA was not managing effectively its 6-year, $1.475 billion flood map modernization program to digitize the approximately 92,000 flood maps that the nation uses to identify flood zones and determine insurance requirements. Specifically, we reported that although FEMA was making progress in the program, its Multi-Year Flood Hazard Plan did not effectively address user and funding needs. Current policies, agreements, and information sharing mechanisms did not effectively support coordination and cooperation among mapping stakeholders. Further, FEMA had made limited progress in developing a web-based mapping system due to unclear contractor expectations, underestimation of program scope and complexity, and, poorly defined requirements, resulting in significant system acquisition delays and cost overruns. Overcoming these program management challenges will be essential to provide the modernized maps needed to guard against floods, among the most frequent and costly of all natural disasters each year.

Objectives: Determine what FEMA has done to help ensure the success of its flood map modernization program by enhancing program planning, guidance, and oversight;

improving coordination with stakeholders; and, defining contractor requirements and methodologies for mapping system development. *Office of IT Audits*

Selected Personnel Practices at FEMA's Maryland National Processing Service Center *(Congressional)*

The Chairman of the House Committee on Homeland Security requested that we review a complaint received from an employee at FEMA's Maryland National Processing Service Center. The employee alleged that the FEMA improperly:

- Concentrated its higher-salaried positions at selected processing centers;
- Terminated employees based on plans to outsource operations; and
- Conducted employee performance evaluations.

Objective: Determine the validity of the allegations. *Office of Inspections*

Federal Emergency Management Agency Carryover Projects from FY 2008

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's disaster acquisition workforce strategy is adequate to satisfy the needs created by 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: Determine the strengths and weaknesses of FEMA's current acquisition process from requirements identification through closeout of the final contract action, and 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*

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 it established procedures for increasing flood insurance premiums for policyholders who decline mitigation offers under the pilot program.

Objectives: Determine to what extent FEMA has implemented strategies to reduce the number of severe, repetitive loss properties through buyouts, elevations, relocations, and flood proofing, and confirm that mitigation activities have been conducted in compliance with statutory and regulatory guidelines and limitations. *Office of Emergency Management Oversight*

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 established and implemented sufficient internal controls over its acquisition management program, and implemented compensating controls when internal controls are waived or bypassed in the event of urgent circumstances. *Office of Emergency Management Oversight*

FEMA's Public Assistance Pilot 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 began to retool its debris removal program and in June 2007, announced its PA pilot program that, among other things, included a debris removal component. We met with officials from FEMA's Disaster Assistance Directorate and modified the audit with the goal of assessing whether the PA pilot program will meet the program's stated goals and whether the program can be adequately evaluated on December 31, 2008, the end of the pilot program period.

Objectives: Determine whether the pilot program will meet the program's stated goals, and whether program evaluation criteria was established to adequately evaluate the program at the end of the pilot. *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 Assistance 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 Mitigation Directorate within FEMA manages the National Flood Insurance Program (NFIP) that provides flood insurance to property owners within participating communities. The maximum coverage that can be obtained is $250,000.

A contractor 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 (NEMIS), and hotels, motels, and apartments are maintained in other databases.

Objectives: Determine whether recipients of FEMA's Disaster Housing home repair grant assistance have also received benefits from the NFIP; and 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*

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 will also be part of this effort.

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

Compendium of Federal Disaster Assistance Programs

We are preparing an inventory of federal disaster assistance programs. This is a high-level review to identify federal disaster benefits provided in the aftermath of a disaster. 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 may be at risk of providing duplicate or overlapping benefits to disaster victims. *Office of Emergency Management Oversight*

FEMA's Exit Strategy for Temporary 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 Temporary 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 5 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 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*

Hurricane Katrina: Wind Versus Flood Issues ***(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, CFR, FEMA has arrangements with individual private sector property insurance companies through the Write Your Own (WYO) program. Participating companies offer flood insurance coverage to eligible applicants and arrange for the adjustment, settlement, payment, and defense of all claims arising from policies of flood insurance issued under this program. The WYO company acts as a fiscal agent of the federal government. When Hurricane Katrina made landfall in August 2005, there was damage from wind and flooding. We will investigate whether, and to what extent, in adjusting and settling claims resulting from Hurricane Katrina, insurers under the WYO program improperly attributed damages to flooding, covered under the insurance provided by the NFIP, rather than to windstorms which are covered under the insurance of the individual private sector property insurers or by 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 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: the Federal Protective Service (FPS), 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*

Formaldehyde Issues Related to FEMA's Emergency Housing Program ***(Mandatory)***

As mandated by Congress, we will investigate FEMA policies and procedures regarding formaldehyde in trailers purchased by the agency to house disaster victims.

Objectives: Determine (1) the process used by FEMA to collect and respond to health and safety concerns of trailer occupants; (2) whether FEMA adequately notified occupants of potential health and safety concerns; and (3) whether FEMA has the proper controls and processes in place to deal with health and safety concerns of those living in trailers following disasters. *Office of Emergency Management Oversight*

Contracts Awarded by the Mississippi Transitional Recovery Office

As of June 12, 2007, FEMA contracting officers at the Mississippi Transitional Recovery Office had awarded 38 contracts totaling an estimated $278 million. These contracts covered a broad range of goods and services including items such as pad leases for temporary housing units, armed guard security, base camps, and meals ready to eat. It is essential that all acquisitions be handled in an efficient, effective, and accountable manner.

Objective: Determine whether contracts awarded by FEMA Mississippi Transitional Recovery Office were awarded and administered according to FAR and FEMA guidelines. *Office of Emergency Management Oversight*

FEMA's Public Assistance Project Management Process ***(Congressional)***

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 Disaster Workforce

One of the critical areas that affected 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 having been performed by the Agency. Following the 2005 hurricane season, FEMA again initiated a study of this subject. In addition to these FEMA-initiated actions, we 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 respond to the next catastrophic disaster.

***Objectives*:** Determine the progress FEMA has made toward 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*

FEMA's Public Assistance Program Funding for Hazard Mitigation Measures

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 Disaster Relief Fund's Support Accounts

FEMA uses the DRF Support Account to fund disaster-related activities that cannot easily be charged to a specific disaster. Expenditures from the Support Account have escalated from $109 million in FY 1997 to over $1 billion in FY 2007. Although Congress intended the DRF to be broad and flexible, this same flexibility makes it difficult to discern whether DRF expenditures should be more appropriately charged to other FEMA appropriations. 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 costs associated with the three 2005 hurricanes, Katrina, Rita, and Wilma, FEMA is required to report only on the DRF as a whole. FEMA is not required to report on DRF subaccounts.

Objectives: To determine whether: (1) FEMA is using the DRF for eligible expenses; (2) funds are accurately tracked; and (3) management controls are in place to prevent and detect misuse of the DRF. *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 determine (1) 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*

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 create a process to transition long-term disaster housing to the Department of Housing and Urban Development. 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 interagency housing coordination; strategic plans for providing emergency housing to future disaster victims; and strategy for addressing the persistent TH issues. *Office of Emergency Management Oversight*

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*

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 establishing mission assignment requirements and identifying appropriate capabilities to fulfill those assignments; and coordinating and monitoring the implementation of mission assignments. *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 Acquisition and Sourcing Strategy for Goods and Services Necessary for Disaster Response

For all incidents, it is essential to prioritize and clearly communicate incident requirements so that resources can be efficiently matched, typed, and mobilized to

support operations. Large-scale events, in particular, may require sophisticated coordination and time-phased deployment of resources from the private sector; nongovernmental organizations; foreign governments and international organizations; and local, tribal, state, and federal government entities. Mobilization and deployment will be most effective when supported by planning that addresses the universe of available resources, including:

- Prepositioned FEMA resources,
- Mission assignments/prescripted mission assignments,
- Interagency agreements,
- Advance readiness contracts, and
- State-owned or state-controlled resources, and a strategy for determining when to use which resources.

Objectives: Determine to what extent FEMA has (1) catalogued key disaster response resources; (2) developed a strategy for the effective mobilization and deployment of critical resources from a variety of sources in response to incidents; (3) developed and tested a system that key stakeholders can readily use to determine what resources are available, and which sources they should use in order to efficiently and effectively send needed goods and supplies; (4) communicated effectively with key stakeholders so that everyone understands the procedures for mobilizing and deploying critical disaster response resources; and (5) developed procedures to minimize unnecessary duplication.

Where sourcing duplication exists, we will conduct case study analyses to determine whether there are major differences in prices/agreements and whether there are guidelines for choosing which source to use. *Office of Emergency Management Oversight*

Federal Incident Management Planning Efforts

The federal incident management planning structure consists of multiple requisites:

- General Guidance;
- National Planning Scenarios;
- Strategic Guidance;
- Federal Interagency Concept Plans;
- Federal Department and Agency Operations Plans; and
- The Secretary's Playbooks, which are detailed checklists that the DHS Secretary uses to ensure a coordinated response to an incident.

In January 2008, DHS released the National Response Framework that provides a general guide to national incident management response. It is now essential that federal plans that support the National Response Framework and federal planning structure be completed.

Objectives: Determine to what extent other planning requisites have been fulfilled within the federal planning structure and to develop a baseline to measure progress in

developing plans that align with each of the fifteen national planning scenarios. *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 no longer be 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*

Tracking Public Assistance Insurance Requirements

According to title 44, CFR 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 the extent to which FEMA and the states monitor and track insurance requirements and whether facilities that were required to maintain insurance, but did not, received assistance a second time. *Office of Emergency Management Oversight*

FEMA's National Processing 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*

State Administration of FEMA's Public Assistance Projects – Multiple State Audits

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 conducing 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 also are 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*

FEMA's Temporary Housing Unit Program - Multiple

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*

Fire Management Assistance Grant Program – Multiple

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*

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 Implementation of Federal Regulations Applying to Government Furnished Equipment

In the Federal Acquisition Regulations 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 Federal Acquisition Regulations and its controls over government-furnished equipment. *Office of Emergency Management Oversight*

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 - 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.

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

FEMA's Management and Oversight of Public Assistance 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.

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

States Management of State Homeland Security Grant Program and Urban Areas Security Initiative Program, Six States to be Determined *(Mandatory)*

FEMA is responsible for enhancing the capabilities of state and local jurisdictions to prevent, protect against, respond to, and recover from incidents of terrorism and other catastrophic events. To meet this responsibility, FEMA awards federal homeland security grant funds to assist states and local jurisdictions in acquiring specialized training, conducting preparedness exercises, and acquiring equipment needed to respond to terrorist attacks and other catastrophic events in their communities. These homeland security grants encompass several different grant programs, including the State Homeland Security Grant Program and the Urban Areas Security Initiative Program. Public Law 110–53, Implementing Recommendations of the *9/11 Commission Act of 2007*, August 3, 2007, requires us to audit each state that receives State Homeland Security Program and Urban Areas Security Initiative grant funds at least once during the next 7 years. As part of our continuing effort to evaluate states' management of homeland security funds, we will initiate audits in six previously unaudited states.

Objectives: Determine the extent to which six selected states have effectively and efficiently implemented the State Homeland Security Grant Program and, if applicable, the Urban Areas Security Initiative program, achieved the goals of the programs, and spent funds in accordance with grant requirements. *Office of Audits*

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. This performance audit will ensure that adequate IT controls are in place over FEMA's NEMIS application.

Objective: Determine whether FEMA has established adequate internal controls for its emergency management systems (i.e., procedures, processes, systems) and that the controls are in place and monitored to ensure accurate and proper reporting and payment to disaster victims. *Office of IT Audits*

FEDERAL LAW ENFORCEMENT TRAINING CENTER

Information Technology Matters Related to the FY 2008 Financial Statement Audit of FLETC ***(Mandatory)***

We contracted with an IPA firm to conduct DHS' annual financial statement audit. An individual audit of FLETC'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 FLETC's critical financial systems.

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

OFFICE OF COUNTERNARCOTICS ENFORCEMENT

Implementation of the DHS Interagency Statement of Intent for Counternarcotics Enforcement

In collaboration with eight other DHS components, the Office of Counternarcotics Enforcement (CNE) developed a document that formally specifies the department's intended baseline level of personnel and resources that will be made available to support counternarcotics operations. This Interagency Statement of Intent, required by the *National Interdiction Command and Control Plan*, assists operational commanders in allocating resources to collect drug-related intelligence, and it supports operations that interdict drug smugglers in South America, Central America, the Gulf of Mexico, the Caribbean, and the Eastern Pacific region.

Through its Drug Terror Nexus Division, CNE has been tasked with tracking and severing connections between illegal drug trafficking and terrorism. CNE works within the Federal Bureau of Investigation's Joint Terrorism Task Force construct and brings together the collective knowledge of numerous DHS components. With operations abroad, the CNE is in a unique position to coordinate DHS counternarcotics efforts.

***Objectives*:** Determine whether the current DHS resources, alignment, and organization are sufficient to support the department's counternarcotics strategy; and what opportunities exist in the United States and internationally for DHS assets to better support mission effectiveness and efficiency. *Office of Inspections*

OFFICE OF INTELLIGENCE AND ANALYSIS

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for Fiscal Year 2009 ***(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 and/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 (DNI), Chief Information Officer, and the Office of Management and Budget, require an annual evaluation and reporting of the security program over agencies' intelligence systems. The *Federal Information Security Management Act* 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 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 Audits*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for Fiscal Year 2009 ***(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 and/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 DNI, Chief Information Officer and the Office of Management and Budget, require an annual evaluation and reporting of the security program over agencies' intelligence systems. The Federal Information Security Management Act (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. The results of this evaluation will be reported to the DNI.

Objective: Perform an independent evaluation 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 Audits*

Office of Intelligence and Analysis
Carryover Project from FY 2008

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 and/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 the Office of Management and Budget, require an annual evaluation and reporting of the security program over agencies' intelligence systems. The Federal Information Security Management Act (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 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 Audits*

Office of Intelligence and Analysis' Fusion Center Initiative

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. According to a 2006 survey, 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 and 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 and Analysis staff to the centers; and (5) what success the Office of Intelligence and Analysis has had in backfilling positions vacated to staff the Fusion Center Initiative. *Office of Inspections*

OFFICE OF OPERATIONS COORDINATION

Office of Operations Coordination Carryover Project from FY 2008

Information Sharing at the National Operations Center

The National Operations Center within DHS provides real-time situational awareness and monitoring of the homeland, coordinates incident response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security and 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 whether the National Operations Center made functional and organizational changes after Hurricane Katrina to improve the flow of information, including whether the center instituted new procedures to ensure that incoming information is properly distributed within the center and to the Secretary. *Office of Inspections*

TRANSPORTATION SECURITY ADMINISTRATION

Whole Body Imaging Testing (Red Team)

TSA is responsible for providing screening of all property, cargo, carry-on and checked baggage, and other articles, that will be transported on a passenger aircraft operated by a domestic or foreign air carrier. TSA is beginning to use Whole Body Imaging technologies to visually screen travelers, allowing the agency to more effectively detect weapons, explosives and other threat items. Whole Body Imaging is being used during secondary screening, on a voluntary basis to produce a three-dimensional image of the body and any concealed items, as an alternative to pat-downs.

Objective: Assess the effectiveness of the technology and determine whether TSA is addressing operational issues, as well as any passenger and privacy concerns. *Office of Audits*

Security of Air Cargo During Ground Movement

Carriage of cargo by air is critical to both the nation's economy and the airline industry that provides this service. More than 80 percent of revenues from air cargo carried on passenger planes are derived from one to two-day deliveries. Express delivery services that rely on air cargo services are a critical element of "just-in-time" manufacturing and distribution facilities. TSA is responsible for providing screening of all cargo that will be transported on a passenger or all-cargo aircraft operated by a domestic or foreign air carrier. As such, TSA is responsible for establishing a system to screen, inspect, or otherwise ensure the security of freight that is to be transported in passenger or all-cargo aircraft as soon as practicable. One important aspect of cargo security is controlling access to cargo during ground movement before cargo is loaded on to an aircraft for transport. In 2005, the Cable News Network (CNN) reported concerns about cargo security and found cargo containers sitting unattended and unsecured on airport ramps where many people had access to the cargo. CNN also observed trucks carrying loads with doors wide open and the cargo within easy view and reach.[1]

Objective: Determine whether TSA provides adequate oversight to ensure indirect air carriers and aircraft operators comply with TSA security requirements for cargo ground movement prior to transport on cargo or passenger aircraft. *Office of Audits*

TSA's Preparedness for Handling Mass Transit Emergencies

Since the terrorist attacks of September 11, 2001, the London subway bombings, and the Madrid rail bombings, DHS has taken steps to manage risk and strengthen our Nation's rail and transit systems. While state and local governments operate the majority of mass transit systems in this country, securing these systems is a shared responsibility between federal, state, and local partners. During emergencies, transit agencies are to rely on well-designed and regularly practiced drills and exercises to rapidly and effectively respond and recover. Recent events on mass transit systems, including a derailment and a fire, have raised questions regarding the adequacy of mass transit agencies' contingency plans and the ability to handle relatively minor, as well as major emergencies.

Objectives: Determine whether TSA has provided mass transit agencies tools, procedures, and training for responding to and recovering from emergencies on passenger rail systems; and review TSA's role in security program management and accountability, security and emergency response training, drills and exercises, public awareness, and other protective measures for passenger rail systems. *Office of Audits*

Penetration Testing of Law Enforcement Credentials Accepted to Bypass Screening *(Congressional)*

During recent penetration testing and related audit work, greater attention has been drawn to the question of whether unauthorized individuals can gain access to secured locations at our Nation's airports. An armed individual carrying counterfeit law enforcement

[1] *CNN Probe Finds Weak Link In Air Security*, August 10, 2005.

credentials could potentially avoid passenger screening and board aircraft while carrying a weapon. Prior to September 11, 2001, the Government Accountability Office reported that they succeeded in using counterfeit credentials to access secured facilities, including airports. The same report was later discovered in a hideaway in Afghanistan after the 2001 attacks. Our office also reported that airport officials including local police stationed at airports were unable to identify counterfeit credentials, generating concern about the policies and procedures TSA has in place to reduce this risk.

***Objective**:* Determine whether TSA has established policies and procedures to prevent armed individuals from using counterfeit law enforcement credentials to bypass security measures before traveling on passenger aircraft. *Office of Audits*

TSA's Clear Registered Traveler's Program

The Clear Register Traveler's Program is TSA's fast pass for airport security. Clear members are prescreened by the TSA, and after application approval, members are provided with a high-tech card, which allows them to access designated airport security fast lanes nationwide. Clear officially opened lanes on March 19, 2008 at Reagan National and Washington Dulles International Airports, amidst record-breaking traffic in a prelaunch test period. Currently there are 16 U.S. airports with registered travelers using Clear. Clear lanes are already operating in airports in Cincinnati, Denver, Indianapolis, Newark, N.J., and San Francisco, in addition to New York's LaGuardia and JFK airports.

Objective: Determine whether TSA has implemented effective and adequate controls over airport security though its Clear Registered Traveler Program. *Office of IT Audits*

Information Technology Matters Related to the FY 2008 Financial Statement Audit of TSA *(Mandatory)*

We contracted with an IPA firm to conduct DHS' annual financial statement audit. An individual audit of the 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 the TSA's critical financial systems.

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

Ability to Communicate With Federal Air Marshals While In Mission Status

The Federal Air Marshal Service consists of thousands of trained law enforcement personnel who are responsible for protecting passengers and flight crews in the event of a

hijacking or terrorist incident. Armed Air Marshals blend in with ordinary passengers to help secure high-risk domestic and international flights on U.S. air carriers. To respond to security situations before, during, and after flights, the Air Marshals need to be able to send and receive timely intelligence information. The Federal Air Marshal Service issues communications equipment to Air Marshals for this purpose, but according to reports, the equipment is not consistently functional.

Objectives: Determine whether TSA is pursuing communication capabilities to ensure that Federal Air Marshals who are in mission status can receive and send time-sensitive, mission related information through secure communication while in flight; and whether the Federal Air Marshal Service is providing Air Marshals with timely and accurate intelligence and situational awareness when they are preparing for or in mission status. *Office of Inspections*

Transportation Security Administration
Carryover Projects from FY 2008

TSA On-Screen Alarm Resolution Protocols for Checked Baggage Screening

TSA established the On-Screen Alarm Resolution Protocol, which was put into place by TSA in May 2004 to improve the through-put of checked baggage screened by Explosive Detection Systems 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 Explosive Detection Systems machines are in fact harmless, allowing the screener to clear the bag. TSA officials believe the protocol 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 the On-Screen Alarm Resolution Protocol to identify and resolve alarms on threat items on the screens of the EDS machines. *Office of Audits*

TSA Known Shipper Program ***(Congressional)***

Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably "known" either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. To ensure compliance, TSA developed the "Known Shipper Program," which includes activities that all regulated entities must carry out prior to transporting cargo onto a passenger aircraft. The Known Shipper Program specifically provides for regulated entities to determine a shipper's validity and integrity, separate "known" shipper cargo from that of "unknown" shippers, and submit information regarding each of its known shippers to TSA. However, anecdotal reports suggest that cargo from unknown shippers is also transported on passenger airplanes, in violation of the Known Shipper Program.

Objectives: Determine how well TSA procedures are designed and implemented to stop cargo from unknown shippers from being shipped on passenger planes. *Office of Audits*

TSA Privacy Management

The *Privacy Act of 1974*, as amended, and the *E-Government Act of 2002* require that DHS protect sensitive, mission-critical data and personally identifiable information contained in its systems of record. To accomplish its mission of protecting the Nation's transportation systems and ensuring freedom of movement for people and commerce, TSA collects, stores, shares, and uses sensitive personally identifiable information. To promote compliance with federal privacy regulations, the TSA Privacy Office works with programs to steward and instill a culture of privacy.

Objectives: Determine whether TSA's privacy program instills a privacy culture that protects sensitive personally identifiable information and ensures compliance with federal privacy regulations. *Office of IT Audits*

Potential Vulnerabilities in TSA's Secure Flight Watchlist Screening *(Mandatory)*

TSA's Secure Flight is an airline passenger prescreening program that intends to compare federal watchlists with information from passenger name records, which passengers give to commercial airline carriers when they book flights. Secure Flight uses information contained in the Terrorist Screening Database, which is a consolidated government watchlist maintained by the Federal Bureau of Investigation's Terrorist Screening Center. The Terrorist Screening Database contains identifying information about suspected and known terrorists.

Although TSA announced its intent to implement the Secure Flight program in 2004, deployment of the system has been delayed numerous times for various reasons. In FY08, Congress fully funded TSA's Secure Flight program. However, concerned about the comprehensiveness of the screening, the House and Senate Committees on Appropriations directed us to report on the vulnerabilities that exist in our aviation system if the Secure Flight program screens airline passenger names against a subset of the Terrorist Screening Database—TSA's No Fly and Selectee lists—instead of the full Terrorist Screening Database.

Objectives: Determine the potential vulnerabilities in the aviation system caused by screening commercial airline passenger names against a subset of the Terrorist Screening Database instead of the full Terrorist Screening Database. *Office of Inspections*

TSA Security Regulations Governing General Aviation *(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 U.S. 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 shown that security at some general aviation airports is easily defeated. At the request of the Chairwoman of the Subcommittee on Transportation Security and Infrastructure Protection within the House Committee on Homeland Security, we will review TSA's efforts to improve the security of general aviation facilities.

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

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

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.

Objectives: Determine whether the USCIS applies consistent and equitable criteria and procedures to its adjudication process and handles applications in a timely manner. *Office of Audits*

Management Controls to Deter Adjudicator Fraud

USCIS adjudicates about six million applications and petitions a year. In comparison to the Department of State's Visa Program, USCIS immigration benefits programs have relatively few safeguards and system checks to identify or deter employee fraud. The Office of Fraud Detection and National Security in USCIS does not consider employee fraud to be within their mandate. The USCIS Office of Security and Integrity is structured to investigate the range of misconduct federal employees might engage in, but it is not focused on adjudicator fraud.

The extent of USCIS employee fraud is unknown, as most fraud is discovered through allegations by applicants or other officers, or as part of a criminal investigation. Employee fraud related to immigration benefits is particularly sensitive because it may involve extortion or coercion of immigrants, or access to benefits by individuals who might otherwise be ineligible as a public safety or national security risk.

***Objectives*:** Determine whether USCIS implemented proper management controls against employee benefit fraud, and whether USCIS should introduce additional controls to improve program integrity. *Office of Inspections*

UNITED STATES COAST GUARD

Annual Review of the United States Coast Guard's Mission Performance (FY 2008) ***(Mandatory)***

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

Objective: Determine the extent to which the Coast Guard is maintaining its historical level of effort on nonhomeland security missions, including how resource hours and performance targets and results for each Coast Guard mission have changed from prior to September 11, 2001, through FY 2008. *Office of Audits*

United States Coast Guard's Acquisition Reorganization

The *Blueprint for Acquisition Reform* (July 13, 2007) is the Coast Guard's strategic document for reshaping its acquisition and contracting capabilities into a single entity, the Acquisition Directorate. The central goal of the *Blueprint* is to enhance Coast Guard mission execution through effective and efficient acquisition and lifecycle management of critical operational systems. The *Blueprint* targets July 1, 2009, for implementation.

A major component of the *Blueprint* is the consolidation of the Integrated Deepwater System acquisition; the Acquisition Directorate; elements of the Command, Control, Communications and Information Systems Directorate; the Resources Directorate; and the Research and Development Center. In addition, the plan encompasses other actions to enhance overall efficiency, including organizational alignment and leadership, policies and processes, human capital, and knowledge and information management. According to the *Blueprint*, the aggregate result will be the development of an enhanced Acquisition

Directorate, capable of efficiently and effectively meeting the increased mission requirement of Coast Guard operational forces.

Objective: Determine the extent to which the Coast Guard has implemented the timetable in its *Blueprint for Acquisition Reform* and the effect of the Reform on Coast Guard acquisitions. *Office of Audits*

USCG IT Management

The U.S. Coast Guard (USCG) is a multimission maritime service and one of the Nation's five Armed Services. USCG uses myriad information technology 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 over 350 commercial ports, USCG is the lead federal agency for maritime border security.

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

Information Technology Matters Related to the FY 2008 Financial Statement Audit of USCG *(Mandatory)*

We contracted with an IPA firm to conduct DHS' annual financial 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 the Coast Guard's critical financial systems.

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

UNITED STATES CUSTOMS AND BORDER PROTECTION

Western Hemisphere Travel Initiative

The *Intelligence Reform and Terrorism Prevention Act of 2004*, as amended, established the Western Hemisphere Travel Initiative. The initiative requires that all people, including United States and Canadian citizens who have historically been exempt from passport requirements present a passport or other approved document that establishes the bearer's identity and citizenship to enter or reenter the United States. The initiative is designed to strengthen border security and facilitate entry into the United States for citizens and legitimate international visitors. The Western Hemisphere Travel Initiative

will greatly reduce the opportunities for misrepresentation of one's identity. Advanced technology embedded in the officially sanctioned travel documents will allow CBP to verify an individual's identity and perform real-time queries against terrorists watch lists and look-out databases. The initiative became mandatory in the air environment on January 23, 2007. CBP will begin the transition to the Western Hemisphere Travel Initiative secure document requirement for the land and sea port environments over the next 18 months with planned implementation as early as June of 2009.

Objective: Determine whether CBP has adequately planned for the implementation of the Western Hemisphere Travel Initiative at land border crossings including identifying personnel and equipment requirements. *Office of Audits*

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 Secure Border Initiative contract actions exceeding $20 million. Congressional concerns expressed about the Secure Border Initiative acquisitions include ensuring the accomplishment of program objectives; understanding of program's trade-offs of competing cost, schedule, and performance objectives; and assuring 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.

Objectives: Determine whether Secure Border Initiative contract actions are designed to accomplish program objectives and to comply with applicable regulations and policies. *Office of Audits*

CBP's Use of Container Security Initiative Information to Identify and Detect High-Risk Containers Prior to Lading

A critical element of DHS' multilayered defense strategy is the Container Security Initiative (CSI). CSI's goal is to identify and inspect containers that pose a potential risk for terrorism at foreign ports before they are placed on vessels destined for the United States. Currently, CSI has been implemented in 58 overseas ports, covering over 85% of U.S.-bound cargo.

CSI shifts the screening process of containerized maritime cargo to an earlier stage in the international maritime supply chain, from the domestic ports of entry to the foreign ports of lading. Under the CSI program, a multidisciplinary team of DHS officers is deployed to work with host nations to target containerized maritime cargo that may pose risks to terrorism prior to being laden on vessels destined for the United States. Through CSI, DHS officials work in partnership with host country counterparts to share information and establish security criteria for identifying high-risk containers. Foreign Customs administrations use standard protocols and non-intrusive technologies to examine mutually designated high-risk maritime containers before they are shipped to U.S. ports. CSI supports the CBP priority mission, which is to prevent terrorists and terrorist

weapons from entering the United States, while facilitating and maintaining legitimate trade.

Objective: Assess the adequacy of staffing, processes, and technology at CSI ports to support identification and inspection of high-risk containers prior to loading them on vessels for transport to the United States. *Office of Audits*

Automated Targeting System (ATS) Use in Foreign Ports *(Mandatory)*

CBP has a multilayered strategy for screening high-risk cargo shipped to the United States. CBP's Automated Targeting System (ATS) is a critical component of this strategy used to identify high-risk cargo that warrants inspection and physical examination. CBP uses ATS to screen more than 11 million containers annually to identify those containers that pose a high risk for terrorism related materials.

The multilayered security strategy extends our borders by working with foreign countries to target and inspect containers before they reach the United States by developing and implementing systems that will capture exam results and images, requiring importers and carriers to provide critical information sooner in the supply chain, and other initiatives that improve security of shipments. ATS is a tool used by CBP to capture and analyze information to identify and target high-risk shipments. It is critical that secure strategies implemented and still under development truly address known system and operational challenges, and allow ATS to become more effective.

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 if CBP's ATS effectively identifies high-risk cargo prior to lading in foreign ports. *Office of Audits*

The Enforcement Communications System Modernization

The Enforcement Communications System (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. TECS will improve information sharing with other agencies, foreign governments, and DHS components, resulting in fewer incorrect admission decisions and increased 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 develop and deploy a modernized replacement for TECS will improve the traveler screening process. *Office of IT Audits*

CBP's IT Management

CBP is responsible for securing the Nation's borders, preventing terrorists and their weapons from entering the country, and facilitating the flow of legitimate trade and travel. To support this mission, CBP relies heavily on a wide-array of information systems, costing more than $1 billion a year. CBP is the single largest user of IT resources within the department.

Objective: Determine whether CBP's IT approach includes adequate planning, implementation, and management to support its mission. *Office of IT Audits*

CBP's Actions in Response to Los Angeles International Airport Network Outage

In May 2008, we reported that CBP had taken actions to address problems related to the August 11, 2007 network outage at Los Angeles International Airport (LAX). We recommended additional actions that CBP could take to prevent network outages at LAX. Additionally, we recommended that CBP review the actions taken at LAX and determine if these, or similar actions, should be taken at other ports of entry.

Objective: Determine what actions CBP has taken to prevent network outages at other ports of entry. *Office of IT Audits*

Information Technology Matters Related to the FY 2008 Financial Statement Audit of CBP ***(Mandatory)***

We contracted with an IPA firm to conduct DHS' annual financial statement audit. An individual audit of CBP'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 CBP's critical financial systems.

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

CBP's Compliance with the *Buy American Act* for Border Fencing ***(Congressional)***

At the request of a member of the House Ways and Means Committee, we will review CBP's compliance with the *Buy American Act* in relation to the construction of border fencing. CBP's contractors may have used Chinese materials to construct a portion of a border fence in Arizona. The member questioned whether the materials' use violated a valid contract that required use of American materials, or whether CBP violated the *Buy American Act* by inserting an inappropriate deviation clause in the contract.

Objectives: Determine whether the contract in question meets the requirements of the *Buy American Act* and whether the contractor met obligations under the contract regarding use of American materials. *Office of Inspections*

United States Customs and Border Protection
Carryover Projects from FY 2008

Refund and Drawback Processes for CBP

CBP is required to refund customs duties that importers determined they overpaid or incorrectly paid for goods entering the United States, and for imported products or portions thereof that ultimately are not consumed in the United States.

Objectives: Determine whether CBP ensures proper payments are being made through these refund processes. *Offices of Audits and IT Audits*

CBP's Northern Border Security Efforts

The U.S.-Canada border consists of approximately 4,000 to 5,000 miles of border. As part of its security strategy, CBP must also address issues inherent in locations along the northern border designated as reservation lands for Native American peoples, which allow more limited access on both the United States and Canadian sides of the border.

Additionally, over 90% of Canada's population lives within 100 miles of the U.S.-Canada border. Although the United States and Canada enjoy an extremely cooperative relationship, intelligence indicates that some individuals and organizations in Canada who reside near the border represent a potential threat to U.S. national security. The northern border also has well-organized smuggling operations, which can potentially support the movement of terrorists and their weapons.

To combat these threats, CBP is developing a comprehensive strategy to protect the Northern Border. As part of this strategy, CBP is placing additional Border Patrol agents and Air and Marine bases, assets along the northern border with Canada. Further, CBP is expanding its use of technology, such as improving its communications and data infrastructure to support sensing and response capability, and implementing the use of Unmanned Aerial Vehicles.

Objectives: To assess the coordination and communication of the DHS components responsible for securing the northern border to ensure an effective northern border security strategy and facilitate sharing of resources and responsibilities. *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 for use 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*

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 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 Congress, 1 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*

Progress Report on CBP's Automated Targeting System ***(Mandatory)***

CBP has a multilayered strategy for screening high-risk cargo shipped to the United States. CBP's ATS is a critical component of this strategy and will be used to identify 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 11 million containers that arrive annually. CBP officers physically inspect the high-risk containers for terrorism-related materials.

The multilayered security strategy extends our borders by working with export countries to target and inspect containers before they reach the United States by developing and implementing systems that will capture exam results and images, requiring importers and carriers to provide critical information sooner in the supply chain, and other initiatives that improve security of shipments. ATS is a tool used by CBP to capture and analyze information that is used to identify and target high-risk shipments. It is critical that secure strategies implemented and still under development truly address known system and operational challenges, and allows ATS to become more effective.

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 CBP's progress in improving ATS as a tool in the multilayered security strategy. *Office of Audits*

CBP Cash Collections and Deposits Revenue FY 2008 ***(Mandatory)***

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, which 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. 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 the Electronic Collection System. 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*

UNTED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

ICE's Review of Medical Treatment Requests

The Division of Immigration Health Services (DIHS) provides or arranges medical care for individuals who are detained by ICE. Originally a part of the Department of Health and Human Services, DIHS joined ICE in October 2007. For nonemergency care, facility clinicians are required to submit a treatment authorization request when detainees need health services. Although the division approves most care requests, ICE has faced criticism and legal action over allegations that some care authorizations were either delayed or inappropriately denied. Outside organizations have also raised concerns that ICE's covered services package, which outlines the scope of medical coverage in detention facilities, is overly prescriptive.

Objectives: Determine whether (1) the timeliness standards for ICE to approve medical services are followed and result in proper care; (2) whether there are enough DIHS nurses working on care authorizations; and (3) whether the covered services package is sufficiently comprehensive given ICE's mission and legal requirements. *Office of Inspections*

United States Immigration and Customs Enforcement Carryover Projects from FY 2008

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 was not consistently deploying qualified and certified contract guards for building in the National Capital Region. Additionally, FPS did not pay invoices in a timely manner, thereby violating the *Prompt Payment Act.* Further, congressional testimony provided by the Government Accountability Office discussed FPS budget shortfalls and a shrinking workforce that could threaten the physical security of government buildings.

Objective: Determine whether FPS is procuring guard services through contracts that are in the best interest of the government. Specifically, we will determine whether FPS is sufficiently and consistently applying criteria to ensure the contract awarded was in the

best interest of the government and whether FPS' oversight provides reasonable assurance that contract guards are satisfying contract requirements. *Office of Audits*

Detentions and Deportations Involving the Parents of U.S. Citizen Children
(Mandatory)

The House Committee on Appropriations directed our office to report data related to ICE's detention center population over the past 10 years. The committee specified that the data should include the total number of deportations; the total number of instances in which one or both parents of a U.S. citizen child was deported; the reasons for parents' deportation; the length of time the parents lived in the U.S. before being deported; whether the U.S. citizen child remained in the U.S. after one or both parents were deported; and the total number of days a U.S. citizen child was held in detention.

Objectives: Determine (1) the number of U.S. deportations; (2) the number of instances in which one or both parents of a U.S. citizen child were deported, reasons for the deportation, and length of time the parent(s) lived in the U.S. before deportation; (3) whether the U.S. citizen child remained in the U.S. after one or both parents were deported; and (4) the number of days a U.S. citizen child was held in detention. *Office of Inspections*

Transfer of Detainees in ICE Custody

ICE's Office of Detention and Removal Operations detains more than 20,000 people a day. According to its *Detention Operations Manual*, the office may transfer detainees between facilities to eliminate overcrowding; to provide required security oversight, medical care, or recreational facilities; to match the venue of a detainee's immigration court case; or to meet other special detainee needs. Nongovernmental organizations report that some transfers may not comply with standards in the *Detention Operations Manual* and create hardship for detainees by changing the venue of their immigration court cases.

Objectives: Determine whether immigration detention facilities properly justify detainee transfers according to the *Detention Operations Manual* and whether resulting changes in court venue impair detainee immigration cases in significant numbers. *Office of Inspections*

ICE Contracting and Procurement Overseas

ICE has approximately 350 staff in more than 30 countries who support the agency's investigative and deportation operations and the Visa Security program. Most ICE staff overseas who coordinates the international dimensions of ICE investigations work with foreign law enforcement entities to provide them with U.S.-based information related to their criminal cases. ICE staff overseas also helps to increase their foreign counterparts' investigative capabilities.

Overseas deployment of ICE personnel involves the acquisition of certain supplies, services, and equipment from host country vendors. Previous DHS OIG work has identified weaknesses in ICE's management controls over foreign acquisitions, permitting opportunities for fraud, waste, and abuse.

Objectives: Review acquisition practices at selected ICE foreign offices in order to determine the extent to which ICE has improved management controls over foreign acquisitions in order to deter fraud, waste, and abuse; and the extent to which ICE applies policies, procedures, and management controls to ensure that its overseas offices conduct proper acquisitions. *Offices of Inspections and Audits*

MULTIPLE COMPONENTS

DHS User Fees

In FY 2007, DHS collected approximately $12 billion from user fees to cover the costs for an array of operational and administrative activities across several components within the department. Some DHS user fees collected include CBP user fees used to conduct customs, immigration, and agricultural inspections; CIS user fees used for adjudication of applications or petitions for immigration and naturalization benefits; FEMA user fees for flood mitigation products and services and flood insurance premiums; and TSA security user fees. Although these user fees are included in the department's annual financial statements, it is unclear how the various components set, collect, use, and review user fees and the effect of user fees on program operations.

Objectives: Identify the universe of user fees throughout the department. Determine what is known about the way various user fees are set, collected, used, and reviewed, and the impact on programs they support. *Office of Audits*

Protection of Personally Identifiable Information (PII) in DHS Data Mining Programs

The *Homeland Security Act* authorizes DHS to use data mining tools and advanced analytics to access, receive, and analyze information. In its 2008 Report to Congress, the DHS Privacy Office identified three data mining programs that meet the definition from the *Federal Agency Data Mining Act of 2007* and employ analytical techniques on data including sensitive personally identifiable information for targeting high-risk cargo for further examination, assisting in analysis of patterns of trade, and detecting anomalies and relationships indicative of criminal activity. The *Privacy Act of 1974*, as amended, and the *E-Government Act of 2002* require that DHS management assess the risks and protect personally identifiable information contained in its systems of record.

Objective: Determine whether DHS data mining systems have implemented adequate policies, procedures, and controls for managing risks, preventing privacy incidents, and

managing activities if personally identifiable data are inadvertently disclosed or compromised. *Office of IT Audits*

Effectiveness of Contracting Support for S&T

The Science & Technology Directorate relies on the DHS Under Secretary for Management's Office of Procurement Operations (OPO) and other federal agencies' contracting officers for procurement services because it does not have a contracting warrant. The OPO contracting officers are co-located in the S&T office space, and they have reporting responsibilities to OPO but not to S&T. The contracting officers in other organizations that provide procurement services to S&T likewise do not report to S&T officials, and they manage the procurements from offsite locations. In the past, S&T was criticized for obligating its research and development funds slowly and, at times, in violation of ethics and procurement rules. Congress rescinded $20 million in S&T's FY 2006 appropriation and another $125 million in its FY 2007 appropriation due to the slow rate at which S&T obligated its funds. S&T attributed some of the delay to OPO's contracting officers not providing an adequate number of qualified, motivated staff. As a result, according to staff in both S&T and OPO, S&T has supplemented OPO's support by using contracting officers outside DHS who do not take the time to ensure compliance with procurement regulations and statutes. S&T officials believe S&T should have its own contracting warrant to exert managerial control over the procurement process and obligate its funds more quickly and effectively.

Objectives: Determine (1) the effectiveness of the coordination between S&T and the contracting services it uses, including the obligation rates for research and development funds in FYs 2006, 2007, and 2008, and controls to ensure compliance with procurement rules; (2) any impediments to efficient, appropriate contractual obligations by either party; and (3) whether improvements could be made to speed obligation rates and strengthen the integrity of S&T's procurements. *Office of Inspections*

Intelligence and Information Sharing Among DHS Immigration Components

DHS components use several information technology systems to screen persons crossing the border, applying for immigration benefits, or involved in potential immigration violations. Some of the systems were inherited from the Immigration and Naturalization Service when DHS was created in 2003. Previous reports from the Government Accountability Office and Department of Justice OIG have criticized the legacy systems as poorly integrated, hampering staff's ability to identify and properly process persons who present a threat to national security or public safety. CBP, ICE, and USCIS have undertaken or participated in several initiatives to improve the sharing of information and intelligence.

Objectives: Determine the effectiveness and the efficiency of the mechanisms through which CBP, ICE, and USCIS share intelligence, considering the degree of coordination, user access to needed information, and potential duplication among data systems. *Office of Inspections*

DHS Spending on Conferences ***(Congressional)***

Federal agencies may sponsor conferences and send their employees to conferences or meetings held in off-site locations. A recent audit by the Department of Justice OIG determined that some of the Justice Department's expenditures for conferences in FYs 2005 and 2006 appeared extravagant, though they were allowed by law. At the request of the Chairman of the House Committee on Homeland Security, we will review DHS expenditures to produce or facilitate conferences and off-site events during the past three years.

Objectives: Identify all the conferences that DHS produced or facilitated during FYs 2005 to 2007 and the total amount DHS spent on them. For a subset of the most expensive conferences, review the justifications offered for the event; the site-cost comparisons on where to hold the event; and certain conference-related costs, including food and beverages, external event planning, and audio-visual support, for compliance with applicable laws and regulations. *Office of Inspections*

Treatment of Unaccompanied Alien Minors

The *Homeland Security Act of 2002* gave primary responsibility for the custody and care of unaccompanied alien children to the Office of Refugee Resettlement in the Department of Health and Human Services, while DHS retains authority over immigration status issues relating to juveniles. Unaccompanied alien children are minors who arrive in the United States without a parent or legal guardian and who are temporarily in the custody of federal authorities because of their immigration status.

On April 6, 2004, the Assistant Secretary for ICE signed a Statement of Principles with the Assistant Secretary for Children and Families in the Department of Health and Human Services, to improve care for unaccompanied alien children. The statement formalized key departmental roles as they related to immigration benefits, immigration enforcement, and the treatment and placement of these children. Pursuant to the statement, DHS will continue to be responsible for apprehension, processing, and immigration benefits. DHS responsibilities include placement in immigration proceedings; removal from the United States when appropriate; decisions in consultation with the Office of Refugee Resettlement regarding consent to the jurisdiction of a state court, when a child wishes to pursue Special Immigrant Juvenile status; and adjudication or petitions for that status. The office will make placement determinations and decisions regarding a child's medical care while the child is in custody. The Office of Refugee Resettlement, however, is not responsible for children placed in facilities without their approval.

DHS is bound by the terms of a settlement agreement known as the *Flores* agreement. The agreement requires DHS to hold minors following arrest in facilities that are safe, sanitary, and consistent with concern for their particular vulnerability as minors. The agreement also restricts the length of time unaccompanied minors can be detained after

apprehension before being transferred to licensed care facilities. There have been allegations of physical and verbal abuse, inadequate food and bedding, delays in transferring minors to appropriate placements, and inadequate medical attention in Border Patrol facilities. The Office for Civil Rights and Civil Liberties in DHS has been accepting these types of complaints and conducting investigations of allegations of abuse.

Objectives: Determine whether DHS is abiding by the terms of the *Flores* agreement by ensuring alien minors are being provided access to (1) toilets and sinks; (2) drinking water and food; (3) medical assistance in an emergency; (4) proper temperature control and ventilation; (5) proper supervision to protect minors from others; and (6) separation from unrelated adults where possible. *Office of Inspections*

DHS Employment Verification Programs

Since the *Immigration Reform and Control Act* passed in 1986, employers must view documentation that an applicant is legally in the United States before hiring that person. E-Verify, an internet-based system operated by USCIS in partnership with the Social Security Administration, is currently free to employers. E-Verify electronically compares information contained on the Employment Eligibility Verification Form I-9 with records contained in Social Security Administration and DHS databases to help employees verify identity and employment eligibility of newly hired employees. The DHS Office for Civil Rights and Civil Liberties has worked with USCIS in the development of E-Verify to include program design, implementation, education, policies, and procedures.

Complementing this effort, ICE has encouraged employer use of verification systems through its voluntary ICE Mutual Agreement between Government and Employers (IMAGE) program. By participating in the IMAGE program, companies can reduce unauthorized employment and the use of fraudulent identity documents. Participating employers must agree to an audit of their employment eligibility records by ICE and verification of the Social Security numbers of their existing labor forces. Enrolled employers gain membership to an employee authorization verification program administered by USCIS, which allows them to verify the eligibility of new hires to work in the United States.

Objectives: Regarding the E-Verify and IMAGE programs, determine (1) the effectiveness of coordination among DHS components, other federal partners, and industry, including assistance DHS provides to employers; (2) the sufficiency of training provided to employers and ICE officers; and (3) the effectiveness of redress procedures for employment-eligible workers who are denied employment as a result of inaccurate information in a DHS or SSA database. *Office of Inspections*

DHS Counterintelligence Activities

Because DHS contains Intelligence Community components, DHS officers have access to a wide array of classified information, much of which would be useful to foreign intelligence services. As such, DHS could be targeted by international terrorist

organizations, some of which have sophisticated intelligence gathering capabilities. To counter this threat, Intelligence Community members possess capabilities to detect and neutralize intelligence vulnerabilities. Although the Federal Bureau of Investigation has the lead for domestic counterintelligence investigations for the federal government, DHS remains responsible for ensuring that counterintelligence matters that affect the department are identified and either passed onto to the Federal Bureau of Investigation for further investigation, or handled internally.

The DHS Secretary identified the Office of Intelligence and Analysis and the Office of Security, operating under the guidance of the Chief Intelligence Officer, to provide DHS with a counterintelligence capability. Currently, the Office of Intelligence and Analysis has a small counterintelligence capability, and the Office of Security has a Counterintelligence Directorate. The Secretary has requested funding in his FY 2009 budget submission to bolster DHS counterintelligence capabilities.

***Objectives*:** Determine the effectiveness of DHS counterintelligence capabilities and the DHS response to counterintelligence threats; and what actions could be taken to mitigate potential deficiencies. *Office of Inspections*

Position Management in Selected DHS Internal Affairs Offices

Within the constraints of federal personnel rules and regulations, mangers have flexibility to allocate their staff positions in different ways in order to maximize effectiveness and efficiency. We received allegations that internal affairs staff in CBP may hold positions with an inflated grade and salary compared to similar federal positions. We also received allegations that internal affairs staff in CBP and ICE may have improperly collected administratively uncontrollable overtime pay. Administratively uncontrollable overtime is a form of premium pay that provides up to 25% additional compensation for substantially increased or irregular work hours.

Objectives: With the assistance of the Office of Personnel Management, determine whether the internal affairs offices in CBP and ICE made efficient use of allocated positions, including in terms of cost; and complied with federal personnel laws and regulations governing use of administratively uncontrollable overtime. *Office of Inspections*

Multiple Components
Carryover Projects from FY 2008

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 Traveler Redress Inquiry Program (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 denied or delayed boarding transportation; denied or delayed entry into or departure from the United States at a port of entry; or 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 the Federal Bureau of Investigation's Terrorist Screening Center. At the request of the Chairman of the House Committee on Homeland Security, we will review the effectiveness of the DHS TRIP program.

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

Investigative Operations within DHS

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.

Objectives*:* Evaluate the effectiveness of the process used to assign, manage, and address misconduct allegations received by DHS components; and coordination among DHS components in responding to allegations. Determine whether procedures components use to refer allegations to the OIG comply with *DHS Management Directive 0810.1*. *Office of Inspections*

DHS Component Coordination of Overseas 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 management control exercised by the component.

Objectives: Determine whether the human, financial, and capital resources in each country are sufficient to accomplish the component's program goals effectively; and whether the effectiveness of the component's oversight and management controls of its international programs and personnel. *Office of Inspections*

Chapter 7 – Other OIG Activities Planned for FY 2009

AUDIT & INSPECTION OFFICES

Listed below are nontraditional projects that our audit and inspection offices will undertake in FY 2009. The nature of the projects may or may not result in our issuing a report at the projects conclusion. Instead, projects may result in the issuance of scorecards, and other documents that capture our work on non DHS projects such as monitoring the work of nonfederal contract auditors.

DHS Scorecard (FY 2009)

In the March 2007 *Semiannual Report to the Congress*, we published a scorecard for selected acquisition functions at DHS. The scorecard showed several major concerns with DHS' acquisition process. Deficiencies, such as a lack of comprehensive program management policies and processes, ineffective internal control over financial reporting, and insufficient program management staffing, negatively impact the acquisition process. Although DHS has made some progress, this review will continue to assess the acquisition elements that are critical for the establishment of an efficient, effective, and accountable acquisition process. Building on work done in respect to other audits, we plan to issue additional scorecards for the following areas:

- Acquisition Management including major acquisition programs, such as USCG's Deepwater and CBP's SBInet
- Financial Management
- Grant Management

Objective: Assess the organizational alignment and leadership, policies and processes, financial accountability, acquisition workforce, and knowledge management and information systems for selected programs. *Office of Audits*

Secure Border Initiative and SBInet 2009 Program Oversight

In November 2005, DHS established the Secure Border Initiative, a multiyear, multibillion dollar program designed to secure the U.S. borders and reduce illegal immigration. One element of SBI is SBInet, the program responsible for developing a comprehensive border protection system. DHS estimates that the total cost of the acquisition phase for the southwest border is $7.6 billion from FYs 2007 through 2011. These funds will facilitate the design, development, integration, and deployment of fencing, roads, vehicle barriers, radar units, command and control communications equipment, along with integrated logistics and operations support. As with any major acquisition, the IG will monitor the SBInet initiative to ensure accomplishment of

program objectives regarding cost, schedule, and performance along with compliance with applicable regulations and policies.

Objective: Provide oversight of CBP's SBInet acquisition practices and the risks associated with accomplishment of program objectives and compliance with applicable regulations and policies. *Office of Audits*

Single Audit Oversight and Coordination

Offices of Inspectors General serve as the federal audit agencies responsible for determining compliance with the *Single Audit Act of 1984*, as amended, by certain state, local, Indian tribal, and Insular area governments and nonprofit organizations as designated by the Office of Management and Budget. All nonfederal organizations that spend $500,000 ($300,000 for FY ending before January 1, 2004) or more per year of federal assistance (i.e., grants, contracts, loans, and cooperative agreements) are required to obtain an annual audit in accordance with the *Single Audit Act of 1984*, as amended. Guidance for performing the audit is presented in Office of Management and Budget Circular A-133, Audits of States, Local Governments and Non-Profit Organizations.

Objective: Determine compliance with the *Single Audit Act of 1984* by monitoring the work performed by nonfederal auditors through the use of Desk Reviews and Quality Control Reviews. *Office of Audits*

Recurring Disaster Operations and Oversight – Multiple State Reviews

We 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 PA repairs and restorations, and hazard mitigation, as well as other support areas such as 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, our regional staff will maintain effective relationships with FEMA regional personnel by meeting with executive and senior FEMA regional office personnel to explain our mission, priorities, and capabilities, and 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 Recovery Working Group

In the wake of the Gulf Coast hurricanes of 2005, the PCIE and ECIE Homeland Security Roundtable created the Disaster Recovery Working Group, which became the primary forum for the IG community to conduct its ongoing discussions of and planning for disaster oversight. Recognizing that coordination of federal emergency management oversight efforts is essential, the Disaster Recovery Working Group continues to meet on a regular basis to share and discuss lessons learned from Gulf Coast hurricane oversight efforts and to plan for current and future disasters, with a broader view that includes all disasters. *Office of Emergency Management Oversight*

Oversight of Contracted IT-Related Testing Performed as Part of DHS' FY 2009 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 Audits*

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

Executive Order 12333 describes the limited, specific cases when a member of the Intelligence Community may collect, retain, or disseminate information on United States persons. Another Executive Order, 13462, requires departments with Intelligence Community members to report on a routine basis how well they have complied with Executive Order 12333 and whether any violations have occurred. DHS has two Intelligence Community members—the USCG and Office of Intelligence and Analysis—and is therefore responsible for intelligence oversight reporting under Executive Order 13462. The OIG and DHS Office of General Counsel collaboratively prepare intelligence oversight reports, which are submitted on a quarterly basis to the Intelligence Oversight Board, a standing committee of the President's Intelligence Advisory Board.

Objective: Validate assertions made by the USCG and Office of Intelligence and Analysis concerning their compliance with Executive Order 12333, and report other possible violations that come to our attention. *Office of Inspections*

OFFICE OF INVESTIGATIONS

The mission of the Office of Investigations is to strengthen the effectiveness and efficiency of DHS; secure and protect the Nation from dangerous people and dangerous things; protect the civil rights and liberties of citizens, immigrants, and nonimmigrants in the United States; enforce and enhance departmental priorities and programs; and promote the OIG law enforcement mission.

To protect the Nation from dangerous people and dangerous goods, the Office of Investigation will:

- Open 100% of referrals relating to allegations of corruption or compromise of DHS employees or systems that relate to securing the nation's borders including the smuggling of drugs, weapons, and people (CBP – ICE).
- Open 100% of referrals relating to allegations of corruption or compromise of DHS employees or systems that relate to securing the Nation's federally regulated transportation systems (TSA).

- Open 100% of referrals relating to allegations of corruption or compromise of DHS employees or systems that relate to the immigration process and documentation (USCIS - CBP).

To protect citizens and DHS employee civil rights and civil liberties, the Office of Investigations will:

- Investigate referrals of ICE detainee deaths, which involve suspicious causes or circumstances.
- Investigate credible referrals of the physical abuse of detainees, suspects, or prisoners.
- Investigate all on-duty shooting incidents involving DHS employees (excluding accidental discharges which are absent unusual circumstance, e.g., personal injury).
- Investigate credible allegations of criminal abuse of authority including, but not limited to those that result in deprivation of rights or large-scale thefts.

To protect the integrity of the department's programs, as well as its assets, information, and infrastructure, the Office of Investigation will:

- Investigate significant grant and contract fraud allegations.
- Investigate gross misuse or abuse of classified information, privacy information, or law enforcement information.
- Continue to actively participate on the Department of Justice Hurricane Katrina Fraud Task Force. The Task Force was established by the United States Attorney General on September 8, 2005 in response to the need to investigate fraudulent activities associated with FEMA disaster relief efforts following Hurricanes Katrina and Rita. To support this effort, 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-call Response Employees.
- Investigate FEMA fraud that involves contractors, claimants or FEMA employees.
- Investigate allegations of corruption or criminal misconduct of DHS employees in the processing of immigrant and nonimmigrant documents (USCIS - CBP).
- Exercise oversight of DHS component element internal affairs investigations.

To strengthen the DHS OIG law enforcement mission and unify DHS operations and management, the Office of Investigation will:

- Continue our reputation for Excellence by producing thorough and timely investigations and reports.
- Ensure recruitment, development and opportunity for a quality and diverse workforce.
- Continue to develop innovative ideas and solutions for progressive development of law enforcement issues and resources. Perfect workflow operations through

continuing development of Hotline and referral process, and administration of a robust training program and innovative training initiatives.
- Enhance relationship and communication with DHS law enforcement component Internal Affairs Offices to advance intelligence gathering and information sharing.
- Participate in the President's Council on Integrity and Efficiency functions; and professional law enforcement organizations and associations.

OFFICE OF ADMINISTRATION

The mission of the Office of Administration is to provide administrative support services and information technology infrastructure and systems to OIG's staff, including auditors, inspectors, and investigators. These services enable audit, inspection, and investigation staff to focus their efforts on improving the efficiency and effectiveness of DHS programs and operations. The Office of Administration is responsible for the following initiatives and programs in FY 2009:

DHS' Information Sharing Coordinating Council

As required by the *Intelligence Reform and Terrorism Prevention Act of 2004*, as amended, and the President's October 2007 *National Strategy for Information Sharing*, DHS is working to improve its information sharing environment for terrorism related information including homeland security and weapons of mass destruction information. As part of this effort, DHS formed an Information Sharing Coordinating Council (ISCC) to set information sharing policies, directives, plans, and recommendations and to provide a department-wide framework for improving information sharing with its federal and nonfederal stakeholders.

DHS OIG actively participates on DHS' ISCC. Our representative from the Office of Administration attends ISCC meetings, monitors ISCC's activities, and contributes to various ISCC initiatives. Those initiatives include responding to requests for comments on information sharing policy and performance measures such as defining common standards for how information is acquired, accessed, shared, and used within the ISE. Our representative also sends frequent updates to OIG management on the department's information sharing initiatives.

As part of our effort to work collaboratively with DHS and the ISCC, the OIG participated in the department's 2007 pilot efforts to determine how DHS shares critical information among its components, federal partners, and private sector stakeholders within the intelligence community. The department surveyed several pilot components, including the OIG, to identify information sharing relationships and whether these relationships were documented. The department found that the OIG is a top-level sharer of information through our various documented Memoranda of Understandings.

In FY 2009, our Office of Administration will continue to participate in ISCC bi-weekly meetings, monitor ISCC activities, and participate in its initiatives, as appropriate.

OIG Policy Directives

In FY 2009, our Office of Administration plans to publish 15 new or revised directives concerning government purchase cards, OIG's Privacy Program, records management, and OIG audit quality control and assurance.

Legislative and Regulatory Reviews

In FY 2009, our Office of Administration will continue to support the department by providing timely comments to proposed legislation and regulations, and drafts of directives, congressional testimony, and other various documents.

Audit Quality Control and Assurance Program

The Office of Administration is responsible for our audit quality control and assurance program. The program includes a system of overlapping internal controls that provide assurance that applicable auditing standards are met for each audit. The program requires that quality control reviews (QCRs) be conducted of issued audit reports.

During FY 2009, our Office of Administration will award a multi-year contract to acquire quality control review services from an outside contractor. The contractor will determine the extent to which our internal quality control system provides reasonable assurance that applicable auditing standards are met by conducting 15 reviews, as follows:

- 3 QCRs of FY 2007 issued audit reports;
- 9 QCRs of FY 2008 issued audit reports; and
- 3 QCRs of FY 2008 or FY 2009 in-progress audits.

Audit Policies and Training

As part of our audit quality control and assurance program, the Office of Administration will:

- Continue to provide audit manual training to all new audit staff;
- Coordinate the permanent formation of a DHS OIG Quality Assurance Committee; and
- Develop and issue, in collaboration with the Quality Assurance Committee, a newly formatted OIG Audit Manual that includes a new Quality Control Review Guide. The new manual will include a crosswalk to applicable Government Auditing Standards.

Continuity of Operations

DHS OIG planned and executed an agency-wide COOP exercise during FY 2008. This initiative was required to ensure the continuous performance of the agency's essential functions and operations during an emergency. The activities allowed the emergency response group to meet the stated exercise training objective, which was to learn from the process and come away with a better appreciation of what it will take to be prepared in a real COOP situation.

Overall, the exercise was positive, organized, well-run, and productive with a very impressive technical and communicative pedigree. Thorough after-action analysis and discussion was also conducted immediately following the close of the exercise. As part of this analysis, participants were asked to submit activities that had positive results. Key accomplishments during the COOP include testing the IT infrastructure, telecommunications and alternate site facility; the first time use of the automated communicator system to account for OIG employees; addressing the injects sent to us from the COOP National Operations Center; and, follow up discussions with numerous suggestions for improving the COOP posture for the OIG. The exercise allowed the OIG to finalize its COOP plan and implement a communicator system that allowed for enhanced accountability of its employees.

For FY 2009, COOP planning will focus on the recommended improvements to the plan that were gathered during the analysis session of lessons learned and best practices and in exploring ways to improve critical services and functions. This will assist in enabling our organization to be able to better prepare for future incidents as well as play a more meaningful and productive role to increase the quality of such COOP exercises. The FY 2009 initiatives will include efforts in addressing issues such as emergency response group team member make-up, alternate facility options, infrastructure, employee accountability, criteria to select essential personnel, and recovery operations.

Security Initiatives

During FY 2009, our Office of Administration will work on the following security initiatives:

- Upgrading the Sensitive Compartmented Information Facility to include a Joint Worldwide Intelligence Communication System, Homeland Security Data Network;
- Implement HSPD 12, which provides for government wide, uniform access standards;
- Reissue OIG credentials to all employees with the new OIG seal and tamper proof special security ink; and
- Write the OIG Security Plan. The Security Plan will detail the five Security disciplines: Physical Security, Personnel Security, Information Security, Industry

Security, and Communication Security. The Security Plan will also encompass the COOP, Shelter in place and occupational emergency response Plans.

Information Technology Enterprise Initiatives

As part of our efforts to improve the efficiency of day-to-day operations within the DHS OIG, the Office of Administration completed three significant technology improvement projects: secure mobile technology, comprehensive enterprise system, and disaster recovery systems testing.

The DHS OIG is a mobile workforce, and requires secure technologies that will support its need for flexibility, speed, and performance as employees work both within the standard OIG office environment, as well as remotely while on travel.

The Office of Administration also completed the initial development and pilot delivery of a new enterprise information management system for the DHS OIG. The DHS OIG Project Tracking and Recommendation Follow-up System are the first two modules of a comprehensive enterprise system that is intended to support mission critical processes of the organization. The development of the DHS OIG Project Tracking and Recommendation Follow-up System was completed during the second quarter of FY 2008. A pilot of the new system was launched in July 2008, with the system scheduled to go into full production during the first quarter of FY 2009.

In support of the need to provide continuity of operations in the event of a major disaster, the Office of Administration conducted a full test of DHS OIG disaster recovery systems. In October 2007, during core operating hours, primary network operations in the Washington, DC headquarters building were completely shut down testing the organization's ability to transfer operations to the alternate disaster recovery facility. The test was successful, providing valuable information on the effectiveness of the DHS OIG systems recovery strategy. The lessons learned developed from the FY 2008 tests were used to prepare corrective action plans, and will be used to conduct additional tests of DHS OIG continuity of operations readiness in FY 2009.

During FY 2009, the Office of Administration will continue to support the overall operations of the DHS OIG with the following planned initiatives:

- Deliver two additional enterprise system modules supporting the annual planning and correspondence control processes within the organization;
- Redesign the OIG Intranet Site; and
- Replace the Office of Investigations Case Management System.

Human Resources Initiatives

In the career development and training program areas, we will continue to write statements of work for several training contracts including leadership, supervisory and retirement training, and to put together a listing of suggested books to establish a

leadership library for our employees to use. Under our wellness program, we will be contacting appropriate individuals for flu immunization shots, and working on obtaining a thrift savings plan training session here for our employees.

For FY 2009, in addition to improving our established programs and day-to-day processes, our major undertaking will be to concentrate on revamping the OIG's performance appraisal system and to introduce an e-performance system to accommodate both managers and employees. We also hope to establish some consistent benchmarks throughout OIG, and tie these benchmarks to the employee survey initiatives. Our goal is to have new performance plans consistent across OIG, have everyone trained in the new system, and ready to implement for FY 2010.

We also plan to continue to coordinate and monitor OIG Action Plans resulting from the 2007 DHS OIG survey results and tie those plans to improving the OIG's performance culture. We will continue conducting assessments in some of our established HR programs to see if they are working the way they should, establishing a more efficient electronic request for personnel action system and increase the use and awareness of employee wellness programs through brown bag lunches.

Privacy Initiatives

Given recent incidents exposing the personally identifiable information of hundreds of thousands of federal employees and citizens to compromise, the federal government has renewed its emphasis on protecting personally identifiable information in its custody. In keeping with this renewed emphasis, the OIG designated a Privacy Officer, initiated in-house classroom training, and issued several privacy awareness messages to all employees.

In FY 2009, OIG will issue an internal directive establishing policies and procedures for privacy compliance, expand privacy training resources available to employees, and enhance the security of its electronic records.

Real Property Management Initiatives

In FY 2009, our Office of Administration will work with the General Services Administration to relocate offices in Houston, Texas; Denton, Texas; Del Rio, Texas; and El Segundo, California. With approved prospectus authority, we will award a 10-year superseding lease for our headquarters located in Washington, DC.

Asset Management Initiatives

In FY 2009, our Office of Administration will procure asset control services, supplies, and equipment to establish a new unified web-based solution to manage and control our assets.

Budget Initiatives

During FY 2009, our Office of Administration will work on the following budget initiatives:

- Assign a desk officer (budget analyst) to each OIG division. The budget analyst will serve as the division's main point-of-contact to handle all budget, financial, and travel-related issues for the division. This customer-oriented approach will ensure that headquarters and field offices are serviced timely, address any special needs that the division may have, and provide guidance and support to managers, supervisors, and administrative officers.

- Author a comprehensive travel manual along with standard travel policies and procedures as promulgated by Federal Travel Regulations.

- Audit headquarters and field offices' compliance with budgetary, procurement, purchase card, travel card, financial and travel policies, procedures and regulations. Address weaknesses and establish corrective action plans.

- Meet with DHS budget officials, OMB officials, and Congressional officials to explain OIG's FY 2010 budget.

- Prepare OIG's FY 2011 budget.

- Prepare OIG's operating plan for FY 2009 and monitor expenditures.

OFFICE OF CONGRESSIONAL AND MEDIA AFFAIRS

The mission of the Office of Congressional and Media Affairs (CMA) is to be the most effective representative of the OIG to the Congress, the White House, and the media. Specifically, the Office responds to inquiries from the Congress, the White House, the public at large, and the media; notifies Congress about OIG initiatives, policies and programs; coordinates preparation of testimony and talking points for Congress; and coordinates distribution of reports to Congress. CMA tracks congressional requests, which are either submitted by a Member of Congress or mandated to the OIG through legislation. It also provides advice to the IG and supports OIG staff as they address questions and requests from the press and Congress.

In the 110th Congress, 86 Congressional committees and subcommittees asserted jurisdiction of DHS by holding hearings or otherwise exercising formal oversight activity, such as staff briefings. The CMA is the primary liaison to Members of Congress and their staffs and the media. CMA regularly provides information to Congress and replies to inquiries from various committees of the House and Senate and to Members of Congress who are interested in various aspects of DHS.

CMA monitors and tracks current legislation to anticipate possible changes to policies affecting DHS and that of the IG Community. In many instances legislation includes reporting requirements for the OIG. During FY 2009, CMA will focus on appropriation bills and other legislation affecting DHS, DHS OIG, and the IG community.

Congress regularly requests the IG or senior staff to submit and present testimony to oversight committees about specific activities of interest to Congress. CMA will continue to draft testimony and assists in the preparation for these hearings covering a wide range of homeland security issues. The office will also responds to all media inquiries that result from the OIG's participation at congressional hearings or OIG reports.

OFFICE OF COUNSEL TO THE INSPECTOR GENERAL

The mission of the Office of Counsel (OC) is to enhance and support the IG's independence and provide a full range of legal services for the OIG. OC is headed by the Counsel to the IG, and is composed of attorneys, paralegals, *Freedom of Information Act* specialists, legal interns, and administrative personnel. OC attorneys are the only attorneys in the DHS who do not report to the department's General Counsel. Instead, attorneys in OC are hired and report, through the chain of command, only to the IG. In this manner, the IG can be assured that the legal advice he receives is entirely objective and not influenced by departmental policy preferences. OC accomplishments are not properly measured solely by statistical measures. During FY 2009, OC will provide the following services:

Report Reviews

OC provides legal advice to the IG and other employees in the OIG. Among other matters, OC interprets laws, rules, and regulations; analyze cases; and researches the legislative history that leads to the passage of a particular Act. Virtually all OIG written products, for example, reports, Congressional testimony, correspondence, and many reports of investigation are reviewed by OC attorneys for legal accuracy. In some instances, OC attorneys may simply verify that legal citations are correct; in others, OC attorneys may identify unrecognized legal issues that may have criminal, civil, or administrative ramifications, and may revise or draft significant portions of the report or testimony.

Freedom of Information Act/Privacy Act

In keeping with the OIG's commitment to transparency, OIG reports, reviews and testimony are posted on the OIG's public website. All of these documents first are examined by OC to ensure compliance with the *Freedom of Information Act*, the *Privacy Act*, and other legal and policy directives. In addition, OC processes *Freedom of*

Information Act and *Privacy Act* requests filed with the OIG, or referred from other DHS components or other agencies, and answers questions from members of the public.

Ethics

Consistent with OIG independence, OC ensures OIG compliance with federal ethics laws and regulations. OC provides guidance on activities and provides individualized advice to OIG employees in response to questions about specific actions. OC provides new employees with an ethics orientation, departing employees with post-employment counseling, and provides annual ethics training and reviews annual financial disclosure reports for OIG employees.

Personnel

OC works closely with the OIG's Human Resources department and with individual supervisors on personnel issues, providing legal review, advice and guidance on handling wide-ranging personnel issues, ranging from the availability of accommodations for a handicapped employee to performance-based matters or disciplinary actions. OC represents the OIG in administrative proceedings before the Merit Systems Protection Board, the Equal Employment Opportunity Commission, and works closely with Department of Justice Attorneys on OIG matters that are the subject of federal litigation.

Administrative Subpoenas

The IG is one of the few DHS officials with authority to issue administrative subpoenas. All administrative subpoenas, ordinarily issued through or in support of OIG's Office of Investigations, undergo legal scrutiny prior to issuance, and OC helps ensure proper followup.

Tort Claims

OC also handles or coordinates with Department of Justice on actions against the OIG under the *Federal Torts Claims Act* or against individual employees for actions taken in their official capacity, so-called Bivens actions. OC attorneys work closely with Department of Justice attorneys, attorneys elsewhere in DHS and throughout the federal government.

Training

OC provides ongoing training throughout the OIG on a wide range of legal issues, including ethics, *Freedom of Information Act* and *Privacy Act*, suspension and debarment, and legislation. OC stays abreast of ongoing legislative and policy initiative and provides written comments as appropriate.

Legislation

OC also plays an active role in various legislative initiatives affecting the OIG, IG authorities throughout the federal government, and matters on which the OIG plays a significant role, such as procurement fraud and emergency management oversight. OC attorneys serve on task forces, prepare policy papers, and review and comment on proposed legislation, regulations, directives and other such matters.

External Liaison

OC ensure a close liaison and successful ongoing working relationship with attorneys in the DHS, Department of Justice, the Office of Special Counsel, the Office of Government Ethics, and throughout the federal government, and, on occasion, with attorneys in state and local governments and in private practice.

Council of Counsels to Inspectors General

Attorneys in OC play a leading role in the Council of Counsels to Inspectors General, the umbrella organization for all attorneys in OIGs throughout the federal government. OC attorneys have served on instructional panels regarding access to information, *Freedom of Information Act* and *Privacy Act*, suspension and debarment, served on working groups to provide responses to legal questions posed by the Federal Law Enforcement Training Center, and helped plan training sessions for new OIG lawyers and summer interns. OC intends to continue to play an active role in the CCIG.

In FY 2009, OC intends to continue its ongoing activities throughout the OIG and on behalf of the OIG throughout the federal government. In particular, OC seeks to finalize and have issued throughout DHS a management directive regarding audit report follow-up and closure. OC also intends to reduce its *Freedom of Information Act* backlog to zero.

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 Audits**
Edward F. Cincinnati	**……...**	**Assistant Inspector General/Administration**
Vacant	**……...**	**Director, Congressional and Media Affairs**
Denise S. Johnson	**……...**	**Executive Assistant to the Inspector General**

Locations of Audits Field Offices

Boston, MA
Boston, MA 02222
(617) 565-8700 / Fax (617) 565-8996

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

Denver, CO
Lakewood, CO 80225
(303) 236-2877/ Fax (303) 236-2880

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

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

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

Location of IT Audits Field Office

Seattle, WA
Kirkland, WA 98033
(425) 250-1363

Locations of Emergency Management Oversight Field Offices

Atlanta, GA
Atlanta, GA 30309
(404) 832-6700/ Fax (404) 832-6645

Biloxi, MS
Biloxi, MS 39531
(228) 385-1713/ Fax (228) 385-1714

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

New Orleans, LA
New Orleans, LA 70114
(504) 762-2148/ Fax (504) 762-2873

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

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

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
Dearborn, MI 48126
(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

Los Angeles, CA
El Segundo, CA 90245
(010) 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) 250-1360 / 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) 314-9679

Appendix B
Acronyms

ATS	Automated Target System
CBP	Customs and Border Protection
CFO-Act	The *Chief Financial Officers Act*
CMA	Office of Congressional and Media Affairs
CNE	Counternarcotics Enforcement
CNN	Cable News Network
COOP	Continuity of Operations
COTRS	Contracting Officer's Technical Representatives
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DIHS	Division of Immigration Health Services
DNDO	Domestic Nuclear Detection Office
DNI	Director National Intelligence
DRF	Disaster Relief Fund
EMPG	Emergency Management Performance Grants
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FPS	Federal Protective Service
FTE	Full-time Equivalent
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive 12
ICE	Immigration and Customs Enforcement
IG	Inspector General
IMAGE	ICE Mutual Agreement between Government and Employers
IPA	Independent Public Accounting
IPv6	Internet Protocol version 6
ISCC	Information Sharing Coordinating Council
IT	Information Technology
JFO	Joint Field Office
LAX	Los Angeles International Airport
NCSD	National Cyber Security Division
NEMIS	National Emergency Management Information System
NFIP	National Flood Insurance Program
OC	Office of Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OPO	Office of Procurement Operations
PA	Public Assistance
QCR	Quality Control Review
S&T	Directorate for Science and Technology

Appendix B (cont'd)
Acronyms

SBI	Secure Border Initiative
SBIR	Small Business Innovative Research
TAC	Technical Assistance Contract
TECS	Treasury Enforcement Communication System
TH	Transitional Housing
TIC	Trusted Internet Connections
TOPOFF 3	Top Officials Three Exercise
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
WYO	Write Your Own

Appendix C – FY 2008 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' strategic objectives, the President's Management Agenda, and major management challenges facing DHS.	95%
1.2	Achieve at least 85% concurrence with recommendations contained in OIG audit and inspection reports.	98%
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 (excludes grant audits).	51%

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.	77%
2.2	At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.	81%
2.3	Provide audit coverage of $1 billion of DHS' grant programs.	265%
2.4	Achieve at least 85% concurrence from DHS management with OIG recommendations on grant audits.	88%

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.	Being Implemented
3.2	Ensure that 100% of DHS OIG employees have an annual Individual Development Plan.	99%
3.3	Ensure that 100% of all eligible DHS OIG employees have an Individual Performance Plan and receive an annual Rating of Record.	99%

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.