Fiscal Year 2012
Annual Performance Plan

Department of Homeland Security

Office of Inspector General

The Department of Homeland Security

Office of Inspector General

Fiscal Year 2012
Annual Performance Plan

The *Government Performance and Results Act of 1993*, Public Law 103-62, requires agencies to submit to the Office of Management and Budget 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.

Photo Credits: DHS Photo Galleries

A Message From the Acting Inspector General

I am pleased to present the *Fiscal Year 2012 Annual Performance Plan* for the Department of Homeland Security's (DHS) Office of Inspector General (OIG). This plan outlines the projects that we intend to undertake this fiscal year to evaluate DHS' programs and operations.

This promises to be an especially challenging year as the Department faces new and emerging threats, while striving to maximize its resources and increase efficiency and effectiveness. Despite these challenges, we will continue to address the many complex issues confronting the Department in its daily effort to reduce America's vulnerability to terrorism, and to minimize the damage and accelerate recovery from manmade attacks and natural disasters that may occur.

In developing the plan, we focused on aligning our planned projects with the Secretary's budget priorities, the six missions identified in the Department's *Quadrennial Homeland Security Review Report*, the *Bottom Up Review*, and the major management challenges identified in our report, *Major Management Challenges Facing the Department of Homeland Security*, OIG-11-11. We also factored in the requirements of the *American Recovery and Reinvestment Act of 2009* and other legislative mandates.

We also attempt to address the interests and concerns of DHS senior management officials, Congress, and the Office of Management and Budget (OMB). We remain 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, and abuse.

Charles K. Edwards
Acting Inspector General

Table of Contents

Chapter **Page**

Appendices

Chapter 1 – OIG Mission and Responsibilities

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

DHS OIG's Inspector General, who is appointed by the President and confirmed by the Senate, reports directly to both the Secretary of DHS and Congress. Barring narrow and exceptional circumstances, the Inspector General may audit, inspect, or investigate anyone in the Department, or any program or operation of the Department. To ensure the Inspector General's independence and objectivity, our office has its own budget, contracting, and personnel authority, separate from that of the Department. Such authority enhances our 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.

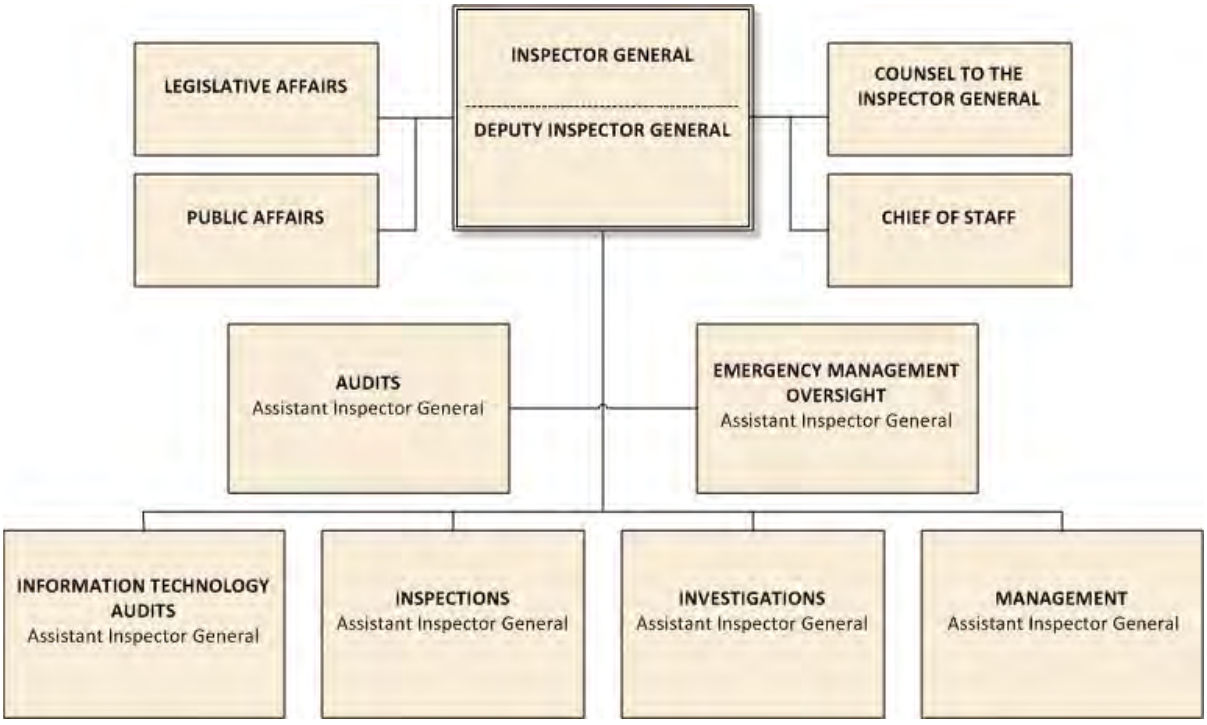
Our office's key legislated responsibilities are as follows:

- 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 the Department's officials and staff, and with other federal, state, and local government agencies and nongovernment entities regarding the mandated duties of our office; and
- Keep the Secretary and Congress fully and currently informed of problems in agency programs and operations.

Chapter 2 – OIG Organizational Structure and Resources

We were authorized 676 full-time employees. We consist of an Executive Office and nine functional components based in Washington, DC. We also have field offices throughout the country. Figure 1 illustrates the DHS OIG management team.

Figure 1: OIG Organization Chart



Our office consists of the following components:

The Executive Office consists of the Inspector General, Deputy Inspector General, Chief of Staff, Special Assistant and Senior Management Analyst. It provides executive leadership to our office.

The Office of Legislative Affairs (OLA) serves as primary liaison to members of Congress and their staffs, the White House and Executive Branch, and to other governmental agencies and entities involved in securing the Nation. OLA staff responds to inquiries from the Congress and the White House; notifies Congress about OIG initiatives, policies, and programs; and informs other governmental entities about OIG initiatives that affect their operations and activities. The office distributes correspondence and final audit, inspection, and special reports to Congress and the White House. It also provides advice to the Inspector General and supports OIG staff as they address congressional, and White House inquiries.

The Office of Public Affairs (OPA) is the Inspector General's principal point of contact for all media outlets and the public. OPA provides information about OIG and its audit, inspection, and investigative reports and findings to news organizations and the public in

compliance with legal, regulatory, and procedural rules. OPA prepares and issues news releases, arranges interviews, and coordinates and analyzes information to support OIG's policy development and mass communications needs. OPA is responsible for developing OIG's integrated communication strategy and helps promote the understanding and transparency of OIG's work process and findings. In addition, OPA advises the Inspector General and others within OIG on programmatic and public affairs issues that affect OIG and its relationship with DHS; other federal agencies; state and local governments; the media; and the public.

The Office of Counsel (OC) provides legal advice to the Inspector General and other management officials; supports audits, inspections, and investigations by ensuring that applicable laws and regulations are followed; serves as OIG's designated ethics office; manages 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 of Audits (OA) conducts and coordinates audits and program evaluations of the management and financial operations of DHS. Auditors examine the methods employed by components, agencies, grantees, and contractors in carrying out essential programs or activities. OA evaluates whether established goals and objectives are achieved and resources are used economically and efficiently; whether intended and realized results are consistent with laws, regulations, and good business practice; and whether financial accountability is achieved and the financial statements are not materially misstated.

The Office of Emergency Management Oversight (EMO) provides an aggressive and ongoing audit effort designed to ensure that disaster relief funds are spent appropriately, while identifying fraud, waste, and abuse as early as possible. EMO keeps the Congress, the Secretary, and the Administrator of the Federal Emergency Management Agency (FEMA), and others fully informed and also addresses problems relating to disaster operations and assistance programs, and progress regarding corrective actions. EMO's 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 allows EMO to stay current on all disaster relief operations and provide on-the-spot advice on internal controls and precedent-setting decisions. A portion of its full-time and temporary employees are dedicated to gulf coast hurricane recovery.

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

The Office of Information Technology Audits (ITA) conducts audits and evaluations of DHS' information management, cyber infrastructure, and systems integration activities. ITA 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 that they are effective, efficient, and implemented according to applicable policies, standards, and procedures. ITA also assesses DHS' information security program as mandated by the *Federal Information Security Management Act* (FISMA), and provides technical forensics assistance to OIG offices in support of OIG's fraud prevention and detection program.

The Office of Investigations (INV) investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and programs. INV concentrates its investigative resources on matters including disaster relief operations and programs; contracts, grants, and procurement fraud; employee corruption; and civil rights and civil liberties abuses. These investigations can result in criminal prosecutions, fines, civil monetary penalties, administrative sanctions, and personnel actions. Additionally, INV provides oversight and monitors the investigations of DHS' various internal affairs offices.

The Office of Management (OM) provides critical administrative support functions, including OIG strategic planning; development and implementation of administrative directives; OIG's information and office automation systems; budget formulation and execution; correspondence control; printing of OIG reports; personnel and procurement services; and oversight of travel and accounting services provided to OIG on a reimbursable basis by the Bureau of Public Debt. OM also prepares OIG's annual performance plans and semiannual reports to Congress.

Chapter 3 – Fiscal Year 2012 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 this plan, we endeavor to assess DHS' progress in meeting the most critical issues it faces.

This plan describes more projects than may be completed in fiscal year (FY) 2012, and tries to take into account future developments and requests from DHS management and Congress that may occur as the year progresses, which may necessitate deferring or cancelling some projects in this plan. Resource issues, too, may require changes to the plan. The plan includes projects that were initiated but not completed in the prior fiscal year, and projects that were listed in our prior fiscal year's plan that will start in FY 2012. Finally, the plan lists some projects that will start during FY 2012 but will carry over into FY 2013.

In establishing priorities, we placed particular emphasis on the major management challenges facing the Department, as described in our report, *Management Challenges Facing the Department of Homeland Security* (OIG-11-11). We identified the following as the most serious FY 2010 management challenges facing DHS:

Acquisition Management	Infrastructure Protection
Financial Management	Border Security
Information Technology Management	Transportation Security
Emergency Management	Trade Operations and Security
Grants Management	

We placed emphasis on legislative mandates such as the *Chief Financial Officers Act* (P.L. 101-576), Federal Information Security Management Act (44 U.S.C. §§ 3541, et seq.) (FISMA), and the *American Recovery and Reinvestment Act of 2009* (ARRA).

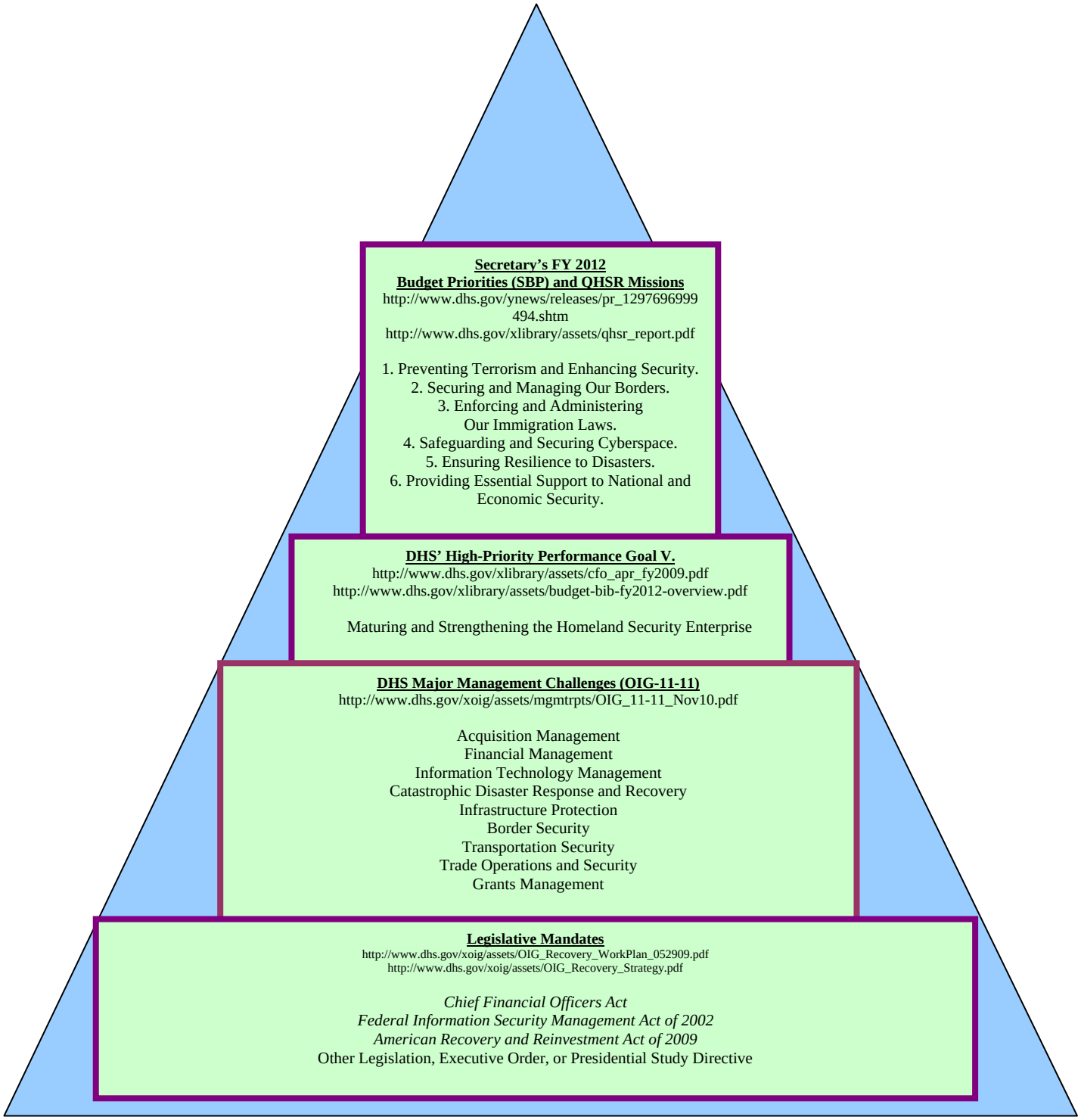
We focused on the Secretary's six budget priorities/missions for FY 2012:

Budget Priority/Mission 1: Preventing Terrorism and Enhancing Security
Budget Priority/Mission 2: Securing and Managing Our Borders
Budget Priority/Mission 3: Enforcing and Administering Our Immigration Laws
Budget Priority/Mission 4: Safeguarding and Securing Cyberspace
Budget Priority/Mission 5: Ensuring Resilience to Disasters
Budget Priority/Mission 6: Providing Essential Support to National and Economic Security

We also addressed the Department's high-priority performance goal (HPPG V) developed during the Department's Quadrennial Homeland Security Review (QHSR). The programs and functions associated with each of these missions are not an all-inclusive inventory of DHS' activities. Rather, they represent the core of DHS' mission and strategic objectives. By answering certain fundamental questions about each of these program and functional areas, we will determine how well DHS is performing, and we will be able to recommend improvements to the efficacy of DHS' programs and operations.

Figure 2 on the following page is a snapshot of the Department's FY 2012 budget priorities and missions—located at the top of the pyramid—and other fundamental performance goals leading toward these priorities. The principal foundation of our pyramid is our legislative mandates. Please refer to the Web links in the illustration for details.

Figure 2: OIG's FY 2012 Planning Priorities



Chapter 4 – Aligning OIG FY 2012 Projects With DHS' Priorities, Missions, and Mandates

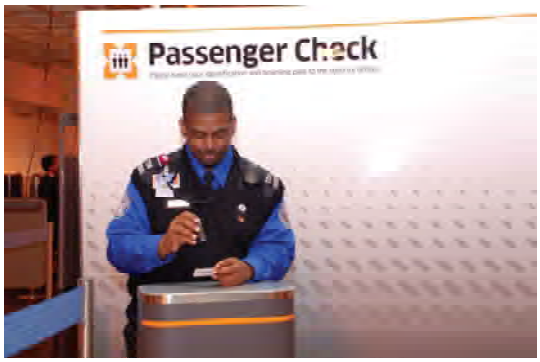
This section lists the FY 2012 Secretary's Budget Priorities (SBPs), the Department's six primary QHSR missions, HPPG V, and our allied FY 2012 projects. In addition, it identifies projects that will assess specific ARRA requirements.

The projects and the resulting reports should aid the Department in evaluating its progress on accomplishing its mission and the Secretary's goals, and on fulfilling ARRA requirements. Chapter 5, Project Narratives, describes each project and its objectives.

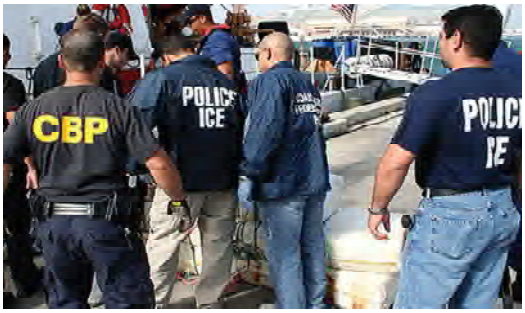
Secretary Napolitano's FY 2012 Budget Priorities/Missions and HPPG V

In February 2010, DHS completed the first QHSR. According to DHS, the QHSR "…established a unified, strategic framework for homeland security missions and goals, as well as the first Bottom-Up Review, which aligned DHS' programmatic activities and organizational structure to better serve those missions and goals. The third and final step of this process is the FY 2012 budget submission, which begins the next phase in strengthening DHS efforts to ensure a safe, secure, and resilient homeland." DHS' FY 2012 budget submission identified six DHS missions:

Budget Priority/Mission 1: Preventing Terrorism and Enhancing Security – Protecting the United States from terrorism is the cornerstone of homeland security. DHS' counterterrorism responsibilities focus on three goals: preventing terrorist attacks; preventing the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear materials and capabilities within the United States; and reducing the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards.

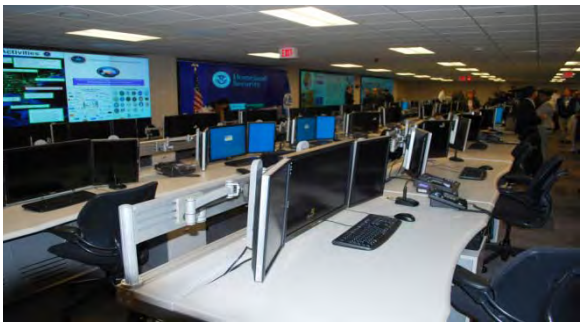


Budget Priority/Mission 2: Securing and Managing Our Borders – DHS secures the Nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and streamlining lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations.



Budget Priority/Mission 3: Enforcing and Administering Our Immigration Laws – DHS is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. The Department has fundamentally reformed immigration enforcement, focusing on identifying and removing criminal aliens who pose a threat to public safety and targeting employers who knowingly and repeatedly break the law.

Budget Priority/Mission 4: Safeguarding and Securing Cyberspace – By statute and presidential directive, DHS has the federal government lead to secure civilian government computer systems. It works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems. DHS analyzes and reduces cyber threats and vulnerabilities; distributes threat warnings; and coordinates the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe.



Budget Priority/Mission 5: Ensuring Resilience to Disasters – DHS provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster, or other large-scale emergency while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. DHS' efforts to build a ready and resilient Nation include fostering a community-oriented approach; bolstering information sharing; providing grants, plans, and training to our homeland security and law enforcement partners; and facilitating rebuilding and recovery along the gulf coast.

Budget Priority/Mission 6: Providing Essential Support to National and Economic Security – DHS leads and supports many activities that provide essential support to national and economic security, including maximizing collection of customs revenue, maintaining the safety and security of the marine transportation system, preventing the exploitation of children, providing law enforcement training, and coordinating the federal government's response to global intellectual property theft. DHS contributes to these elements of broader U.S. national and economic security while fulfilling its other homeland security missions.

DHS' High-Priority Performance Goal V – Maturing and Strengthening the Homeland Security Enterprise

Maturing and strengthening the homeland security enterprise—the collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private sector partners, as well as individuals, families, and communities—is critical to the Department's success in carrying out its core missions and operational objectives. This includes enhancing shared awareness of risks and threats, building capable communities, and fostering innovative approaches and solutions through cutting-edge science and technology, while continuing to foster a culture of efficiency and fiscal responsibility and streamline management across the Department.

OIG FY 2012 Projects Aligned With DHS' Priorities, Missions, and Mandates

The following projects and the resulting reports should aid the Department in assessing its progress toward achieving its FY 2012 budget priorities, missions, performance goals, and initiatives. Table 1 lists our projects in the same order as their narratives appear in chapter 5.

Table 1: OIG - New Projects, Planned Projects, and Projects in Progress

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
DIRECTORATE FOR MANAGEMENT							
New Projects							
DHS' Acquisition of Unmanned Aircraft Systems	OA	√	√				22
DHS' FY 2012 Compliance With the *Improper Payments Elimination and Recovery Act of 2010* (Mandatory)	OA	√		√			22
Other than Full and Open Competition Contracting During Fiscal Year 2012 (Mandatory)	OA	√	√	√			23
FY 2012 *Chief Financial Officers Act* Audits – Audits of DHS' Consolidated Financial Statements, Internal Control Over Financial Reporting, and the Individual Financial Statements of Select DHS Components (Mandatory)	OA	√	√	√			23
FY 2012 Office of National Drug Control Policy (ONDCP) Reviews at CBP, ICE, and USCG (Mandatory)	OA	√		√			24
IT Matters Related to the FY 2011 Financial Statement Audit – DHS Consolidated (Mandatory)	ITA		√	√			25
Annual Evaluation of DHS' Information Security Program for FY 2012 (Mandatory)	ITA			√			25
DHS' Data Center Consolidation Effort	ITA	√					25
Homeland Security Presidential Directive 7 (HSPD-7) – Follow-up	ITA	√					26

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Government 2.0/Web 2.0 – Social Media Use in DHS	ITA	√					26
Technical Security Evaluation of Hartsfield-Jackson International Airport	ITA	√					26
Internet Protocol Version 6 Implementation	ITA	√		-			26
Portable Device Security	ITA	√					27
DHS Financial Systems Consolidation Project	ITA	√	√				27
Projects in Progress							
DHS' Use of Other than Full and Open Competition Contracting During Fiscal Year 2011 (Mandatory)	OA	√	√	√		√	27
Tactical Communication Equipment	OA	√					28
DHS Risk Assessment Impact on Acquisition Processes FY 2011	OA	√	√				28
DHS' FY 2011 Compliance With the *Improper Payments Elimination and Recovery Act of 2010* (Mandatory)	OA	√		√			29
FY 2011 *Chief Financial Officers Act* Audits – Audits of DHS' Consolidated Financial Statements, Internal Control Over Financial Reporting, and the Individual Financial Statements of Select Components (Mandatory)	OA	√	√	√			29
FY 2011 ONDCP Reviews at CBP, USCG, and ICE (Mandatory)	OA	√		√			30
DHS IT Management Structure	ITA	√	√				31
Planning for IT Infrastructure at the St. Elizabeth's Homeland Security Complex	ITA	√					31

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS							
New Project							
Federal Protective Service's Acquisitions and Contracts (Congressional)	ISP	√	√		√		31
Projects in Progress							
NPPD's Use of FY 2006 Program Appropriations to Fund Shared Service Administrative Transactions (DHS Request)	OA	√					32
National Cybersecurity Center's (NCSC) Effort To Coordinate Cyber Operations Centers Across the Government	ITA	√					32
NPPD IT Management	ITA	√	√				32
Control Systems Cybersecurity	ITA	√					33
DHS' Implementation of Its Additional Cybersecurity Responsibilities	ITA	√					33
Controls Over the Use of Multiple Identities To Obtain Entrance Into the United States and Other Benefits	ITA	√	√				33
DHS' Efforts To Build Effective International Partnerships for Global Cybersecurity Policy	ITA	√					34
DIRECTORATE FOR SCIENCE AND TECHNOLOGY							
New Projects							
S&T's Research and Development Efforts To Address the Chemical, Biological, Radioactive, Nuclear, and Explosive Threat to Mass Transit Systems	ISP	√					34
S&T IT Management	ITA	√	√				35
Planned Project							
Goals and Metrics for S&T's Research Projects	ISP	√					35

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
FEDERAL EMERGENCY MANAGEMENT AGENCY							
New Projects							
FEMA's Integrated Training and Exercises	OA	√					35
State Homeland Security and Urban Area Grant Audits, 14 States (Mandatory)	OA	√	√	√			36
FEMA's Oversight of Grantees Using a Risk-Based Approach	OA	√					36
Preliminary Damage Assessments	EMO	√					36
Disaster Assistance Grants – Regional Offices	EMO	√					37
National Dam Safety Program	EMO	√					37
FEMA's Hazard Mitigation– Technical Assistance Programs	EMO	√					37
FEMA's Audit Resolution and Follow-up Process for Disaster Assistance Grant Audits	EMO	√					37
IT Matters Related to the FEMA Component of the FY 2011 DHS Financial Statement Audit (Mandatory)	ITA		√	√			38
FEMA Privacy Stewardship	ITA	√					38
Laptop Security	ITA	√					38
FEMA Wireless Security	ITA	√					38
Projects in Progress							
National Level Exercise 2011 – Lessons Learned	EMO	√					39
National Level Exercise – Federal Partner Participation	EMO	√					39
Continuing Effort To Audit States' Management of State Homeland Security Program and Urban Areas Security Initiative Program Grants, Georgia and Kansas (Mandatory)	OA	√		√			39
DHS' Emergency Support Function Roles and Responsibilities	EMO	√					40

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Flood Map Modernization Program	EMO	√					40
Hazard Mitigation Planning	EMO	√					40
Future Directions of FEMA's Temporary Housing Assistance Programs	EMO	√					40
Regional Office Inspections	EMO	√					41
Relationship Between Fusion Centers and Emergency Operations Centers	EMO	√					41
Status of Efforts To Expedite Disaster Recovery in Louisiana	EMO	√					41
FEMA's Progress in Implementing Disaster Responders' Credentials	EMO	√					42
Tracking Public Assistance Insurance Requirements	EMO	√					42
Capping Report – FY 2011 Public Assistance and Hazard Mitigation Grant Audits	EMO	√					42
OFFICE OF INSPECTOR GENERAL							
New Project							
DHS OIG IT Management	ITA	√					43
OFFICE OF INTELLIGENCE AND ANALYSIS							
New Projects							
DHS' Watchlisting Cell Efforts to Coordinate Departmental Nominations	ISP	√					43
Annual Evaluation of DHS' Information Security Program (Intelligence Systems-DNI) for FY 2012 (Mandatory)	ITA			√			43
Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2012 (Mandatory)	ITA			√			44
Laptop Security	ITA	√					44

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Projects in Progress							
DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers	ISP	√					44
Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2011 (Mandatory)							45
OFFICE OF POLICY							
New Project							
The Visa Waiver Program	ISP	√					45
TRANSPORTATION SECURITY ADMINISTRATION							
New Projects							
TSA National Explosives Detection Canine Team Program	OA	√					46
TSA Penetration Testing: Liquid Container Screening Systems	OA	√					46
TSA's Office of Inspections Efforts	OA	√					47
TSA Transportation Threat Assessment and Credentialing Office's Clearance and Suitability System (Congressional)	ISP	√			√		47
TSA's National Deployment Force – FY 2012 Follow-up (Congressional)	ISP	√			√		47
IT Matters Related to the TSA Component of the FY 2011 DHS Financial Statement Audit (Mandatory)	ITA		√	√			48
Planned Projects							
Workforce Strength and Deployment in TSA's Federal Air Marshal Service	ISP	√					48
Projects in Progress							
TSA Penetration Testing: Access Control at Domestic Airports (Congressional)	OA	√			√		49

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Policies and Procedures for Access Control to the Airport Security Identification Display Area (Congressional)	OA	√			√		49
Management and Oversight of Transportation Security at Honolulu International Airport (Congressional)	OA	√			√	√	50
Security Breaches at Newark Liberty International Airport (Congressional)	OA	√			√	√	50
Implementation and Coordination of the Secure Flight Program	ISP	√					50
Efficiency and Effectiveness of TSA's Visible Intermodal Prevention and Response (VIPR) Program	ISP	√					51
Allegations of Misconduct and Mismanagement Within TSA's Office of Global Strategies	ISP	√					51
The IT Insider Threat at TSA	ITA	√					51
UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES							
New Projects							
USCIS Worksite Enforcement Strategy	OA	√					52
Adjudication of I-140 Immigrant Worker Petitions	OA	√					52
Follow-up Review of the L Intra-company Transferee Visa Program (Congressional)	ISP	√			√		53
IT Matters Related to the USCIS Component of the FY 2011 DHS Financial Statement Audit (Mandatory)	ITA		√	√			53
Controls To Monitor the Approval of Naturalization Applications	ITA	√					54
Accuracy of Information Used in Programs Intended To Certify an Individual's Status for Employment and Other Benefits	ITA	√					54

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Planned Project							
DHS Administration of the T and U Visa Process	ISP	√					54
Projects in Progress							
Adjudication of I-130 Marriage-based Petitions	OA	√					55
Laptop Security	ITA	√	√				55
UNITED STATES COAST GUARD							
New Projects							
Efficacy of USCG's NAIS Acquisition Strategy	OA	√					55
Marine Accident Reporting to the USCG	OA	√					56
USCG's Annual Mission Performance (FY 2011) (Mandatory)	OA	√		√			56
IT Matters Related to the USCG Component of the FY 2011 DHS Financial Statement Audit (Mandatory)	ITA			√			57
USCG Privacy Stewardship	ITA	√					57
Projects in Progress							
USCG Sentinel Class Acquisition (Fast Response Cutter)	OA	√	√				57
USCG Reutilization and Disposal Program	OA	√					58
USCG Maritime Patrol Aircraft HC-144	OA	√				√	58
UNITED STATES CUSTOMS AND BORDER PROTECTION							
New Projects							
CBP Use of Radiation Portal Monitors at Seaports (Mandatory)	OA	√		√			58
Tracking and Analysis of CBP's In-Bond Cargo Processes (Congressional)	OA	√			√		59

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Border Patrol Agent Preparedness	OA	√					59
Tunnel Detection Strategy	OA	√					60
CBP Protection High-Security Bolt Seal Program (Congressional)	OA	√			√		60
IT Matters Related to the FY 2011 Financial Statement Audit of CBP (Mandatory)	ITA			√			60
The IT Insider Threat at CBP	ITA	√					61
Laptop Security	ITA	√					61
CBP TECS Modernization	ITA	√					
							61
Projects in Progress							
Free and Secure Trade Program – Continued Driver Eligibility	OA	√					61
Efficacy of CBP's Penalties Process (Congressional)	OA	√			√		62
Efficacy of the Office of Regulatory Audit Operations (Congressional)	OA				√		62
CBP's Management of Its *Federal Employees' Compensation Act* Program	OA	√					62
CBP's Textile Transshipment Enforcement	OA	√					63
Customs-Trade Partnership Against Terrorism (C-TPAT)	OA	√					63
CBP IT Management	ITA	√					63
CBP's Controls To Ensure the Suitability of Border Patrol Agents and CBP Officers	ITA	√					64
UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT							
New Project							
IT Matters Related to the ICE Component of the FY 2011 DHS Financial Statement Audit (Mandatory)	ITA			√			64

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Planned Project							
DHS' Expansion of the Visa Security Program to Additional Overseas Posts (Congressional)	ISP	√			√		64
Projects in Progress							
Secure Communities (Congressional and Department Request)	OA	√			√	√	65
Legislative Issues Surrounding the Secure Communities Program (Congressional and Department Request)	OA	√			√	√	65
MULTIPLE COMPONENTS							
New Project							
Temporary Protected Status	ISP	√					66
Planned Project							
Information Sharing on Foreign Nationals: Interior Immigration Enforcement and Activities	ISP	√					66
Projects in Progress							
DHS' Efforts To Address Weapons Smuggling to Mexico	ISP	√					67
DHS' Intelligence Community Members' Continuity of Operations and Intelligence Readiness Capabilities	ISP	√					67
AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009							
New Projects							
Review of Costs Claimed by Recipients of *American Recovery and Reinvestment Act* Funds Granted by FEMA for Fire Station Construction, Maritime Port Security, and Transit Security	OA	√				√	68

Project Title	OIG Office	Secretary s Budget Priorities /QHSR/ HPPG V/ DHS Request	Management Challenges	Legislative Mandate (Mandatory)	Congressional	ARRA	Page # in the Plan
Review of *American Recovery and Reinvestment Act* Funds Awarded by TSA to Airport Organizations for Checked Baggage Explosive Detection Systems and Checkpoint Explosive Detection Equipment	OA					√	68
Projects in Progress							
Fire Station Construction Grants Funded by the *American Recovery and Reinvestment Act of 2009*	OA	√				√	69
Alterations of Bridges Funded by the *American Recovery and Reinvestment Act of 2009*	OA	√				√	69
Improvements to Shore Facilities Funded by the *American Recovery and Reinvestment Act of 2009*	OA	√				√	70
Review of Costs Incurred by Recipients of *American Recovery and Reinvestment Act of 2009* Funds Within Selected States (Mandatory)	OA	√		√		√	70

Chapter 5 – Project Narratives

DIRECTORATE FOR MANAGEMENT

New Projects

DHS' Acquisition of Unmanned Aircraft Systems

The United States Customs and Border Protection (CBP) and the United States Coast Guard (USCG) are working together to acquire, test, and operate unmanned aircraft systems to meet mission requirements. Prior to the formation of the CBP and USCG Joint Program Office in 2008, the two DHS components had separate unmanned aircraft system programs with different results. In 2007, the USCG discontinued its program, citing development risks and lack of funding beyond 2007. CBP first employed an unmanned aerial system at the southwest border in 2005. As of 2009, the CBP Office of Air and Marine had acquired and is currently operating six unmanned aircraft systems, consisting of five Predator Bs and one Guardian, which was modified for maritime operations. The USCG is now exploring the Guardian to increase reconnaissance, surveillance, and targeting acquisition capabilities in maritime operating environments. By late 2010, CBP planned to acquire a seventh unmanned aircraft system to support interagency missions in 2011.

As of February 2011, DHS approved an acquisition strategy to acquire both cutter-based and land-based unmanned aircraft systems. The acquisition strategy emphasizes commonality with existing DHS and Department of Defense programs. The strategy precedes any future acquisition with adequate mission analysis, market research, alternatives analysis, testing, and evaluation.

Objective: Determine whether DHS' acquisition strategy for the acquisition of unmanned aircraft systems is cost effective. *Office of Audits*

DHS' FY 2012 Compliance With the *Improper Payments Elimination and Recovery Act of 2010* *(Mandatory)*

The *Improper Payments Elimination and Recovery Act of 2010* requires that DHS (1) publish a Performance and Accountability Report (PAR) or Agency Financial Report (AFR) for the most recent fiscal year and every three years thereafter and post that report and any accompanying materials required by OMB on the agency website; (2) conduct a program-specific risk assessment for each program or activity that conforms with section 3321 of Title 31 U.S.C. (if required); (3) publish improper payment estimates for all programs and activities identified as susceptible to significant improper payments under its risk assessment (if required); (4) publish programmatic corrective action plans in the PAR or AFR (if required); (5) publish and meet annual reduction targets for each program assessed to be at risk and measured for improper payments; (6) report a gross improper payment rate of less

than 10% for each program and activity for which an improper payment estimate was obtained and published in the PAR or AFR; and (7) report information on its efforts to recapture improper payments.

Objective: Determine whether, for FY 2012, the Department is in compliance with the *Improper Payments Elimination and Recovery Act of 2010*. *Office of Audits*

Other than Full and Open Competition Contracting During Fiscal Year 2012 ***(Mandatory)***

The *Competition in Contracting Act of 1984* promotes full and open competition in government contracting. In FY 2010, DHS obligated $1.3 billion for noncompetitive contracts. The Federal Acquisition Regulation provides specific instructions for federal agencies when using one of the seven exceptions for full and open competition, or noncompetitive contracting. Beginning in FY 2008, Congress included appropriate language for the Inspector General to review its agency's use of other than full and open competition contracting procedures from the prior year. We expect this requirement to continue in the 2012 fiscal year appropriation bill.

Prior Inspector General reports showed that the Department improved acquisition management oversight over the last 3 fiscal years, but acquisition personnel did not always follow federal regulations when awarding noncompetitive contracts. The Department continues to have some problems with insufficient evidence in contract files to support justifications and approvals, market research, acquisition planning, and consideration of contractor past performance prior to contract award.

Objective: Determine whether DHS acquisition personnel supported their use of other than full and open competition and contractors' past performance. *Office of Audits*

FY 2012 *Chief Financial Officers Act* Audits – Audits of DHS' Consolidated Financial Statements, Internal Control Over Financial Reporting, and the Individual Financial Statements of Select DHS Components ***(Mandatory)***

We will complete the required *Chief Financial Officers Act* audits related to the following consolidated and individual component financial statements:

- DHS Consolidated Audit Report – Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting. Final Report November 2012.
- DHS Consolidated Audit Report – Management Letter for DHS FY 2012 Consolidated Financial Statements Audit. Final Report January 2013.
- CBP Audit Report – Independent Auditors' Report on CBP's FY 2012 Consolidated Financial Statements. Final Report January 2013.
- CBP Audit Report – Management Letter for CBP's FY 2012 Consolidated Financial Statements Audit. Final Report March 2013.

- National Flood Insurance Program (NFIP) Audit Report – Independent Auditors' Report on NFIP's FY 2012 Consolidated Financial Statements. Final Report January 2013.
- NFIP Audit Report – Management Letter for NFIP's FY 2012 Consolidated Financial Statements. Final Report March 2013.
- FEMA Audit Report – FEMA's Management Letter for FY 2012 DHS Consolidated Financial Statement Audit. Final Report February 2013.
- Immigration and Customs Enforcement (ICE) Audit Report – ICE's Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- United States Citizenship and Immigration Services (USCIS) Audit Report – USCIS' Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- Federal Law Enforcement Training Center (FLETC) Audit Report – FLETC's Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- USCG Audit Report – Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- Transportation Security Administration (TSA) Audit Report – Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- Office of Financial Management (OFM) Audit Report – Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- National Protection and Programs Directorate (NPPD) Audit Report – Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- United States Secret Service (USSS) Audit Report – Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- Management Directorate Audit Report – Management Directorate's Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.
- Science and Technology (S&T) Audit Report – S&T's Management Letter for FY 2012 DHS Consolidated Financial Statements Audit. Final Report February 2013.

Objectives: Determine the fairness of presentations of DHS general and individual component FY 2012 financial statements by (1) obtaining an understanding of internal control over financial reporting, performing tests of those controls to determine audit procedures, and reporting on weaknesses identified during the audit; (2) performing tests of compliance with certain laws, regulations, and provisions of contracts or grant agreements to identify noncompliance that could affect financial statements; and (3) reporting noncompliance. Also, determine the effectiveness of DHS' internal controls over financial reporting. This audit addresses financial performance in the President's Management Agenda. *Office of Audits*

FY 2012 ONDCP Reviews 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 review assertions made by

management related to FY 2012 obligations for the National Drug Control Program. We will contract with independent public accounting firms to review CBP, USCG, and ICE 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 2012 ONDCP Management Assertions
- CBP Audit Report – Review of FY 2012 ONDCP Performance Summary Report
- ICE Audit Report – Review of FY 2012 ONDCP Management Assertions
- ICE Audit Report – Review of FY 2012 ONDCP Performance Summary Report
- USCG Audit Report – Review of FY 2012 ONDCP Management Assertions
- USCG Audit Report – Review of FY 2012 ONDCP Performance Summary Report

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

IT Matters Related to the FY 2011 Financial Statement Audit – DHS Consolidated ***(Mandatory)***

We contracted with an independent public accounting (IPA) firm to conduct DHS' annual financial statement audit. As a part of this annual audit, the IPA firm's information technology (IT) auditors perform a review of general and application controls in place over DHS' critical financial systems.

Objective: Determine the effectiveness of DHS' general and application controls over critical financial systems and data. *Office of IT Audits*

Annual Evaluation of DHS' Information Security Program for FY 2012 ***(Mandatory)***

In response to the increasing threat to information systems and the highly networked nature of the federal computing environment, Congress, in conjunction with OMB, requires an annual review and reporting of agencies' compliance with the requirements under FISMA. FISMA includes provisions aimed at further strengthening the security of the federal government's information and computer systems through the implementation of an information security program and the development of minimum standards for agency systems.

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

DHS' Data Center Consolidation Effort

OMB has recognized the benefits of data center consolidation and has established the Federal Data Center Consolidation Initiative. The DHS Chief Information Officer (CIO) was

appointed cochair of this initiative. Although the Department has taken steps to consolidate data centers, we reported previously that more work was needed.

Objective: Determine whether the Department's data center consolidation initiative is in compliance with the OMB initiative and is achieving stated goals. *Office of IT Audits*

Homeland Security Presidential Directive 7 (HSPD-7) – Follow-up

Prioritization of DHS' internal cyber critical infrastructure is a major challenge for the Under Secretary for Management. In March 2008, we reported that DHS had not prioritized its inventory of cyber critical infrastructure and needed to improve coordination among elements of the Management Directorate. During this follow-up review, we will examine progress made in addressing these issues over the last 3 years.

Objective: Determine the effectiveness DHS' actions to determine protection priorities for the Department's internal cyber critical infrastructure. *Office of IT Audits*

Government 2.0/Web 2.0 – Social Media Use in DHS

Several components in DHS are utilizing Government 2.0/Web 2.0 technologies, such as Facebook and Twitter, to facilitate internal and external information sharing. In addition, the implementation of a DHS enterprise-wide Government 2.0/Web 2.0 capability is a critical part of future strategic communication efforts. The use of Government 2.0/Web 2.0 technologies, however, has substantial information security and privacy challenges.

Objective: Determine the effectiveness of DHS' and its components' use of Government 2.0/Web 2.0 technologies. *Office of IT Audits*

Technical Security Evaluation of Hartsfield-Jackson International Airport

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 worksites. We have developed an agency-wide information system security evaluation program to assist with these efforts.

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

Internet Protocol Version 6 Implementation

In September 2010, OMB issued additional guidance to facilitate its goal of deploying Internet Protocol version 6 (IPv6) across the federal government. As part of OMB's new requirements, federal agencies must upgrade their public and external-facing servers and services (e.g., Web, email, domain name servers) to operationally use native IPv6 by the end

of FY 2012. In addition, agencies must upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to use IPv6 by the end of FY 2014.

Objective: Determine the progress that DHS has made to complete the IPv6 transition as required by OMB. *Office of IT Audits*

Portable Device Security

One of the largest internal threats to network security and a major source of concern for DHS is the use of portable media devices. Portable devices allow users to copy, store, and transport information, but they are also capable of carrying malware and spyware. Once connected to a network, infected devices may enable the spread of malware throughout that network. As technology continues to improve, new devices with updated features, such as smartphones, are developed. Smartphones allow the user to access many applications within a single portable device.

Objective: Determine the progress that the Department has made in addressing the emerging threat and mishandling of sensitive and classified information as a result of the increased use of portable devices through policy and security controls. *Office of IT Audits*

DHS Financial Systems Consolidation Project

DHS canceled its Transformation and Systems Consolidation program, and now must develop a new approach to reengineering its financial systems and processes and consolidating them across the enterprise.

Objective: Determine the progress DHS is making in reengineering and consolidating its core financial processes and systems. *Office of IT Audits*

Directorate for Management
Projects in Progress

DHS' Use of Other than Full and Open Competition Contracting During Fiscal Year 2011 ***(Mandatory)***

The *Competition in Contracting Act of 1984* promotes full and open competition in government contracting. In FY 2010, DHS obligated $1.3 billion for noncompetitive contracts. The Federal Acquisition Regulation provides specific instructions for federal agencies when using one of the seven exceptions for full and open competition, or noncompetitive contracting. Beginning in FY 2008, Congress included language for the Inspector General to review its agency's use of other than full and open competition contracting procedures from the prior year.

Prior Inspector General reports showed that the Department improved acquisition management oversight over the last 3 fiscal years, but acquisition personnel did not always

follow federal regulations when awarding noncompetitive contracts. The Department continues to have some problems with insufficient evidence in contract files to support justifications and approvals, market research, acquisition planning, and consideration of contractor past performance prior to contract award.

Objective: Determine whether, for FY 2011, DHS acquisition personnel supported their use of other than full and open competition and contractors past performance. *Office of Audits*

Tactical Communication Equipment

DHS is in the process of upgrading its tactical communications equipment using funds appropriated through the annual funding process and ARRA. The Department is responsible for ensuring that all its components can effectively communicate during normal and emergency situations and with other federal departments and state and local officials. Ten years after September 11, 2001, many department personnel still operate using legacy, analog land mobile radio systems and other equipment that is not interoperable with the components of other federal and state emergency responders. Obsolete, noninteroperable equipment may inhibit and jeopardize effective emergency responses and place official responders, as well as civilians, at a greater risk during a national or local emergency. We plan to evaluate the Department's process for ensuring that component purchases of tactical communications are coordinated and include an established standard for communication equipment that ensures interoperability. We also plan to evaluate the Department's process for ensuring that component purchases of tactical communications are coordinated and include an established standard for communication equipment that ensures interoperability.

Objective: Determine the effectiveness of the Department's oversight of component acquisition of tactical communication equipment to ensure interoperability. *Office of Audits*

DHS Risk Assessment Impact on Acquisition Processes FY 2011

DHS relies on goods and services contractors to help fulfill many of its critical mission areas. Effective acquisition management is vital to achieving DHS' overall mission. Acquisition management requires a sound management infrastructure to identify mission needs and develop strategies to fulfill those needs while balancing cost, schedule, and performance. To effectively implement any acquisition program, the DHS Office of Chief Information Officer, component heads of contracting activity, contracting officers, and contracting officer's technical representatives (COTRs) need to understand the risks present in an acquisition program and develop a life cycle management plan to reduce risks throughout the acquisition life cycle. This calls for the continual assessment of program risks beginning with the initial phase of an acquisition program, and the development of risk management approaches before moving forward with the next acquisition phase.

Objective: Determine whether DHS and its components conduct effective risk management to ensure that program cost, schedule, and performance objectives are achieved at every stage in the life cycle of the acquisition. *Office of Audits*

DHS' FY 2011 Compliance With the *Improper Payments Elimination and Recovery Act of 2010* *(Mandatory)*

The *Improper Payments Elimination and Recovery Act of 2010* requires that DHS (1) publish a PAR or AFR for the most recent fiscal year and post that report and any accompanying materials required by OMB on the agency website; (2) conduct a program-specific risk assessment for each program or activity that conforms with section 3321 of Title 31 U.S.C. (if required); (3) publish improper payment estimates for all programs and activities identified as susceptible to significant improper payments under its risk assessment (if required); (4) publish programmatic corrective action plans in the PAR or AFR (if required); (5) publish and meet annual reduction targets for each program assessed to be at risk and measured for improper payments; (6) report a gross improper payment rate of less than 10% for each program and activity for which an improper payment estimate was obtained and publish in the PAR or AFR; and (7) report information on its efforts to recapture improper payments.

Objective: Determine whether, for FY 2011, the Department is in compliance with the *Improper Payments Elimination and Recovery Act of 2010*. *Office of Audits*

FY 2011 *Chief Financial Officers Act* Audits – Audits of DHS' Consolidated Financial Statements, Internal Control Over Financial Reporting, and the Individual Financial Statements of Select DHS Components *(Mandatory)*

We will complete the required *Chief Financial Officers Act* audits related to the following consolidated and individual component financial statements:

- DHS Consolidated Audit Report – Independent Auditors' Report on DHS FY 2011 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting. Final Report November 2011.
- DHS Consolidated Audit Report – Management Letter for DHS FY 2011 Consolidated Financial Statements Audit. Final Report January 2012.
- CBP Audit Report – Independent Auditors' Report on CBP's FY 2011 Consolidated Financial Statements. Final Report January 2012.
- CBP Audit Report – Management Letter for CBP's FY 2011 Consolidated Financial Statements Audit. Final Report March 2012.
- NFIP Audit Report – Management Letter for NFIP's FY 2011 Consolidated Financial Statements. Final Report March 2012.
- FEMA Audit Report – FEMA's Management Letter for FY 2011 DHS Consolidated Financial Statement Audit. Final Report February 2012.
- Immigration and Customs Enforcement (ICE) Audit Report – ICE's Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- United States Citizenship and Immigration Services (USCIS) Audit Report – USCIS' Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.

- Federal Law Enforcement Training Center (FLETC) Audit Report – FLETC's Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- USCG Audit Report – Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- Transportation Security Administration (TSA) Audit Report – Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- Office of Financial Management (OFM) Audit Report – Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- National Protection and Programs Directorate (NPPD) Audit Report – Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- United States Secret Service (USSS) Audit Report – Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- Management Directorate Audit Report – Management Directorate's Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.
- Science and Technology (S&T) Audit Report – S&T's Management Letter for FY 2011 DHS Consolidated Financial Statements Audit. Final Report February 2012.

Objectives: Determine the fairness of presentations of DHS general and individual component FY 2011 financial statements by (1) obtaining an understanding of internal control over financial reporting, performing tests of those controls to determine audit procedures, and reporting on weaknesses identified during the audit; (2) performing tests of compliance with certain laws, regulations, and provisions of contracts or grant agreements to identify noncompliance that could affect financial statements; and (3) reporting noncompliance. Also, determine the effectiveness of DHS' internal controls over financial reporting. *Office of Audits*

FY 2011 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 review assertions made by management related to FY 2011 obligations for the National Drug Control Program. We will contract with independent public accounting firms to review CBP, USCG, and Immigration ICE 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 2011 ONDCP Management Assertions
- CBP Audit Report – Review of FY 2011 ONDCP Performance Summary Report
- ICE Audit Report – Review of FY 2011 ONDCP Management Assertions
- ICE Audit Report – Review of FY 2011 ONDCP Performance Summary Report
- USCG Audit Report – Review of FY 2011 ONDCP Management Assertions
- USCG Audit Report – Review of FY 2011 ONDCP Performance Summary Report

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

DHS IT Management Structure

Creating a single infrastructure for effective communications and information exchange remains a major management challenge for the DHS CIO. In our September 2008 report, *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain*, we reported that the Department had made progress with its IT management practices and solidified the DHS CIO's IT management authority. However, we identified issues and made recommendations related to the DHS Office of the CIO's staffing levels, the DHS CIO's control of department-wide IT alignment and budgets, and component-level strategic planning. During this follow-up review, we will examine progress made in addressing these issues and recommend actions to be taken, as appropriate.

Objective: Assess progress made in establishing CIO oversight and authority, achieving IT integration, improving IT management functions, and addressing our prior report recommendations. *Office of IT Audits*

Planning for IT Infrastructure at the St. Elizabeths Homeland Security Complex

DHS is consolidating its key leadership, policy, management, programs, and mission execution personnel to the St. Elizabeths campus, located in Southeast Washington, DC. As part of this effort, DHS awarded an $867 million contract to General Dynamics to install, test, and operate a secure IT infrastructure throughout this campus.

Objective: Determine the effectiveness of DHS planning to develop and implement an IT infrastructure at its St. Elizabeths headquarters campus. *Office of IT Audits*

DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS

New Project

Federal Protective Service's Acquisitions and Contracts ***(Congressional)***

The Federal Protective Service (FPS), a National Protection and Programs Directorate component, is a federal law enforcement agency that provides integrated security and law enforcement services to federally owned and leased buildings, facilities, properties, and other assets. To meet its mission, the FPS contracts with private companies for guard services. The FPS uses the Risk Assessment and Management Program (RAMP) to collect, analyze, and share risk data with inspectors and officers charged with securing federal facilities. Concerns that RAMP is not meeting expectations and a serious security breach at Detroit's Patrick V. McNamara Federal Building have led Congressman Bennie G. Thompson, ranking member of the Committee on Homeland Security, to question how FPS awards and oversees its contracts. Congressman Thompson requested that we undertake this review.

Objectives: Determine (1) whether the FPS provided sufficient oversight of the RAMP contract; (2) the plausibility of opening the RAMP contract to full and open competition; (3) the amount spent on the program; (4) the extent to which the FPS has deployed the program; and (5) whether the actions of the FPS and the contractor responsible for guard services following the security breach of the Patrick V. McNamara Federal Building sufficiently remedied the causes of the breach and the performance of the contractor. *Office of Inspections*

Directorate for National Protection and Programs
Projects in Progress

NPPD's Use of FY 2006 Program Appropriations to Fund Shared Service Administrative Transactions ***(DHS Request)***

The DHS Acting Chief Financial Officer (CFO) has requested that we conduct a formal investigation and provide a report on *Anti-Deficiency Act* violations at the NPPD (formerly the Preparedness Directorate). The possible violations involve the NPPD's use of FY 2006 program appropriations to fund shared service administrative transactions.

Objective: Determine whether an *Anti-Deficiency Act* violation occurred regarding the NPPD's use of FY 2006 program appropriations to fund shared service administrative transactions. *Office of Audits*

National Cybersecurity Center's (NCSC) Effort To Coordinate Cyber Operations Centers Across the Government

With the increasing threats to the Nation's information infrastructures, it has become more vital for government information security offices and strategic operations centers to share data regarding malicious activities against federal systems, have a better understanding of the entire threat to government systems, and take maximum advantage of each organization's unique capabilities to produce the best possible overall national cyber defense strategy. The Comprehensive National Cybersecurity Initiative (CNCI) provides the key means to enable and support shared situational awareness and collaboration across six centers, including the Department of Defense, National Security Agency, and intelligence communities, which are responsible for carrying out U.S. cyber activities.

Objective: Determine the progress that NCSC has made in coordinating cyber operations centers across the government. *Office of IT Audits*

NPPD IT Management

NPPD's mission is to lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. In support of this mission, the NPPD CIO approves, oversees, and monitors IT investments for Cyber Security and Communications, the United States Visitor and Immigration Status Indication Technology (US-VISIT)

program, Infrastructure Protection, Federal Protective Service, and Risk Management and Analysis. NPPD also performs system engineering life cycle reviews.

Objective: Determine the effectiveness of NPPD's IT management and investment activities supporting its effort to protect the Nation's physical and cyber infrastructure. *Office of IT Audits*

Control Systems Cybersecurity

Control systems, also known as supervisory control and data acquisition systems, are used to gather and analyze real-time data to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation. NCSC faces challenges in reducing the cybersecurity risks to the Nation's control systems. For example, in 2009, we identified deficiencies and areas of improvement in DHS' efforts to implement a cybersecurity program for control systems.

Objective: Evaluate the progress DHS has made in addressing cybersecurity issues and coordinating the response efforts for control systems between the public and private sectors. *Office of IT Audits*

DHS' Implementation of Its Additional Cybersecurity Responsibilities

To improve the security posture of federal agencies, OMB has recently delegated DHS additional cybersecurity responsibilities. The Federal Network Security (FNS) branch of NPPD has been tasked to serve as the focal point for implementing the additional responsibilities. For example, FNS is responsible for implementing aspects of the President's HSPD-23 and CNCI. In addition, FNS has established a security management program to prevent attacks against federal agencies' networks and provides support to implement OMB's initiatives to improve cybersecurity, such as FISMA support management and Trusted Internet Connections.

Objective: Determine whether the FNS branch of NPPD has established an effective program to implement its additional cybersecurity responsibilities to improve the security posture of the federal agencies' networks. *Office of IT Audits*

Controls Over the Use of Multiple Identities To Obtain Entrance Into the United States and Other Benefits

To support DHS' mission of protecting our Nation, US-VISIT collects biometrics—digital fingerprints and a photograph—from international travelers at U.S. visa-issuing posts and ports of entry. This information helps federal, state, and local government decision makers determine whether a person is eligible to receive a visa to enter the United States, deter identity fraud, and prevent criminals and immigration violators from crossing our borders. However, US-VISIT does not use the biometric information it collects to determine whether individuals used different biographic information—such as different names or dates of birth—to seek entry into the United States.

Objective: Determine the extent to which the same individuals enter the United States using different biographic identities. *Office of IT Audits*

DHS' Efforts To Build Effective International Partnerships for Global Cybersecurity Policy

Because cyberspace crosses geographic and jurisdictional boundaries, the United States must work actively with countries around the world to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations. More than a dozen international organizations address issues concerning the information and communications infrastructure. Thus, addressing network security issues requires a public-private partnership as well as international cooperation and norms.

The National Strategy to Secure Cyberspace recognizes that securing cyberspace is a global matter because of the interconnectedness of the world's computer systems. Furthermore, the recently released U.S. International Strategy for Cyberspace outlines the U.S. vision for the future of cyberspace, and sets an agenda for partnering with other nations and peoples to realize it.

Objective: Determine the effectiveness of DHS' efforts to build partnerships within the international community to facilitate cooperation and the development of cyberspace policy and norms as they relate to the security and stability of the global information and communications infrastructure. *Office of IT Audits*

DIRECTORATE FOR SCIENCE AND TECHNOLOGY

New Projects

S&T's Research and Development Efforts To Address the Chemical, Biological, Radioactive, Nuclear, and Explosive Threat to Mass Transit Systems

Every day, more than 14 million Americans use public transportation to commute. It is widely known that mass transit systems are targets for terrorist attacks. Thus, each day, millions of transit users are exposed to the threat of terrorism. This review will explore S&T's role in assisting the TSA, NPPD, Domestic Nuclear Detection Office, and the Office of Health Affairs to execute the shared mission of detecting and minimizing the threat of chemical, biological, radioactive, nuclear, and explosive materials use against mass transit systems.

Objectives: Determine (1) S&T's research and development efforts for detecting chemical, biological, radiological, nuclear, and explosive agents in the mass public transit environment; and (2) the extent to which S&T and other DHS components are coordinating in research and development. *Office of Inspections*

S&T IT Management

S&T's mission is to strengthen America's security and resiliency by providing knowledge products and innovative homeland security technology solutions. S&T captures the Department's technical requirements and performs advanced critical homeland security technology research, development, and transition activities.

Objective: Determine the effectiveness of S&T's IT management activities supporting its critical homeland security technology requirements gathering, research, development, and transition activities. *Office of Information Technology Audits*

Directorate for Science and Technology
Planned Projects

Goals and Metrics for S&T's Research Projects

Congress is concerned that DHS does not have a clear risk-based methodology to determine what projects to fund, how much to fund, and how to evaluate a project's effectiveness or usefulness. Without metrics, it becomes difficult for Congress to justify increases in programmatic funding.

Objectives: Determine (1) how S&T sets goals for research projects, (2) how S&T measures research project success, and (3) whether S&T's processes for setting goals and measuring success should be improved. *Office of Inspections*

FEDERAL EMERGENCY MANAGEMENT AGENCY

New Projects

FEMA's Integrated Training and Exercises

FEMA requires state grantees to support training and exercises that contribute to improved preparedness. However, approved training coursework is limited mainly to Incident Command System training, which may not be comprehensive enough to address first responder needs. Exercises are conducted only by subgrantees with the financial resources to do so. Other subgrantees' participation depends on their financial ability to do so. Therefore, fully integrated exercises are rarely conducted.

Objective: Determine whether improvements are needed to ensure that FEMA's training and exercise program effectively contributes to state preparedness. *Office of Audits*

State Homeland Security and Urban Area Grant Audits, 14 States ***(Mandatory)***

Public Law (P.L.) 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 between FY 2008 and FY 2014. As part of our continuing effort to ensure the effective and appropriate use of FEMA-administered grants, we will review states' and urban areas' management of homeland security funds through the initiation of 14 audits in previously unaudited states.

Objective: Determine whether selected states have effectively and efficiently implemented the State Homeland Security Program and, where 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 Oversight of Grantees Using a Risk-Based Approach

A recent DHS OIG audit of FEMA grant funds identified several key indicators that could have increased a grant recipient's need for additional oversight, including unresolved issues raised by the Technical Evaluation Panel during the application process and being a first-time grant recipient. Despite these indicators, FEMA did not elevate the recipient to a level requiring direct oversight, and therefore did not initiate proactive actions to ensure that this recipient was compliant with the grant terms, such as implementing, evaluating, and administering the grant as expected. Since that time, FEMA reportedly has moved to a risk-based approach to identify and select grantees for desk reviews and site visits. With approximately $3 billion awarded each year for homeland security preparedness grants, FEMA must mitigate its risk for loss and implement an effective methodology to identify and closely monitor grantees with increased risk.

Objective: Determine whether FEMA's monitoring and oversight plans, including its methodology for identifying and selecting grantees for review and the factors used in the selection process, are adequate for the proper oversight of grantees with increased risk. *Office of Audits*

Preliminary Damage Assessments

A federal disaster is declared when an incident occurs that is beyond the capability of state and local governments to respond. Preliminary damage assessments are used to determine whether a federal disaster should be declared, making federal funds available to the state.

Objective: Assess the accuracy of the preliminary damage assessments used as the basis for presidential disaster declarations. *Office of Emergency Management Oversight*

Disaster Assistance Grants – Regional Offices

FEMA awards disaster assistance grants to individuals and states, local governments, and certain nonprofits. We will perform audits of grantees and subgrantees, focusing on grants with potential for problems and areas that are of interest to Congress and FEMA.

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

National Dam Safety Program

The National Dam Safety Program is a FEMA-led partnership to encourage individual and community responsibility for dam safety through grant assistance to the states for dam safety research and training.

Objective: Determine the extent of FEMA efforts with state, local, and tribal governments to reduce the risk of property damage and loss of lives caused by dam failure and to assess the cost-effectiveness of the National Dam Safety Program. *Office of Emergency Management Oversight*

FEMA's Hazard Mitigation–Technical Assistance Programs

The Hazard Mitigation–Technical Assistance Programs (HM-TAP) is the third-largest disaster program in FEMA. It is composed of four contractors, each with a 5-year contract up to $150 million. The contracts allow for both pre- and post-disaster mitigation activities.

Objective: Determine the efficacy of FEMA's management of the hazard mitigation–technical assistance program contractors, including policies and procedures for (1) awarding individual task orders, (2) monitoring contractor performance, and (3) certifying contractor billings. *Office of Emergency Management Oversight*

FEMA's Audit Resolution and Follow-up Process for Disaster Assistance Grant Audits

OIG disaster assistance grant reports question millions of dollars in charges. Effective and timely FEMA action is necessary to recover these funds. DHS OIG has more than 100 open grant reports and more than 300 open recommendations with questioned costs over $200 million.

Objective: Determine the processes and procedures followed by FEMA's regional offices to implement recommendations and address the issues that have hindered progress in closing recommendations and reports. *Office of Emergency Management Oversight*

IT Matters Related to the FEMA Component of the FY 2011 DHS Financial Statement Audit ***(Mandatory)***

We contracted with an IPA firm to conduct DHS' annual financial statement audit. As 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: Determine the effectiveness of FEMA's general and application controls over critical financial systems and data. *Office of IT Audits*

FEMA Privacy Stewardship

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 supporting our citizens and first responders to prepare for, protect against, respond to, recover from, and mitigate all hazards, FEMA collects, shares, and uses sensitive personally identifiable information. To promote compliance with federal privacy regulations, the FEMA Privacy Office works with programs to steward and instill a culture of privacy.

Objectives: Determine whether FEMA (1) instills a privacy culture that is effective in protecting sensitive personally identifiable information and (2) ensures compliance with federal privacy regulations. *Office of IT Audits*

Laptop Security

As the weight and price of laptops have decreased and their computing power and ease of use have increased, so has their popularity for use by government employees, particularly for telework. DHS and its components rely heavily on laptop computers for conducting business in support of its mission. The mobility of laptops has increased the productivity of DHS' workforce, but at the same time has increased the risk of theft, unauthorized data disclosure, and virus infection.

Objective: Determine whether FEMA has implemented an effective program to protect the security and integrity of its laptop computers. *Office of IT Audits*

FEMA Wireless Security

Wireless networking (i.e., 802.11x [Wi-Fi], Bluetooth, IrDA [infrared], and cellular) frees computer users from the shackles of network cables. In particular, wireless technologies can provide productivity improvements for mobile FEMA employees. However, the technologies can also expose sensitive information systems to potential security vulnerabilities when wireless devices are not secured properly.

Objective: Determine whether FEMA has implemented effective controls to ensure that sensitive information processed by its wireless networks and devices is protected from potential exploits. *Office of IT Audits*

Federal Emergency Management Agency
Projects in Progress

National Level Exercise 2011 – Lessons Learned

National Level Exercises (NLEs), formerly designated as Top Officials exercises, are designed to reinforce the Nation's ability to prepare for, prevent, respond to, and recover from large-scale terrorist attacks or natural disasters. These exercises test high-level government officials' response to simulated attacks and disasters and identify corrective actions resulting from problems discovered during these exercises. NLE 2011 simulated a catastrophic earthquake in the central U.S. region of the New Madrid Seismic Zone.

Objective: Determine whether FEMA incorporated lessons learned and corrective actions from prior exercises and disasters into its NLE 2011 exercise. *Office of Emergency Management Oversight*

National Level Exercise – Federal Partner Participation

NLEs test the Nation's and high-level government officials' ability to prepare for, prevent, respond to, and recover from large-scale terrorist attacks or natural disasters. These exercises help identify needed corrective actions. NLE 2011 simulated a catastrophic earthquake in the central U.S. region of the New Madrid Seismic Zone.

Objective: Provide a descriptive report on federal participation in NLE 2011, emphasizing the importance of assessing every department's or agency's preparedness.

Continuing Effort To Audit States' Management of State Homeland Security Program and Urban Areas Security Initiative Program Grants, Georgia and Kansas *(Mandatory)*

The Implementing Recommendations of the *9/11 Commission Act of 2007* require us to audit each state that receives State Homeland Security Program and Urban Areas Security Initiative grant funds at least once between FY 2008 and FY 2014. As part of our continuing effort to ensure the effective and appropriate use of grants administered by FEMA, we will review states' and urban areas' management of homeland security funds through audits in previously unaudited states.

Objective: Determine whether selected states have effectively and efficiently implemented the State Homeland Security Program and, where applicable, the Urban Areas Security Initiative program; achieved the goals of the programs; and spent funds according to grant requirements. *Office of Audits*

DHS Emergency Support Function Roles and Responsibilities

The National Response Framework (NRF) presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies—from the smallest incident to the largest catastrophe. The NRF includes 15 Emergency Support Function (ESF) Annexes that group federal resources and capabilities into functional areas that are most frequently needed in a national response (e.g., Transportation, Firefighting, and Mass Care). DHS has coordinating and/or primary responsibilities for five ESFs: (1) ESF-2 – Communications, (2) ESF-9 – Search and Rescue, (3) ESF-10 – Oil and Hazardous Materials Response, (4) ESF-14 – Long-Term Community Recovery, and (5) ESF-15 – External Affairs.

Objective: Determine to what extent DHS is prepared to fulfill its ESF roles and responsibilities outlined in the NRF. *Office of Emergency Management Oversight*

Flood Map Modernization Program

FEMA uses flood maps to designate areas prone to flooding, called Special Flood Hazard Areas. The map modernization program is a national effort, performed by contractors, to develop new flood maps using old flood information as a baseline. According to our 2005 audit report, 70% of FEMA's maps were at least 10 years old. Many of the updated maps are based on partial or outdated information, which results in confusion and unanticipated expense for homeowners who might unknowingly find themselves in a Special Flood Hazard Area. FEMA contracts out this effort, which is estimated to exceed $1 billion.

Objective: Ascertain to what extent FEMA has followed Federal Acquisition Regulation requirements in ensuring the effective and wise use of taxpayer funds while administering the NFIP's map modernization program. *Office of Emergency Management Oversight*

Hazard Mitigation Planning

States and localities are required to have mitigation plans approved by FEMA to qualify for various federal grants and programs.

Objective: Determine whether the current approach to state and local hazard mitigation planning is efficient and effective. *Office of Emergency Management Oversight*

Future Directions of FEMA's Temporary Housing Assistance Programs

FEMA encountered serious problems in providing temporary housing to Hurricane Katrina victims, including disturbances at group housing sites, criticism for evicting tenants after the legally imposed 18-month deadline, and the much-publicized health concerns of travel trailers beset with mold and formaldehyde. Since then, FEMA and other federal and nonfederal stakeholders have developed strategies to deal with future temporary housing needs.

Objectives: Determine the progress made in recent FEMA efforts such as interim housing initiatives in the National Disaster Housing Strategy, which include the Disaster Housing Implementation Plan and the accompanying 2010 Comprehensive Disaster Housing Concept of Operations; assess the progress in efforts such as Noncongregate Housing, the Alternative Housing Pilot Program, and ready-for-dispatch mobile units; and evaluate state and local partners' commitment to those programs. *Office of Emergency Management Oversight*

Regional Office Inspections

FEMA's regional offices are on the front lines of facilitating emergency management programs. FEMA has begun a process of realigning key operational responsibilities and authorities to the regional offices. For example, FEMA's regional offices now have the authority to issue mission assignments in excess of $10 million and select and hire staff in senior regional positions.

Objectives: Assess the realignment of responsibilities and authorities to FEMA's 10 regional offices and determine whether these offices (1) have the resources to meet their responsibilities, (2) are operating in a manner consistent with new authorities, and (3) are appropriately applying policies and procedures directed and approved by FEMA headquarters. *Office of Emergency Management Oversight*

Relationship Between Fusion Centers and Emergency Operations Centers

FEMA supports state and local fusion centers, as well as state/local Emergency Operations Centers. Where a state or local jurisdiction has both a fusion center and an Emergency Operations Center, there can be challenges in ensuring that vital information is shared among law enforcement, intelligence, and emergency management personnel in a timely manner.

Objective: Determine whether fusion centers and Emergency Operations Centers interact and share information in an effective, efficient, and economical manner. *Office of Emergency Management Oversight*

Status of Efforts To Expedite Disaster Recovery in Louisiana

Under the PA program, FEMA provides grants to state, local, and tribal governments and specific types of nonprofit organizations. FEMA provides funds to state governments (grantees), which in turn provide funds to local governments (applicants). There have been significant delays in providing PA funding to applicants in Louisiana.

Objective: Determine the extent to which FEMA, grantees, and applicants are working together to carry out the PA program effectively and efficiently to rebuild the gulf coast after Hurricane Katrina. *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 in which 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 before, during, and since Hurricane Katrina. Credentialing is mandated by the National Incident Management System and in accord with HSPD-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*

Tracking Public Assistance Insurance Requirements

According to title 44, C.F.R. 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*

Capping Report – FY 2011 Public Assistance and Hazard Mitigation Grant Audits

Each year our Capping Report summarizes the results of our PA grant audits to provide a snapshot of the problems we encountered. Our FY 2011 report will identify frequently reported audit findings and quantify the financial impact of these findings. This year's report will include a summary of our audits of FEMA Hazard Mitigation grants.

***Objective*:** Summarize the results of PA and Hazard Mitigation disaster grant audits issued in FY 2011, identify frequently occurring audit findings, and quantify the financial impact of these findings. *Office of Emergency Management Oversight*

OFFICE OF INSPECTOR GENERAL

New Project

DHS OIG IT Management

The DHS OIG's mission is to promote effectiveness, efficiency, and economy in DHS' programs and operations, and to prevent and detect fraud, abuse, mismanagement, and waste. In support of the OIG's mission, its Information Technology Division is responsible for managing, directing, and providing overall IT and telecommunications program support to OIG programs, operations, and functions.

Objective: Determine the effectiveness of DHS OIG's IT management activities in support of its department-wide mission. *Office of IT Audits*

OFFICE OF INTELLIGENCE AND ANALYSIS

New Projects

DHS' Watchlisting Cell Efforts to Coordinate Departmental Nominations

Federal departments and agencies provide information to the Office of the Director of National Intelligence's National Counterterrorism Center (NCTC) as one means of keeping our Nation safe. In December 2010, DHS established the Watchlisting Cell (WLC) within the Office of Intelligence and Analysis to centralize and coordinate this function.

Objectives: Determine (1) whether the WLC is timely, effective, and efficient in submitting DHS nominations to the NCTC; (2) whether the information provided to external partners is complete, accurate, and timely; (3) the effect that establishing the WLC has had on the DHS component nomination process; and (4) whether the WLC has developed and communicated effective policies and procedures for coordinating nomination submissions within DHS. *Office of Inspections*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems-DNI) for FY 2012 ***(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 Director of National Intelligence (DNI), the CIO, and OMB, requires an annual evaluation and reporting of the security program over agencies' intelligence systems. FISMA and the Director, Central

Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, requirements will be used as criteria for the evaluation. Prior audits identified problems in the areas of management oversight, Plan of Action and Milestones process, and the implementation of a formal security training and awareness program for intelligence personnel.

Objective: Determine what progress DHS has made in resolving weaknesses cited in the prior year OIG review. *Office of IT Audits*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2012 ***(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 DNI, the CIO, and OMB, requires an annual evaluation and reporting of the security program over agencies' intelligence systems. FISMA and the Director, Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, requirements will be used as criteria for the evaluation. Prior audits identified problems in the areas of management oversight, Plan of Action and Milestones process, and the implementation of a formal security training and awareness program for intelligence personnel.

Objective: Determine what progress DHS has made in resolving weaknesses cited in the prior year OIG review. *Office of IT Audits*

Laptop Security

While DHS has increased its reliance on laptop computers for conducting business in support of its mission and for facilitating telework with positive results; the risk of theft, unauthorized data disclosure, and virus infection has also increased.

Objective*:* Determine whether the Office of Intelligence and Analysis (I&A) has implemented an effective program to protect the security and integrity of its laptop computers. *Office of IT Audits*

Office of Intelligence and Analysis
Projects in Progress

DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers

To promote greater information sharing and collaboration among federal, state, and local intelligence and law enforcement entities, state and local authorities established fusion centers throughout the country. These centers are a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity. This review focuses on I&A's State and Local Program Office (SLPO) strategies,

execution, and ability to fulfill its role. On July 31, 2009, DHS' Secretary approved DHS' recommitment to the State, Local, and Regional Fusion Center Initiative, and to overcome its past deficiencies by instituting a well-coordinated, department-wide approach to support and interact with fusion centers. DHS established the SLPO in December 2009 to ensure coordination across all DHS components toward the twin priorities of strengthening fusion centers and DHS intelligence products. We will examine the development, standup, and execution of the SLPO and assess program office effectiveness in fulfilling DHS' goal to achieve a renewed, revised, and enhanced information sharing and communication capability with fusion centers.

Objectives: Determine whether (1) the development of the SLPO satisfies the intent of DHS' recommitment to the State, Local, and Regional Fusion Center Initiative; (2) SLPO efforts ensure coordinated support of DHS and its components to provide needed information and resources to fusion centers; and (3) any functional or organizational challenges exist within DHS that hinder its successful support to fusion centers. *Office of Inspections*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2011 ***(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 DNI, CIO, and OMB, requires an annual evaluation and reporting of the security program over agencies' intelligence systems. FISMA and the Director, Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems, requirements will be used as criteria for the evaluation.

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

OFFICE OF POLICY

New Projects

The Visa Waiver Program

The Visa Waiver Program (VWP) enables citizens from 36 participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. The program was established to eliminate unnecessary barriers to travel, stimulating the tourism industry and permitting the Department of State to focus consular resources in other areas. To be admitted to the VWP, a country must meet various security and other requirements, such as enhanced law enforcement and security-related data sharing with the United States and timely reporting of both blank and issued lost and stolen passports. VWP

members are also required to maintain high counterterrorism, law enforcement, border control, and document security standards.

Objectives: Determine (1) how effectively the Office of Policy Development collaborates with key VWP stakeholders such as the Department of State and the Department of Justice; (2) the efficiency of VWP policies and the effectiveness of the process for assessing current VWP countries; (3) the effectiveness of the multilayered security approach used to admit new countries; and (4) whether the Office of Policy Development's performance metrics deter fraud and abuse. *Office of Inspections*

TRANSPORTATION SECURITY ADMINISTRATION

New Projects

TSA National Explosives Detection Canine Team Program

TSA relies on canines as one of its many methods and layers to detect and deter acts of terrorism in aviation, mass transit, and cargo environments. The TSA National Explosives Detection Canine Team Program uses canine teams to deter terrorism directed toward transportation systems. This program provides timely and mobile response support to facilities, rail stations, airports, passenger terminals, seaports, and surface carriers. TSA dogs are looking for a variety of explosive odors that they have been trained to detect. Once the dog identifies the explosive odor, it responds accordingly. After the 2009 Christmas Day terrorist attack, DHS increased the presence of law enforcement and explosives detection canine teams at airports. In the FY 2011 DHS budget request, TSA requested $71 million to fund additional explosive detection canine teams.

Objective: We will conduct covert testing at airports and rail stations to assess whether canines are effectively identifying explosives. *Office of Audits*

TSA Penetration Testing: Liquid Container Screening Systems

After an unsuccessful August 2006 terrorist plot to blow up U.S.-bound passenger jets with liquid explosives hidden in carry-on luggage, TSA issued new rules that banned liquids, gels, and aerosols on aircraft. After conducting extensive research, TSA determined that liquids, aerosols, and gels, in limited quantities, are safe to bring aboard an aircraft. TSA established a one bag limit per traveler. Consolidating the bottles into one bag and x-raying them separately from the carry-on bag enables security officers to quickly clear the items. Medications, baby formula and food, and breast milk are allowed in reasonable quantities exceeding 3 ounces and are not required to be in the zip-top bag. However, TSA requires passengers to declare these items for inspection at the checkpoint. TSA uses liquid container screening systems to differentiate liquid explosives from common, benign liquids.

Objective: Through covert testing, we will evaluate the effectiveness of TSA's liquid container screening systems at passenger screening checkpoints. *Office of Audits*

TSA's Office of Inspections Efforts

TSA is responsible for the security of all modes of transportation and improving the security of airport perimeters, access controls, and airport workers. Inspections and covert testing are critical elements of the transportation security system. These activities attempt to measure effectiveness and identify vulnerabilities, while incorporating new intelligence in a usable way. TSA's Office of Inspection consists of more than 195 employees who conduct reviews and covert tests nationwide. This work can be costly, as it requires many staff hours and significant travel. The activities also duplicate those performed by OIG and the Government Accountability Office (GAO). TSA has not demonstrated considerable improvements in security as a direct result of these efforts. Prior audit work showed that TSA has not responded to or taken action as a result of its own Office of Inspection reports, allowing security risks to remain.

Objective: Determine whether TSA's Office of Inspection's efforts enhance the effectiveness of transportation security. *Office of Audits*

TSA Transportation Threat Assessment and Credentialing Office's Clearance and Suitability System ***(Congressional)***

Congressman Bennie G. Thompson requested that we assess the quality, fairness, and impartiality of the clearance and suitability system at the TSA Transportation Threat Assessment and Credentialing (TTAC) office, and that we examine the circumstances surrounding the issuance of a security clearance and suitability determination to a general manager of the TTAC office. The office plays an active role in determinations affecting whether individuals engaged in or with access to various aspects of the U.S. transportation system pose a threat to transportation or national security.

Objectives: (1) Assess the quality and impartiality of the clearance and suitability system at the TTAC; and (2) determine the circumstances under which a TTAC office general manager was granted a clearance. *Office of Inspections*

TSA's National Deployment Force – FY 2012 Follow-up ***(Congressional)***

Congressman John L. Mica, Chairman of the House Committee on Transportation and Infrastructure, requested that we conduct a follow-up inspection of the TSA National Deployment Force (NDF) to determine whether it is being used as Congress intended. TSA's NDF deploys Transportation Security Officers to support airport screening operations during emergencies, seasonal demands, or other circumstances requiring more staffing resources than are regularly available. DHS OIG published a report on the NDF in April 2008 entitled *The Transportation Security Administration's National Deployment Force* (OIG-08-49), also requested by Congressman Mica. The report addressed when, where, and why the NDF had been deployed since the inception of the program, along with a breakdown

of deployment expenses, including travel, per diem, hotel, and overtime costs for FY 2004, 2005, and 2006.

Objectives: (1) Determine when, where, and why the NDF has been deployed by TSA since our 2008 report was published, specifically highlighting high-use airports; (2) obtain a complete accounting and breakdown of every instance in which the NDF has been deployed, the reason for the deployment, the duration, and the total cost per deployment for the following airports: Glacier Park International Airport, Yellowstone Airport, Missoula International Airport, Bert Mooney Airport, and Springfield Branson National Airport; (3) develop a complete accounting and breakdown of all expenses related to maintenance and deployment of the NDF since our 2008 report, including but not limited to any and all fringe benefits, hotel, travel, and per diem; (4) break down all overtime pay attributed to the NDF since our 2008 report, including how overtime is allocated while on deployment; (5) provide a status update and analysis of TSA's standard operating procedures for the NDP; (6) provide an explanation of how TSA chooses the NDF, what percentage are supervisors, and how often supervisors are deployed; and (7) provide an update on the recommendations made in our 2008 report. *Office of Inspections*

IT Matters Related to the TSA Component of the FY 2011 DHS Financial Statement Audit ***(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 TSA's critical financial systems.

Objective: Determine the effectiveness of TSA's general and application controls over critical financial systems and data. *Office of IT Audits*

Transportation Security Administration
Planned Project

Workforce Strength and Deployment in TSA's Federal Air Marshal Service

The TSA Federal Air Marshal Service (FAMS) is responsible for deterring hijackings and other hostile acts against commercial aircraft in the United States and on certain overseas flights. Air marshals served aboard U.S. aircraft as early as 1970, but the September 11, 2001, terrorist attacks gave the service new urgency. Air marshals gained widespread public recognition as a bulwark against similar attacks in the future. For additional security, TSA runs the Federal Flight Deck Officer Program, which trains pilots to carry and use handguns on aircraft, and the Law Enforcement Officers Flying Armed Training Program, which certifies law enforcement personnel to carry handguns in flight. For the flying public, affirmation of an effective FAMS matched with other complementary security measures helps maintain confidence in the security of U.S. air travel. However, FAMS suffered public criticism based on charges of high attrition rates, inadequate coverage of flights, and hiring of less experienced personnel. TSA responded that the service remains adequately staffed and that its risk-based approach to deployment delivers reasonable security. Yet media criticism

persists, frequently based on anonymous sources in TSA and the airline industry. Prolonged staffing shortages, hiring and retention difficulties, and insufficient coverage of flights would signal serious vulnerabilities in airline security, especially during unanticipated periods of heightened threats. Plans to overcome such challenges and adjust deployments accordingly are vital to ensuring the service's long-term effectiveness.

Objectives: Determine the adequacy of TSA's FAMS workforce readiness, including numbers of available marshals, staffing models and projected needs, attrition rates, and hiring plans. *Office of Inspections*

Transportation Security Administration
Projects in Progress

TSA Penetration Testing: Access Control at Domestic Airports ***(Congressional)***

The *Aviation and Transportation Security Act* directs TSA to improve the security of airport perimeters, access controls, and airport workers. TSA has the statutory responsibility for requiring employment investigations, including a criminal history record check and a review of available law enforcement databases and other records for individuals who have unescorted access to the secure areas of airports and aircraft. The TTAC office within TSA is responsible for conducting name-based and fingerprint-based checks on individuals with Security Identification Display Area (SIDA) access, Sterile Area workers, and other individuals holding or seeking airport badges or credentials. TSA implements policies associated with airport secure areas and provides support to the airport and airline security officers who adjudicate the results of the criminal history checks.

Objective: Determine whether TSA's security procedures prevent unauthorized individuals from accessing the airports' Sterile Areas and SIDAs. *Office of Audits*

Policies and Procedures for Access Control to the Airport Security Identification Display Area ***(Congressional)***

The *Aviation and Transportation Security Act* directs TSA to improve the security of airport perimeters, access controls, and airport workers. Terrorists, illegal immigrants, and undocumented workers may use false information and work within selected airport SIDAs and Sterile Areas. TSA may have limited controls over the issuance of SIDA badges. TSA may not have comprehensive processes to ensure that undesirable individuals cannot pass the required background checks by providing false biographic identities such as name, Social Security number, and date of birth. Although TSA relies on biographic identity to clear potential employees, these individuals may find ways to circumvent the process.

Objectives: Determine whether TSA's security threat assessment oversight and control process is adequate to prevent individuals with questionable backgrounds from receiving badges or credentials that give them unescorted access to secure airport areas. We will also determine whether airports and aircraft operators are complying with TSA's security requirements to control access to these areas. *Office of Audits*

Management and Oversight of Transportation Security at Honolulu International Airport ***(Congressional)***

Reps. John Mica (R-FL) and Jason Chaffetz (R-UT) called on DHS OIG to investigate lapses at Honolulu International Airport that prompted a move to fire dozens of baggage screeners. In a letter to Acting DHS Inspector General Charles Edwards, the two lawmakers urged a probe into why TSA screeners failed in their responsibilities. The move to terminate the employees—the largest personnel action in the agency's history—demonstrates "the conflict that exists when the TSA acts as both the operator and regulator of the aviation screening programs," the congressmen said.

TSA announced that it was recommending firing 37 employees after what it called an extensive investigation. The workers reportedly allowed baggage to pass through security that had not been properly screened for explosive devices. TSA Administrator John Pistole said his agency "holds its workforce to the highest ethical standards" and that it has "taken appropriate action" to resolve the issue.

Objective: Evaluate the management and oversight of screening operations at Honolulu International Airport. *Office of Audits*

Security Breaches at Newark Liberty International Airport ***(Congressional)***

Senator Lautenberg request an investigation concerning the security breaches that have transpired at the Newark Liberty Terminal. In the wake of the incidents that have occurred because of the breach in security, Senator Lautenberg would like an investigation to be performed to determine the leading factors and TSA's response.

Objective: Evaluate the management and oversight of screening operations at Newark Liberty International Airport. *Office of Audits*

Implementation and Coordination of the Secure Flight Program

The *Intelligence Reform and Terrorism Protection Act of 2004* required DHS to assume from air carriers the responsibility of prescreening international and domestic passengers against government terrorist watchlists before they board an aircraft. In June 2010, TSA implemented the Secure Flight program to fulfill this requirement for DHS. Through Secure Flight, TSA uses the No Fly and Selectee Lists to identify individuals who are prohibited from boarding an aircraft or who are to receive additional physical screening prior to boarding an aircraft. The No Fly and Selectee lists are subsets of the Terrorist Screening Database, which is maintained by the Department of Justice's Terrorist Screening Center and serves as the U.S. government's consolidated watchlist of all known or reasonably suspected terrorists. This review focuses on TSA's implementation and coordination of the Secure Flight program.

Objectives: Determine (1) whether the Secure Flight program is screening all appropriate persons; (2) whether processes and standards for aircraft operators to submit Secure Flight

personal data and receive boarding pass instructions are timely and effective; (3) how the Secure Flight program's screening processes are tested for accuracy, prioritization, and timeliness during high-volume travel periods; and (4) how Secure Flight is protecting varying layers of personally identifiable and sensitive watchlist information. *Office of Inspections*

Efficiency and Effectiveness of TSA's Visible Intermodal Prevention and Response (VIPR) Program

Key aspects of the DHS mission are to secure modes of transportation by deterring and preventing terrorist attacks. To fulfill this mission, DHS relies, in part, on TSA to work with federal, state, and local officials to protect airports, rail systems, highways, and ferries operated by thousands of private and public sector entities. Following the March 2004 commuter train bombings in Madrid, Spain, TSA began deploying VIPR Program teams composed of federal, state, and local entities to enhance security in U.S. airports, trains, and mass transit systems nationwide, to look for suspicious behavior, and to act as a visible deterrent for potential terrorist attacks.

Objectives: Determine (1) the methodology TSA uses to select VIPR deployments; (2) whether geographic location or critical infrastructure affect the conduct of VIPR team operations; and (3) whether VIPR teams are efficient and effective in augmenting local, state, and federal efforts to enhance security in rail and mass transit systems. *Office of Inspections*

Allegations of Misconduct and Mismanagement Within TSA's Office of Global Strategies

TSA's Office of Global Strategies (OGS) was established in October 2007 to increase international aviation security by collaborating with foreign governments and industry partners. OGS employs a multilayered approach to improve global transportation security. This approach includes performing liaison activity with foreign governments and foreign air carriers, evaluating and documenting security vulnerabilities at foreign airports, and assisting foreign governments with the development of aviation security programs that bring them into compliance with international standards. The basis for this review is allegations of egregious behavior and mismanagement.

Objectives: Determine whether evidence exists that confirms the allegations of (1) mission and program mismanagement that has resulted in increased security risks and (2) discrimination, favoritism, abuse, waste, and inefficiencies. *Office of Inspections*

The IT Insider Threat at TSA

As the agency becomes increasingly dependent upon complex information systems, the inherent risk to these systems in the form of computer crimes and security attacks increases. Because of the high-tech nature of these systems and the technological expertise required to develop and maintain them, the emphasis on adequate attention devoted by experts to technological vulnerabilities and solutions has not always followed suit. Trusted insiders,

given their access and status within the organization, pose the biggest threat to the protection of life, property, and information for a component.

Objective: Determine the current risk posed by the trusted IT insider by assessing how effectively components are prepared to detect or prevent insider attacks. *Office of IT Audits*

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

New Projects

USCIS Worksite Enforcement Strategy

The opportunity for employment is one of the most important magnets attracting illegal aliens to the United States. In 1986, Congress enacted the *Immigration Reform and Control Act*, which required employers to verify the eligibility of their employees to engage in lawful employment in the United States. A system of civil and criminal penalties known as employer sanctions was also established and a new form, the I-9, was introduced as a means of documenting that the employer conducted the required verification. ICE is the DHS component responsible for worksite enforcement. ICE's overall worksite enforcement program/strategy has been sharply criticized by stakeholders as being either "too tough" or "not tough enough" when it came to punishing I-9 violators. The program has also been criticized for not utilizing a "full spectrum" approach to enforcement that includes both audits and raids, fines and arrests, and that focuses on both employers and employees. ICE has since announced its intent to refocus its worksite enforcement resources on the criminal prosecution of employers who knowingly hire illegal aliens, not on the prosecution and deportation of large numbers of illegal workers. However, ICE has also stated its intention to continue arresting and deporting illegal aliens encountered during worksite enforcement operations.

Objective: Determine whether ICE's worksite enforcement efforts are effectively detecting, responding, and deterring U.S. employers and workers from violating *Immigration Reform and Control Act* requirements. *Office of Audits*

Adjudication of I-140 Immigrant Worker Petitions

USCIS' I-140, Immigrant Petition for Alien Worker (I-140 petitions) are used by U.S. employers seeking to sponsor foreign nationals with extraordinary knowledge, skills, and abilities to live and work in the United States. I-140 petitions fall into the following visa preference categories: (1) first preference—priority workers; (2) second preference—professionals with advanced degrees or aliens with exceptional abilities; (3) third preference—skilled workers, professionals, and needed unskilled workers; (4) fourth preference—special immigrants; and (5) fifth preference—employment creation (investors). Recipients of employment-based visas are granted lawful permanent residency or "green card status." They

are entitled to a variety of rights and privileges under U.S. law, including the right to (1) reside and work permanently in the United States; (2) apply for dependent visas for their spouse and minor children; (3) travel freely in and out of the United States; (4) apply for U.S. citizenship; (5) receive in-state or resident tuition rates for colleges and universities; (6) receive government grants; and (7) make political contributions in connection with state and federal elections. During FYs 2009–2010, the United States issued I-140-based visas to 292,377 alien workers and their dependent family members. According to USCIS, the process for adjudicating I-140 Immigration Worker petitions is considered to be particularly susceptible to fraud.

Objective: Determine whether USCIS' adjudication of I-140 immigrant worker petitions is being conducted in accordance with agency policies and procedures and in a manner that effectively detects, deters, and prevents immigration benefit fraud. *Office of Audits*

Follow-up Review of the L Intra-company Transferee Visa Program ***(Congressional)***

Senator Charles E. Grassley requested that we conduct a follow-up to our January 2006 *Review of Vulnerabilities and Potential Abuses of the L-1 Visa Program* (OIG 06-22). The L Visa classification originated with the 1970 amendments to the *Immigration and Nationality Act* and is designed to facilitate the temporary transfer of foreign nationals' management, executive, and specialized knowledge skills to the United States to continue employment with an office of the same employer, its parent, branch, subsidiary, or affiliate. Visas are granted to transferees for 3 years and may be extended up to 7 years for managers or executives and 5 years for individuals possessing specialized knowledge.

Objectives: (1) Provide a statistical analysis of the numbers of L-1A (managers/executives) and L-1B (persons with specialized knowledge) visa holders; (2) determine how USCIS' adjudicators define and use the "specialized knowledge" provision in the *Immigration and Nationality Act*, as amended (section 214(c)(2)(B)); (3) explore fraud and abuse issues regarding using L visas to establish new branch offices; (4) report on the use of blanket petitions, wage rates, lengths of stay, outsourcing, and matters relating to L visa worker recourse and enforcement; and (5) provide an update on USCIS' actions to resolve the recommendations we provided in our 2006 report. *Office of Inspections*

IT Matters Related to the USCIS Component of the FY 2011 DHS Financial Statement Audit ***(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 USCIS' critical financial systems.

Objective: Determine the effectiveness of USCIS' general and application controls over critical financial systems and data. *Office of IT Audits*

Controls To Monitor the Approval of Naturalization Applications

The Constitution and laws of the United States give many rights to citizens and noncitizens living in the United States. However, some rights and benefits are given only to U.S. citizens. Among those rights and benefits are voting for elected officials; obtaining federal jobs and other jobs requiring U.S. citizenship; helping family members come to the United States; and traveling with a U.S. passport. Because of the benefits associated with U.S. citizenship and that fact that it is rare for someone to have U.S. citizenship revoked, USCIS needs to effectively monitor its officials adjudicating who is eligible to be granted U.S. citizenship.

Objective: Determine the effectiveness of selected USCIS controls intended to monitor the approval of naturalization applications. *Office of IT Audits*

Accuracy of Information Used in Programs Intended To Certify an Individual's Status for Employment and Other Benefits

USCIS operates two systems—known as Systematic Alien Verification for Entitlements (SAVE) and eVerify—to respond to queries related to an individual's immigration status. eVerify is an Internet-based system that allows businesses to determine the eligibility of their employees to work in the United States. SAVE is designed to aid benefit-granting agencies in determining an applicant's immigration status, and thereby ensure that only entitled applicants receive federal, state, or local public benefits and licenses.

Objective: Determine the extent of immigration status errors in the SAVE and eVerify programs. *Office of IT Audits*

United States Citizenship and Immigration Services
Planned Project

DHS Administration of the T and U Visa Process

Annually, an estimated 800,000 individuals are trafficked across international borders, including 14,500 to 17,500 into the United States. In 2000, passage of the *Victims of Trafficking and Violence Protection Act of 2000* (VTVPA) established T and U nonimmigrant visas to allow trafficking victims or other aliens who have suffered abuse the opportunity to remain in the United States for a specific period of time. In 2009, the USCIS Ombudsman reported that since the enactment of the VTVPA, delays have thwarted the success of the legislation, causing thousands of victims to not receive VTVPA benefits.

Objectives: Determine (1) whether USCIS has adequate staff and resources to adjudicate existing and anticipated T and U visa applications; (2) what standards and performance measures exist for processing T and U visas; (3) whether public guidance available for T and U visa applicants is sufficient; and (4) whether inconsistent cooperation from law enforcement officials is an obstacle to successful adjudication. *Office of Inspections*

United States Citizenship and Immigration Services
Projects in Progress

Adjudication of I-130 Marriage-based Petitions

The I-130 marriage-based petition is designed for U.S. citizens legally married to foreign nationals. Once the petition is approved and the visa issued, the foreign national spouse may enter, live, and work permanently in the United States. The I-130 visa also provides a pathway to U.S. citizenship for the foreign nationals and their families. A USCIS Benefit Fraud and Compliance Assessment review of the I-130 marriage-based petition revealed a fraud rate of 17%. This rate could have significant impact because of (1) the high volume of I-130 visa petitions filed with USCIS annually and (2) the fact that approval of I-130 marriage-based visa petitions provides visa beneficiaries (and their families) access to permanent resident status and the right to apply for a green card and U.S. citizenship.

Objective: Determine whether I-130 marriage-based petitions are being adjudicated uniformly, according to established policies and procedures, and in a manner that fully addresses all fraud and national security risks. *Office of Audits*

Laptop Security

While DHS has increased its reliance on laptop computers for conducting business in support of its mission and for facilitating telework with positive results; the risk of theft, unauthorized data disclosure, and virus infection has also increased.

***Objective*:** Determine whether USCIS has implemented an effective program to protect the security and integrity of its laptop computers. *Office of IT Audits*

UNITED STATES COAST GUARD

New Projects

Efficacy of USCG's NAIS Acquisition Strategy

The Nationwide Automatic Identification System (NAIS) enables the USCG to identify, track, and communicate with marine vessels using the Automatic Identification System (AIS), a maritime digital communication system that continually transmits and receives vessel data over very high frequencies. The goal of NAIS is to enhance Maritime Domain Awareness, with particular focus on improving maritime security, marine and navigational safety, search and rescue, and environmental protection services.

In 2009, the USCG entered an $11.5 million, 2-year base period and six 12-month options contract, worth $68 million with all options exercised. NAIS leverages existing government

infrastructure and capabilities delivered in three discrete, usable increments. Currently the USCG is receiving AIS messages in all 58 high-priority ports and 11 coastal areas, and has completed integrated factory acceptance testing and installed core system equipment at the USCG's Command and Control Engineering Center, Navigation Center, and Operation Systems Center. Developmental test and evaluation will occur in 2011, and the program is scheduled to be completed by 2015. However, as of December 2010, NAIS has experienced challenges with program execution, schedule, resources, and budget planning.

Objective: Determine whether NAIS' acquisition strategy has minimized costs, mitigated performance risks, and maximized the use of commercially available technology. *Office of Audits*

Marine Accident Reporting to the USCG

To aid in identifying, preventing, and minimizing marine accidents and casualties, the USCG requires the reporting of marine accidents, injury, or death. According to 46 C.F.R. 4.05-1, a report submission is required for several specific mishaps, including those involving vessels, mobile offshore drilling units, Outer Continental Shelf facilities, and diving. Though the filing of the CG-2692 form is required for these specific categories, it is unclear how the USCG enforces this requirement.

If the feedback loop in this report filing process is not adequately enforced, the USCG's ability to identify hazardous conditions or conduct statistical analysis is hindered and skewed by a lack of information. Therefore, any new or revised safety initiatives could potentially lag serious hazardous conditions, be unnecessary, or not be implemented due to the lack of information or erroneous information. If underreporting of crew personal injury accidents occurs, the USCG would have a false overall picture of safety levels in the underreported maritime industry sector. This may lead to insufficient inspection, regulatory, and prevention efforts and response planning on the part of the USCG for the underreported sector.

Objective: Determine whether the USCG has adequate policies, procedures, and internal controls to monitor, track, and enforce the filing of Marine Accident Reports as required by the Marine Casualty and Investigations section of 46 C.F.R. 4.05-1. *Office of Audits*

USCG's Annual Mission Performance (FY 2011) ***(Mandatory)***

The *Homeland Security Act of 2002* directs the Inspector General to review annually the performance of all USCG missions, with particular emphasis on non-homeland security missions. Homeland security missions consist of Illegal Drug Interdiction; Undocumented Migrant Interdiction; Foreign Fish Enforcement; Ports, Waterways, and Coastal Security; and Defense Readiness. Non-homeland security missions consist of Search and Rescue, Aids to Navigation, Ice Operations, Living Marine Resources, Marine Safety, and Maritime Environmental Protection.

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

IT Matters Related to the USCG Component of the FY 2011 DHS Financial Statement Audit ***(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 USCG's critical financial systems.

Objective: Determine the effectiveness of USCG's general and application controls over critical financial systems and data. *Office of IT Audits*

USCG Privacy Stewardship

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 maritime economy and the environment, defending maritime borders, and saving those in peril, USCG collects, shares, and uses sensitive personally identifiable information. To promote compliance with federal privacy regulations, the USCG Privacy Officer works with programs to steward and instill a culture of privacy.

Objectives: Determine whether USCG (1) instills a privacy culture that is effective in protecting sensitive personally identifiable information and (2) ensures compliance with federal privacy regulations. *Office of IT Audits*

United States Coast Guard
Projects in Progress

USCG Sentinel Class Acquisition (Fast Response Cutter)

In 2006, USCG removed eight 123-foot patrol boats from service owing to structural failures. To mitigate this loss, USCG accelerated the procurement of its Fast Response Cutter. This acquisition was openly competed outside of the Deepwater contract. An $88 million contract was awarded in September 2008 for the lead vessel, which is scheduled for delivery in the third quarter of FY 2011. In December 2009, USCG awarded a $141 million contract option for the Low Rate Initial Production of the next three vessels. The total contract, if 34 cutters are constructed, is estimated to be worth $1.5 billion.

Objective: Determine whether (1) the current Fast Response Cutters under construction will meet the performance specifications put forward in the contract, (2) USCG's technical authorities exercised oversight of the performance specifications, (3) the performance specifications reflect the actual USCG requirements, and (4) any cost overruns or budget shortfalls have affected the performance specifications. *Office of Audits*

USCG Reutilization and Disposal Program

Annually, USCG identifies millions of dollars of property as excess, surplus, or scrap. Many of these assets may be vulnerable to theft and inappropriate unauthorized resale on the open market, costing USCG millions in potential resale dollars, as well as lost opportunities to reallocate usable assets as needed throughout various government agencies. A recent audit of the USCG Maritime Safety and Security Team program revealed a shortage of computers at five Maritime Safety and Security Team sites visited, which might have been alleviated through the reallocation of computers to these units.

Objectives: Determine whether USCG policies, procedures, and processes ensure the proper (1) identification and classification of excess personal property, and (2) reutilization or disposal method for excess personal property (property valued at less than $25,000). *Office of Audits*

USCG Maritime Patrol Aircraft HC-144

USCG's Ocean Sentry Maritime Patrol Aircraft (HC-144A): In fiscal year 2010, the Ocean Sentry Maritime Patrol Aircraft (HC-144A) comprised about 46% of the USCG's Aviation Division's budget. The USCG awarded the contract for the most recent acquisitions of the HC-144A on July 29, 2010 for a total of about $360 million. The contract was awarded to EADS North America, and subcontracted to EADS CASA, for up to nine HC-144A aircraft, including warranties. We are conducting an audit to determine whether USCG personnel awarded the contract in accordance with applicable laws and regulations and to assess the adequacy of contract oversight.

Objective: To determine the effectiveness of the processes and procedures the USCG used to award the Ocean Sentry Maritime Patrol Aircraft HC-144A contract.
Office of Audits

UNITED STATES CUSTOMS AND BORDER PROTECTION

New Projects

CBP Use of Radiation Portal Monitors at Seaports ***(Mandatory)***

Radiation Portal Monitors are a passive, nonintrusive means to screen cars, trucks, and cargo for the presence of radioactive and nuclear materials. Radiation Portal Monitors are currently employed by CBP to assist in identification of dangerous cargo. CBP uses Radiation Portal Monitors to provide an efficient means of scanning cargo—it takes seconds for one of the portal monitors to scan a standard cargo container, whereas it takes a single CBP officer minutes to scan one using a handheld device. In 2009, the GAO conducted tests on Radiation Portal Monitors and found that the machines were not consistently detecting

radioactive material and were alarming for nonradioactive material. Through FY 2010, CBP acquired and deployed additional Radiation Portal Monitors at both land and sea ports of entry. If machines are performing at the same level as those in the GAO test sample, there is a potential for cargo security breaches.

Objective: Determine whether Radiation Portal Monitors are effectively screening imported cargo for harmful materials. *Office of Audits*

Tracking and Analysis of CBP's In-Bond Cargo Processes ***(Congressional)***

The in-bond cargo system is designed to facilitate trade throughout the United States by allowing cargo to move from its arrival port without appraisal or payment of duties to another U.S. port for official entry into U.S. commerce or for exportation. The cargo is bonded to provide for damages if bond conditions are not met. CBP officials estimate that in-bond shipments represent from 30% to 60% of goods received at their ports. The *SAFE Port Act of 2006* mandated that CBP implement a plan for tracking in-bond cargo using the Automated Commercial Environment system, which is used to track, control, and process all commercial goods imported into the United States.

Objectives: Determine whether CBP conducted an analysis of the extent of use of the in-bond system and the patterns of shipments within the system, and whether CBP has implemented a plan for tracking in-bond cargo in the Automated Commercial Environment information system, as mandated by the *SAFE Port Act of 2006*. *Office of Audits*

Border Patrol Agent Preparedness

Violence has significantly increased against Border Patrol agents. Since 2007, assaults on agents have risen more than 35%, including 13 deaths. Most recently, in December 2010, a Border Patrol agent was killed when his unit encountered a group of illegal border crossers armed with AK-47 assault weapons. When the illegal entrants were ordered to drop their weapons and refused, the Border Patrol agents fired beanbags at the migrants, who returned fire with their assault weapons. The agents then returned fire with one long gun and a pistol. One agent was killed and the other badly wounded. There are concerns that Border Patrol agent training, deployed weapons, and rules of engagement have not kept pace with the increased violence on the border. Along with this, the push to hire new agents may have created a void in experience levels of the agents deployed to facilitate the Border Patrol's mission. It is estimated that 40% of the agents have no more than 2 years of on-the-job experience. It is paramount that Border Patrol agent training, rules of engagement (including use of nonlethal weapons), and agent-issued weapons are commensurate with the current border threat environment.

Objective: Determine whether CBP has updated its threat analysis and operational strategy to address the current boarder threat environment. *Office of Audits*

Tunnel Detection Strategy

Smugglers continue to construct tunnels beneath both our southern and northern borders to transport drugs, illegal aliens, and other contraband. Dozens of tunnels have been found in recent years, including some of remarkable sophistication, but it is likely that tunnels remain undetected. Between 1990 and November 2008, 93 cross-border tunnels were discovered, 35 in California, 57 in Arizona, and 1 in Washington State. In 2010, a tunnel was discovered near Otay Mesa in California that began with a 90-foot-deep vertical shaft on the Mexican side that gradually ascended to an exit point in California more than half a mile north. The tunnel was 7 feet in height, with electrical power and ventilation throughout the tunnel. This is the longest tunnel found under the U.S. border to date. At least six new tunnels were discovered in the first quarter of FY 2009. CBP currently relies on human intelligence to locate subterranean passages. CBP has yet to acquire tunnel detection technology or to develop clear policy regarding the prevention, detection, and remediation of illegal border tunnels. CBP cannot achieve operational control of the borders until it has an operational strategy and the technology to detect and remediate illegal under-border tunnels.

Objective: Determine whether CBP has developed an operational strategy and acquired technology to detect and remediate illegal under-border tunnels. *Office of Audits*

CBP High-Security Bolt Seal Program ***(Congressional)***

Approximately 11 million cargo containers enter the United States annually. CBP's mission includes detecting oceangoing cargo containers that may be used by terrorists, and preventing them from entering this country with weapons of mass destruction, illicit arms, stowaways, illegal narcotics, or other cargo linked to terrorism. CBP is responsible for administering container security and reducing vulnerabilities associated with the supply chain in order to secure the Nation's borders as well as protect and facilitate legitimate trade. High-security bolt seals preserve the integrity of containerized cargo leaving CBP's custody. CBP officers inspect containers that arrive, depart, or transit the United States via sea or land. The officers affix a high-security bolt seal as a primary means of security. CBP distributes the seals to each field office and subsequently to each port of entry. According to the high-security bolt directive, each port should implement a strict inventory control system and accountability procedures over high-security bolt container seals.

Objective: Determine whether CBP is ensuring that high-security bolt seals on cargo containers are properly accounted for and monitored. *Office of Audits*

IT Matters Related to the FY 2011 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 will perform a review of general and application controls in place over CBP's critical financial systems.

Objective: Determine the effectiveness of CBP's general and application controls over critical financial systems and data. *Office of IT Audits*

The IT Insider Threat at CBP

As the agency becomes increasingly dependent upon complex information systems, the inherent risk to these systems in the form of computer crimes and security attacks increases. Because of the high-tech nature of these systems and the technological expertise required to develop and maintain them, the emphasis on adequate attention devoted by experts to technological vulnerabilities and solutions has not always followed suit. Trusted insiders, given their access and status within the organization, pose the biggest threat to the protection of life, property, and information for a component.

Objective: Determine the current risk posed by the trusted IT insider by assessing how CBP addresses the risks posed by insider IT threats. *Office of IT Audits*

Laptop Security

While DHS has increased its reliance on laptop computers for conducting business in support of its mission and for facilitating telework with positive results; the risk of theft, unauthorized data disclosure, and virus infection has also increased.

Objective: Determine whether CBP has implemented an effective program to protect the security and integrity of its laptop computers. *Office of IT Audits*

CBP TECS Modernization

CBP's Traveler Enforcement Compliance System (TECS) is a key border enforcement system that supports the screening of travelers entering the United States as well as the screening requirements of other federal agencies. The objective of this project is to enhance CBP and ICE mission capabilities by developing and deploying a modernized system to replace the current one.

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

United States Customs and Border Protection
Projects in Progress

Free and Secure Trade Program – Continued Driver Eligibility

Free and Secure Trade (FAST) is a program to provide a harmonized clearance process for known low-risk commercial shipments. Under the FAST program, importers, manufacturers, commercial carriers, and truck drivers who meet certain security criteria are provided expedited clearance through designated lanes when they cross into the United States. During

FY 2009, approximately 114,000 FAST drivers and 2,600 carriers were participating in the program. Recent media coverage has emphasized the vulnerability of FAST drivers to the influence of the drug cartels encouraging participation in transporting illicit narcotics. It is critical that CBP implement adequate continued eligibility control processes to ensure that CBP's border security mission is not compromised by FAST drivers who should no longer remain in the program.

Objective: Determine whether CBP's FAST program continued eligibility process ensures that only eligible drivers and carriers remain in the program. *Office of Audits*

Efficacy of CBP's Penalties Process ***(Congressional)***

This is part of a series of audits to address concerns raised by a member of Congress. CBP agents, import specialists, and auditors work individually and collectively to identify high-risk importers and trade violations by conducting inspections and reviewing entry documentation that indicates noncompliance. Trade violations, such as commercial fraud, negligence, unlawful importation, and poor record keeping, result in penalty referrals. CBP considers the penalty process a priority trade issue that it uses to deter trade noncompliance. Despite the importance given to the penalty process, concerns have been expressed about its timeliness, as well as differences in the amount of penalties assessed and collected.

Objective: Determine whether CBP's use of penalties to enforce and ensure compliance with U.S. trade laws is administered in a consistent manner and is an effective deterrent. *Office of Audits*

Efficacy of the Office of Regulatory Audit Operations ***(Congressional)***

We were notified of concerns with CBP's revenue collection programs, including issues regarding the implementation of audit recommendations. CBP's Office of Regulatory Audit uses a two-phased risk-based audit management approach to identify revenue risk in various program areas to determine the extent of its audit procedures.

Objective: Determine the efficacy of CBP's Office of Regulatory Audit's risk-based audit management approach. *Office of Audits*

CBP's Management of Its *Federal Employees' Compensation Act* Program

The *Federal Employees' Compensation Act* (FECA) (5 U.S.C. §§ 8101, et seq.) provides wage loss compensation, medical care, and survivors' benefits to federal and postal workers around the world for employment-related traumatic injuries and occupational diseases. FECA also provides for payment of benefits to dependents if a work-related injury or disease causes an employee's death. FECA is administered by the Department of Labor and is a self-insured program. FECA benefits are financed by the Employees' Compensation Fund, which is replenished annually through chargeback to employing agencies. The Department of Labor furnishes agencies with a chargeback report that is a statement of payments made from the Employees' Compensation Fund on account of injuries to each agency's employees. In

FY 2009, DHS' unaudited FECA liability was $1.82 billion, with CBP being the largest contributor with a $715 million actuarial liability.

Objectives: Determine whether CBP is effectively and aggressively managing its FECA program to minimize lost workdays and FECA-related compensation costs by returning work-capable employees to work as soon as possible and reducing workplace injuries. Additionally, determine whether CBP has an effective process to validate its workers' compensation chargeback reports to ensure that the billing is correct. *Office of Audits*

CBP's Textile Transshipment Enforcement

The numerous requirements placed on textile products entering the United States under various free trade agreements and legislative preference programs on textile transshipment make them problematic to administer. Owing to the high-risk nature of imports of textile and apparel products and a history of noncompliance, CBP designated the industry as a Priority Trade Issue in FY 2009. Although textiles and apparel represent only 8% of U.S. imports, these two sectors alone account for 42% of all duties collected by CBP.

Objective: Determine whether CBP effectively enforces the laws governing the importation of textiles and apparel into the United States. *Office of Audits*

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary government-business initiative to build cooperative relationships that strengthen and improve the international supply chain and U.S. border security. Its goal is to shift responsibility for cargo security onto stakeholders in the supply chain. C-TPAT companies commit to meeting security standards in order to use their leverage to prevent terrorist organizations from exploiting their supply chains, thereby reducing the risk that terrorist weapons will be introduced into, or concealed within, their shipments.

Objective: Determine the efficacy of CBP's process for verifying C-TPAT members' security practices. *Office of Audits*

CBP IT Management

CBP has a responsibility for securing and facilitating trade and travel while enforcing U.S. regulations, including immigration and drug laws. The agency guards nearly 7,000 miles of land border shared with Canada and Mexico and partners with the USCG to protect America's maritime border. Given the magnitude of CBP's enforcement responsibility, the agency uses myriad information technology capabilities to support its mission of keeping terrorists and their weapons out of the United States.

Objective: Determine the effectiveness of CBP's research, acquisition, implementation, and use of technology to support its efficient and effective border protection. *Office of IT Audits*

CBP's Controls To Ensure the Suitability of Border Patrol Agents and CBP Officers

CBP is the largest law enforcement agency in the United States. It has a workforce of more than 43,600 sworn federal agents and officers, including over 20,000 Border Patrol agents and over 20,000 CBP officers. These employees have access to a considerable amount of classified and otherwise sensitive information and must undergo a background investigation before being appointed. They are also required to periodically undergo background reevaluations while employed. Despite these requirements, in March 2010, CBP's Assistant Commissioner for Internal Affairs testified that "while the overwhelming majority of CBP agents and officers demonstrate the highest levels of integrity and perform their duties with honor and distinction every day, isolated acts of corruption do occur."

Objective: Determine the effectiveness of controls CBP has in place to assess and continually monitor the suitability of Border Patrol Agents and CBP officers. *Office of IT Audits*

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

New Project

IT Matters Related to the ICE Component of the FY 2011 DHS Financial Statement Audit ***(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 ICE's critical financial systems.

Objective: Determine the effectiveness of ICE's general and application controls over critical financial systems and data. *Office of IT Audits*

United States Immigration and Customs Enforcement
Planned Project

DHS' Expansion of the Visa Security Program to Additional Overseas Posts ***(Congressional)***

The Visa Security Program was established to increase the security of the visa process at U.S. embassies and consulates worldwide. ICE law enforcement agents assigned to Visa Security Units administer the program at visa-issuing posts by reviewing visa applications to identify security threats, provide security-related advice and training to consular officers, and investigate security-related visa matters. At an April 21, 2010 hearing, the U.S. Senate

Committee on Homeland Security and Governmental Affairs expressed several concerns regarding the slow pace at which the program has been expanded.

Objectives: Determine (1) why DHS has not submitted the required annual reports to Congress to justify the DHS Secretary's determinations not to assign ICE agents to particular overseas posts; (2) what obstacles are hindering the expansion of the Visa Security Program at additional overseas posts; and (3) how ICE plans to expand the program to more overseas posts with a "flat" FY 2011 budget request to support it. *Office of Inspections*

United States Immigration and Customs Enforcement
Projects in Progress

Secure Communities ***(Congressional and Department Request)***

The Secure Communities Program was established on December 26, 2007, as part of the *FY 2008 DHS Appropriations Act*. Secure Communities is an initiative that focuses on the time-sensitive screening and identification of incarcerated criminal aliens during the booking process. The program relies on interoperable technology to share biometric information among law enforcement agencies. ICE began deploying Secure Communities in October 2008, and as of August 31, 2010, ICE had activated the interoperability capability at 574 jurisdictions in the United States.

Objective: Evaluate the effectiveness of the Secure Communities Program in identifying and removing criminals from the United States. *Office of Audits*

Legislative Issues Surrounding the Secure Communities Program ***(Congressional and Department Request)***

The Secure Communities Program was established on December 26, 2007, as part of the *FY 2008 DHS Appropriations Act*. Secure Communities is an initiative that focuses on the time-sensitive screening and identification of incarcerated criminal aliens during the booking process. The program relies on interoperable technology to share biometric information among law enforcement agencies. ICE began deploying Secure Communities in October 2008, and as of August 31, 2010, ICE had activated the interoperability capability at 574 jurisdictions in the United States.

Objective: Determine whether the Secure Communities Program was communicated to local jurisdictions and maintained according to its established mission and goals. *Office of Audits*

MULTIPLE COMPONENTS

New Project

Temporary Protected Status

Temporary Protected Status (TPS) is an immigration status that grants eligible beneficiaries an opportunity to remain in the United States and obtain a work permit. Foreign countries are designated as TPS nations if a natural or other disaster puts its citizens at risk if they remain in or return to their country.

Objectives: Determine (1) USCIS' process for adjudicating TPS applications and its effect on application processing; and (2) whether Deferred Enforced Departure processes and procedures are enforced. *Office of Inspections*

Multiple Components
Planned Project

Information Sharing on Foreign Nationals: Interior Immigration Enforcement and Activities

Several DHS elements with immigration or border security missions have their own intelligence and information gathering programs, databases, and computer systems. Partnerships among these components are necessary to improve the screening of U.S.-bound persons, enhance border security, protect against criminal aliens, and introduce exit controls. Up-to-date biographic and biometric information about an individual is important to all these agencies if they are to make sound and timely decisions, such as determining whether the individual seeking entry is a potential threat. A unified information sharing structure among these DHS immigration components would enhance decisions on claims and applications, impede the entry of ineligible persons, and augment investigations. Owing to the broad range of responsibilities DHS operational components have for verifying, evaluating, and adjudicating claims and cases involving foreign nationals; the number of data sources maintained by DHS and other federal agencies; and the variations in legal options and responsibilities beyond, at, and within U.S. borders, this review will be divided into three phases: (1) Pre-Entry Applications and Screening; (2) Border Determinations; and (3) In-Country Adjudications and Investigations. Each phase will result in a separate report.

Objectives: Determine (1) the timeliness and thoroughness of information sharing that occurs between DHS components; (2) whether the intelligence and information sharing is sufficient to meet DHS immigration goals; (3) how DHS components responsible for evaluating eligibility, security, and public safety risks check and evaluate information available in immigration, criminal, and intelligence databases; (4) the strengths and weaknesses of current information sharing mechanisms, ranging from the numbers of systems that must be checked manually to the quality of data available; (5) plans to

consolidate, automate, and create interfaces between existing DHS data systems; and (6) human and technological vulnerabilities and inefficiencies in the existing system and possible short-term solutions. *Office of Inspections*

Multiple Components
Projects in Progress

DHS' Efforts To Address Weapons Smuggling to Mexico

ICE investigates the smuggling of weapons out of the United States and facilitates the work of the DHS Border Enforcement Security Task (BEST) Forces. CBP intercepts outbound illicit firearms through border inspections and participation in BEST. DHS, federal, state, local, and tribal authorities and the Government of Mexico (which is represented on several BEST teams) collaborate to identify, disrupt, and dismantle transborder criminal networks that smuggle weapons from the United States into Mexico.

Objectives: Determine (1) what DHS initiatives and strategies exist to interdict and suppress the flow of weapons to Mexico; (2) whether there is effective and efficient information sharing and operational coordination among DHS components; (3) whether DHS collaborates successfully with its federal, state, local, tribal, and Government of Mexico partners; and (4) what performance measures DHS uses to evaluate interdiction and investigation activities. *Office of Inspections*

DHS' Intelligence Community Members' Continuity of Operations and Intelligence Readiness Capabilities

The Assistant Inspectors General for Inspections Working Group of the Intelligence Community's (IC) Inspectors General Forum agreed in January 2010 to conduct concurrent evaluations of Continuity of Operations (COOP) and Intelligence Readiness programs within their organizations. These reviews are being conducted to assess COOP in organizations that are funded by the National Intelligence Program. The Office of the Director of National Intelligence will use findings from all IC departments and agencies to produce a report that examines COOP and Intelligence Readiness at the IC level. We will specifically evaluate the COOP and Intelligence Readiness of its IC members, I&A, and the USCG intelligence elements.

Objectives: Determine whether (1) the definitions of COOP that I&A and USCG intelligence elements use align with the National Continuity Policy; (2) I&A and USCG intelligence elements COOP plans adequately address requirements set forth in the National Continuity Policy; (3) COOP training and exercises test capabilities and identify potential areas of improvement; and (4) new planning efforts incorporate lessons learned and corrective action resulting from prior exercises or actual events. *Office of Inspections*

AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

New Projects

Review of Costs Claimed by Recipients of *American Recovery and Reinvestment Act* Funds Granted by FEMA for Fire Station Construction, Maritime Port Security, and Transit Security

FEMA awarded 350 grants for approximately $500 million, as follows:

Grant Program	Purpose of Grant	Amount	Number of Grants
Fire Station Construction	Construct or modify fire stations	$207,117,279	115
Maritime Port Security	Upgrade facilities and systems, train staff, and improve capabilities to detect attacks/weapons	149,957,774	216
Transit Security	Hire antiterrorism and canine teams, conduct training and public awareness, and improve infrastructure	143,656,500	19
Totals		$500,731,553	350

OIG will select grantees for audit on the basis of grant expenditures and locations of the project, and will issue separate reports on each grantee reviewed. This effort completes Phase III of the OIG audit oversight strategy of ARRA funds, which evaluates outcomes of individual component projects.

Objective: Determine whether costs claimed by the grantees were allowable, allocable, and reasonable according to applicable laws and regulations and award documents. *Office of Audits*

Review of *American Recovery and Reinvestment Act* Funds Awarded by TSA to Airport Organizations for Checked Baggage Explosive Detection Systems and Checkpoint Explosive Detection Equipment

Out of $1 billion appropriated to TSA for explosive detection systems under the Recovery Act, TSA awarded about $636 million to airport organizations under the following programs:

Program	Purpose of Funding	Amount	Number of Awards
Checked Baggage	Modify airports for new baggage screening systems and buy and install closed-circuit TV equipment	$574,023,183	29
Checkpoint	Buy and install closed-circuit TV equipment	61,915,096	28
Totals		$635,938,279	57

OIG will select airports for audit on the basis of the airport expenditures and locations of the facilities, and will issue separate reports on each recipient reviewed. This effort completes Phase III of the OIG audit oversight strategy of ARRA funds, which evaluates outcomes of individual component projects.

Objective: Determine whether costs incurred by the recipients were allowable, allocable, and reasonable according to applicable laws and regulations and award documents. *Office of Audits*

American Recovery and Reinvestment Act of 2009
Projects in Progress

Fire Station Construction Grants Funded by the *American Recovery and Reinvestment Act of 2009*

ARRA appropriated $210 million to FEMA for Fire Station Construction Grants and specified that no grant may exceed $15 million. The purpose of the grants is to provide financial assistance directly to fire departments so that they can enhance response capabilities and increase safety for firefighters and surrounding communities. FEMA competitively awarded 110 grants totaling approximately $200 million. The balance of funds is for program administration.

FEMA gave the highest consideration for grant award to fire stations that already owned or had acquired land designated for fire station construction or modifications and that had already obtained permits for their project. FEMA also gave weight to the purpose of the construction project. The highest priorities for award were construction projects that replaced unsafe or uninhabitable structures or expanded fire protection coverage to meet increased service demand in compliance with the National Fire Protection Association standards for career and voluntary fire departments. Of lesser priority were projects that modified or expanded existing structures to provide sleeping quarters or other amenities, to expand existing structures to accommodate support functions, and to replace or expand habitable structures that are not structured for maximum efficiency.

Objectives: Determine (1) whether FEMA is administering ARRA funds for Fire Station Construction Grants according to plans and requirements, and (2) the status of ARRA funds and projects. *Office of Audits*

Alterations of Bridges Funded by the *American Recovery and Reinvestment Act of 2009*

ARRA appropriated $142 million to USCG for "alteration or removal of obstructive bridges, as authorized by Section 6 of the *Truman-Hobbs Act*." Under the *Truman-Hobbs Act*, funds are reimbursed to bridge owners to cover payments of the government's share for work performed in altering the obstructive bridge according to the approved general plans and specifications. All changes to plans and specifications need approval by USCG before

reimbursement of expenditure can be authorized. USCG funded four bridge projects in Alabama, Illinois, Iowa, and Texas.

Objective: Determine whether USCG is administering ARRA funds according to its approved plans and requirements. *Office of Audits*

Improvements to Shore Facilities Funded by the *American Recovery and Reinvestment Act of 2009*

ARRA appropriated $98 million for "acquisition, construction, and improvements to USCG's shore facilities and aids to navigation facilities, priority procurements due to material and labor increases; and costs to repair, renovate, assess or improve vessels." USCG plans to use $88 million of the $98 million to construct, renovate, and repair seven shore facilities in six states (Alaska, Delaware, North Carolina, Oregon, Virginia, and Washington).

Objective: Determine whether USCG is administering ARRA funds according to its approved plans and requirements. *Office of Audits*

Review of Costs Incurred by Recipients of *American Recovery and Reinvestment Act of 2009* Funds Within Selected States ***(Mandatory)***

ARRA appropriated $2.55 billion to the Department for items such as airport baggage and passenger explosive detection systems; construction and renovation of CBP land ports of entry and deployment of security technology along the southwest border; FEMA grants for Emergency Food and Shelter, Public Transportation and Railroad Security Assistance, Port Security, and Construction of Nonfederal Fire Stations; alteration of bridges, improvements to shore facilities, and repairs to vessels; and upgrades of ICE's and CBP's tactical communication systems.

In completing these activities, the Department awarded contracts, grants, and other transactional agreements totaling $1.4 billion to approximately 400 government, nonprofit, and for-profit organizations in 46 states and the District of Columbia. ARRA recipients are required to follow the terms of the award documents, including the applicable federal administrative requirements and cost principles.

Objective: Determine whether costs incurred by certain recipients in selected states were allowable, allocable, and reasonable according to applicable laws and regulations and award documents. *Office of Audits*

Chapter 6 – Other OIG Activities Planned for FY 2012

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY, HOMELAND SECURITY ROUNDTABLE

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the *Inspector General Reform Act of 2008* (P.L. 110-409) to (1) address integrity, economy, and effectiveness issues that transcend individual government agencies; and (2) increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Inspector General community.

CIGIE is composed of all Inspectors General whose offices were established under section 2 or section 8G of the *Inspector General Act of 1978* (5 U.S.C. App.), who are presidentially appointed and confirmed by the Senate, or who are appointed by agency heads (designated federal entities).

CIGIE Homeland Security Roundtable

Since September 11, 2001, the Inspector General community has played a significant role in overseeing and reviewing the performance of agency programs and operations that affect homeland security. To a large extent, this oversight has been accomplished through collaborative efforts among multiple Inspector General offices; their efforts are being coordinated by CIGIE Homeland Security Roundtable.

On June 7, 2005, the Vice Chair of the President's Council on Integrity and Efficiency, now CIGIE, established the Homeland Security Roundtable. The roundtable supports the Inspector General community by sharing information, identifying best practices, and participating on an ad hoc basis with various external organizations and government entities addressing homeland security issues. The Acting Inspector General, DHS, is the roundtable chair.

CIGIE – Investigations Committee Hotline Review

We volunteered to lead the "Hotline" review on behalf of the Investigations Committee. The working group consists of attorneys and hotline operators from the Inspector General community, including representatives of presidentially appointed and designated federal entity Inspectors General. The working group was tasked with (1) building on the results of previous reviews of our hotline operations, such as the report issued by Project on Government Oversight in March 2009 and the survey performed by the Social Security Administration OIG in July 2009; (2) providing a basis for internal CIGIE dialogue regarding our hotline operations; and (3) identifying recommended practices for our hotline operators. The

working group's review focused on identifying practices and techniques for improving a hotline's performance, as defined by the percentage of allegations that are substantiated through investigation. The techniques discussed included training hotline intake staff, using specialized technology, identifying trends in the intake process to better assist in call management, engaging in an ongoing dialogue with our senior management, effectively communicating with complainants, and proposed hotline community initiatives designed to share information across the community. A report will be issued on behalf of CIGIE.

Objectives: Provide guidance to our hotline operators on how to improve hotline performance, defined as increasing the percentage of allegations that are substantiated by our subsequent investigations; and identify certain issues that affect the entire OIG hotline community as well as areas that might merit further review. *Office of Investigations and Office of Counsel*

CIGIE – Management Advisory Report on OIG Cybersecurity (Phase 2)

At the request of the CIGIE Homeland Security Roundtable and with the approval of the CIGIE Executive Council, DHS OIG chairs a Cybersecurity Working Group of attorneys and IT professionals (i.e., IT security professionals, IT auditors, and other IT practitioners) and other cybersecurity experts from OIGs of various sizes, including representatives of the presidentially appointed and designated federal entity Inspector General community. The Working Group was charged with undertaking a two-part review to identify cybersecurity issues and best practices. In FY 2011, DHS OIG issued a Phase I report on behalf of CIGIE.

Objectives: Identify practices for maintaining the integrity of OIG IT systems and protecting them against internal threats and vulnerabilities and examine the role of the Inspector General community in current federal cybersecurity initiatives. *Office of Management*

CIGIE – Suspension and Debarment Working Group (Initiatives Pending)

In May 2010, CIGIE formed a Suspension and Debarment Working Group tasked with promoting awareness of suspension and debarment and its potential effectiveness in combating fraud, waste, abuse, and mismanagement in the Inspector General community and government-wide. Proposed initiatives include an education and outreach "road show" for OIG investigators and auditors and other relevant stakeholders; a practitioner's "toolkit," including identifying best practices for OIG investigators and auditors and creating checklists and "go-bys" for their use; and promoting the use of suspension and debarment as a remedy for the repeated misuse of ARRA funds. We are actively involved in the CIGIE Suspension and Debarment Working Group, as well as in promoting awareness of suspension and debarment within our organization, and its increased use by DHS program officials.

Objectives: Increase awareness of suspension and debarment in the Inspector General community as well as among other stakeholders, such as federal prosecutors and agency program officials; and promote its use as an effective tool to combat procurement and nonprocurement fraud and the waste or mismanagement of federal funds. *All Offices*

CIGIE – Recommended Practices for Office of Inspectors General Use of New Media (Phase 2)

CIGIE launched a new initiative intended to examine the use of social or new media communications (e.g., Twitter, YouTube, LinkedIn) within the Inspector General Community. We were asked to chair this effort in late FY 2010. Looking ahead to FY 2012, we will coordinate with other members of the CIGIE community to convene a working group to research the feasibility of introducing these new media tools into existing communications and outreach programs. The group will also examine the fiscal, ethical, and cybersecurity challenges associated with using these tools in the federal sector, and recommend new media policies to provide guidance on use of these tools in the Inspector General community.

Objective: Identify best practices and guidance for the Inspector General community to implement the use of social/new media safely and effectively. *Office of Management*

AUDIT AND INSPECTION OFFICES

Listed below are nontraditional projects that our audit and inspection offices will undertake in FY 2012. The projects may or may not result in our issuing a report at the conclusion of the projects. Instead, these 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 Major Management Challenges FY 2012 ***(Mandatory)***

The *Homeland Security Act of 2002* brought together 22 agencies to create a new Cabinet-level department focusing on reducing U.S. vulnerability to terrorist attacks and minimizing damages and assisting in recovery from attacks that do occur. DHS has made progress, but it still has much to do to establish a cohesive, efficient, and effective organization.

As required by the *Reports Consolidation Act of 2000* (P.L. 106-531), DHS annually reports what it considers to be the most serious management and performance challenges facing the agency and briefly assesses its progress in addressing those challenges. The report is included in the Department's annual report submitted to the President, the Director of OMB, and Congress no later than 150 days after the end of the agency's fiscal year.

The major management challenges identified, including department-wide and operational challenges, are a major factor in setting our priorities for audits, inspections, and evaluations of DHS programs and operations.

Objective: Summarize the Department's major management challenges for FY 2012 as required by the *Reports Consolidation Act of 2000*. *Office of Audits*

Single Audit Act* Reviews** ***(Mandatory)

The Inspector General community is responsible for determining whether nonprofit organizations as well as state and local governments comply with the *Single Audit Act*. All nonfederal organizations that spend $500,000 or more a year in federal assistance funds (i.e., grants, contracts, loans, and cooperative agreements) are required to obtain an annual audit, according to the Act. According to OMB Circular A-133, recipients expending more than $50 million a year in federal awards shall have a cognizant agency for audit. For recipients expending less than $50 million but more $500,000 a year, the agency providing the most direct funding will have oversight responsibilities. We are the cognizant agency for 8 recipients and have oversight responsibility for 633 recipients. Under OMB Circular A-133, cognizant and oversight agency responsibilities include performing quality control reviews of the single audit work performed by the nonfederal auditors.

Objective: Determine whether the work performed by the nonfederal auditors complies with OMB Circular A-133 requirements and applicable auditing standards and regulations. *Office of Audits*

Intelligence Oversight and Quarterly Reporting ***(Mandatory)***
[Quarterly reports published not later than 60 days after the end of each calendar year quarter]

Executive Order 12333 describes the limited, specific cases in which a member of the IC may collect, retain, or disseminate information on U.S. persons. Executive Order 13462 requires departments with IC members to routinely report on how well they have complied with Executive Order 12333 and whether any violations have occurred. DHS has two IC members—USCG and I&A—and is therefore responsible for intelligence oversight reporting under Executive Order 13462. Our office and DHS' Office of General Counsel collaboratively prepare quarterly intelligence oversight reports, which are submitted to the Intelligence Oversight Board, a standing committee of the President's Intelligence Advisory Board.

Objectives: (1) Validate quarterly assertions by USCG and I&A concerning their compliance with Executive Order 12333; and (2) report other possible violations that come to our attention. *Office of Inspections*

OFFICE OF INVESTIGATIONS

The mission of INV is to strengthen the effectiveness and efficiency of DHS; secure and protect the Nation from dangerous people and dangerous goods; 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, INV 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); and
- 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 the civil rights and civil liberties of citizens and DHS employees, INV will—

- Investigate referrals of ICE detainee deaths that 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 without unusual circumstances, such as personal injury); and
- Investigate credible allegations of criminal abuse of authority, including 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, INV will—

- Investigate significant grant and contract fraud allegations;
- Investigate gross misuse or abuse of classified information, privacy information, or law enforcement information;
- Investigate FEMA fraud involving 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); and
- Exercise oversight of DHS component element internal affairs investigations.

To strengthen the law enforcement mission and unify DHS operations and management, INV 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 our 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; and
- Participate in CIGIE functions and professional law enforcement organizations and associations.

OFFICE OF MANAGEMENT

OM provides critical administrative support functions to our organization, including strategic planning; development and implementation of administrative directives; information and office automation systems; budget formulation and execution; personnel; procurement; correspondence; training, and workforce development; printing reports: and oversight of travel and accounting services provided to our organization on a reimbursable basis by the Bureau of Public Debt. OM also prepares our annual performance plans, and semiannual reports to Congress.

Efficiency Review Initiative

OM leads the effort in participating in the Department's Efficiency Review Initiative, a major program launched during FY 2009 to improve efficiency, streamline operations, and promote greater accountability, transparency, and customer satisfaction in six main categories: Acquisition Management, Asset Management, Real Property Management, Employee Vetting and Credentialing, Hiring/onboarding, and IT. The Efficiency Review Initiative encompasses both simple, commonsense reforms and longer term, systemic changes that will, over time, make DHS a leaner, smarter department better equipped to protect the Nation.

Efficiency Task Forces

OM leads the effort in coordinating our office's participation in several of the Secretary's efficiency task forces, including Civil Rights and Civil Liberties, Executive Secretariat, *Freedom of Information Act* (FOIA)/Privacy, Intergovernmental Programs, International Affairs, Legal Issues/General Counsel, Legislative Affairs, and Policy and Public Affairs. The ultimate goal of all task forces is to optimize the alignment of responsibilities, resources, and critical coordination and collaboration requirements across components in an effort to streamline operations and improve performance and consistency.

The OM Planning and Compliance Division also participates in the Executive Secretariat Task Force meetings. This task force examines whether there are opportunities for increasing coordination or streamlining efforts in regard to duties that component Executive Secretariats are performing in direct support of the Department Secretary's requirements.

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 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.

OM will continue to participate in Information Sharing Coordinating Council biweekly meetings, monitor council activities, and participate in its initiatives, as appropriate.

Audit and Inspection Quality Assurance Program

OM is responsible for our audit and inspection quality control and assurance program. The program includes annual internal quality control reviews to ensure that audits and inspections are conducted according to applicable auditing/inspection standards and our OIG internal audit/inspection policies. During FY 2012, OM will conduct internal quality control reviews using its Planning and Compliance Division staff. We will also determine whether our quality assurance program is suitably designed, operating effectively, and as intended.

Audit and Inspection Policies

OM is responsible for coordinating the development and issuance of audit policy, training audit staff on policy updates, and reviewing inspection policy. During FY 2012, OM will train audit staff on audit manual revisions. Using FY 2012 annual internal quality control review results, and through continued collaboration with our audit/inspection offices, we will determine the need for additional improvements to internal policies and implement necessary revisions, and ensure that policies and practices are consistent with generally accepted government auditing standards.

Human Resources Initiatives

OM will recruit and retain a highly qualified, engaged, and diverse workforce to carry out the mission and enhance the reputation and distinctiveness of our office. As part of our efforts to improve the efficiency of day-to-day operations within our office, we will review and enhance human resources systems, processes, procedures, and policies using the principles of continuous quality improvement and service excellence. OM will focus on carrying out human resources policies and procedures in an open and honest fashion, welcoming input and advice from our customers, while partnering with upper management by providing professional and expert advice and services on those matters that impact upon human resources issues. It is our goal to work with supervisors to create an environment that will motivate and reward exemplary performance and enhance strategies and programs that provide support, networking, and mentoring opportunities for new employees, especially for those from underrepresented groups.

Alternative Workplace Arrangements

The OM is overseeing the implementation of an alternative workplace arrangement (AWA) program within our office. AWA is a work arrangement that combines nontraditional work practices, settings/locations, and/or technologies, to achieve workplace progress. During FY 2012, AWA will be launched as an approach to designing and implementing new work environments for our field office locations with the objective of maintaining leasing costs, minimizing renovation costs (if necessary), and improving organizational flexibility and agility to respond to current and future workforce demands. Since real estate represents the second most significant cost for our office, reducing space per employee and increasing use of space by implementing an AWA program can provide an excellent return on investment.

Training and Workforce Development

During FY 2012, OM will support organizational-wide training and development through the Training and Workforce Development Division. For FY 2012, OM will focus on—

- Enhancing programs that support employees' personal and organizational skills, knowledge, abilities, and competencies to enhance organizational effectiveness, quality, customer service and satisfaction, productivity, and employee retention;
- Collaboration with program offices and subject matter experts to conduct formal needs assessments and training analyses; benchmarking studies and research; and development of training standards, policies and procedures, lesson plans, and locally produced curriculum;
- Partnering with CIGIE, DHS Enterprise Learning Division, and other external stakeholders to standardize and consolidate Learning/Knowledge Management, and other Web-based systems; and
- Refinement and coordination of the OIG training budget and budget execution.

Budget Initiatives

During FY 2012, OM will work on the following budget initiatives:

- Conduct periodic audit of headquarters and field offices budget allotment to ensure compliance with budgetary, procurement, purchase card, travel card, financial, and travel policies, procedures, and regulations;
- Address noncompliance and establish corrective action plans;
- Prepare and execute FY 2012 operating plan;
- Obligate funds and monitor and report expenditures;
- Perform midyear review of budget status;
- Forecast year-end budget position;
- Respond to data calls from Congress, GAO, OMB, and DHS;
- Review and comment on federal government policy documents;
- Submit regulatory reports to Congress, OMB, and DHS;
- Execute interagency agreements and make payments;

- Review and approve PRISM requests;
- Manage travel service, including government travel card transactions and travel voucher processing;
- Collaborate with stakeholders such as DHS, OMB, and congressional officials regarding FY 2013 budget; and
- Formulate FY 2014 budget.

Acquisition

The Division will be transferring the PRISM functions, currently being processed by the Bureau of the Public Debt, to the Department by October 2012 (FY 2013). PRISM is a Department-wide (enterprise) contract management system.

Project Tracking System

OM will continue to manage and enhance the OIG Project Tracking System (PTS). PTS allows OIG executives and staff to electronically monitor and track the status of a project, from the initial planning stages through the draft/final report review process and distribution of the final product and published report. PTS is used to monitor and track congressional requests and other correspondence that requires a response from OIG. The system uses a Web-based commercial-off-the-shelf application, Intranet Quorum, to develop and deliver the electronic workflows that are used to track projects and provide reporting capabilities to end-users of the system. The workflows within PTS are a standard series of prescribed steps (or cycle) that must be completed for most OIG projects. The steps are assigned to a user and/or group, and users record the actions taken in PTS for tracking purposes. Steps are assigned and reassigned, and subworkflows may be created until all required steps are completed or the project is completed, suspended, or terminated.

In addition to the tracking and workflow functions of the system, PTS provides electronic document management support. OIG staff are to use the document management functions built into the system to draft and review documents electronically from within PTS.

Time Tracking System

In August 2011, OM implemented an electronic time tracking system designed to allow employees and designated contractors to identify the number of hours spent on specific activities during the pay period. The system allows for the tracking of hours spent on activities under 1) direct time and effort categories such as projects or cases and 2) indirect time and effort categories such as travel or training.

Performance Management Program

OIG Performance Management Program's mission is to support the OIG organizational goals by promoting and sustaining a high-performance culture.

The purpose of the OIG's Performance Management Program is to establish and maintain an employee performance appraisal program designed to improve individual and organizational performance through effective communication of performance. The program is designed to foster two-way communication, establish accountability, and provide joint ownership of performance goals and outcomes.

OFFICE OF LEGISLATIVE AFFAIRS

The Office of Legislative Affairs plans significant activities, which will include—

- Planning, coordinating, and managing DHS OIG briefings with Members of Congress and staff,
- Preparing Assistant Inspectors General and the Inspector General in submitting and presenting testimony to oversight committees about specific activities of interest to Congress,
- Tracking congressional requests that are either submitted by a member of Congress or mandated through legislation,
- Monitoring and tracking current legislation to anticipate possible changes to policies affecting DHS and the Inspector General community, and
- Distributing correspondence and final audit, inspection, and special reports to Congress and the White House.

OFFICE OF PUBLIC AFFAIRS

OPA is committed to delivering informed, media-savvy public affairs services based on superior industry knowledge. The OPA staff understands the issues that affect our office and the Inspector General community at large. The OPA staff effectively communicates to our customers through public information dissemination. Our aim is to produce results that directly and positively affect the Inspector General's mission, goals, and objectives, and add transparency to OIG work processes and products. OPA is committed to providing a professional working environment that encourages and rewards creativity, insight, teamwork, and enthusiasm.

OPA has major responsibility for:

- Serving as the principal spokesperson for OIG;
- Developing issue management strategies for OIG;

- Providing public affairs counsel in matters related to the issuing of OIG reports, and publicly discussing audit and investigative work;
- Recommending and advocating actions to enhance opportunities for OIG to remain a leader in the information field through multimedia avenues such as the Internet and other electronic media outlets;
- Promoting openness and transparency in the work of OIG; and
- Direct and thoughtful public engagement.

We accomplish our roles and responsibilities through the following venues**:**

External Communications

The Media

OPA is the principal point of contact with the media. OPA is responsible for ensuring that the public is informed about OIG's activities and of the priorities and policies of the Inspector General. OPA provides news organizations with accurate and timely information in compliance with legal, regulatory, and procedural rules and ensures that information provided is current, accurate, and issued in a timely manner.

DHS OIG.Gov

In FY 2012, OPA will lead OIG efforts in developing and coordinating all social media tools and creating fresh Web content. OPA will promote OIG's mission to reduce waste, fraud, and abuse through showcasing OIG reports and other activities. Additionally, we will use our website as a tool for education and promoting transparency and openness among our internal and external customers.

Internal Communications

OIG Newslink

OPA develops the *OIG Newslink,* the digital monthly employee newsletter of the Office of Inspector General. The *Newslink* serves as a primary source of communication within OIG, with a target audience of more than 600 employees. The purpose of the *Newslink* is to communicate OIG current events while recognizing employee accomplishments.

OIG Media Review

OPA produces a weekly OIG Media Review, which provides comprehensive OIG press coverage and current public perceptions. The Media Review informs OIG personnel of current OIG news coverage. It is an important tool in leveraging an effective and engaging agency-public interface.

Event Coverage

When OIG is involved in a special event such as a media interview, congressional briefing, or hearing, OPA accompanies those efforts with additional media coverage and monitoring. OPA staff examines media outlets to pinpoint increased coverage and analyze trends. These efforts assist in increasing public knowledge of OIG efforts, and information dissemination.

OFFICE OF COUNSEL TO THE INSPECTOR GENERAL

OC enhances and supports the Inspector General's independence and provide a full range of legal services for our office. OC is headed by the Counsel to the Inspector General and is composed of attorneys, paralegals, FOIA specialists, legal interns, and administrative personnel. OC attorneys are the only attorneys in 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 Inspector General. In this manner, the Inspector General can ensure that the legal advice received is entirely objective and not influenced by departmental policy preferences.

Report Reviews

OC provides legal advice to the Inspector General and other employees in our office. Among other matters, OC interprets laws, rules, and regulations; analyzes cases; and researches the legislative history that leads to the passage of a particular act. OC attorneys review virtually all our written products, such as reports, congressional testimony, correspondence, and many reports of investigation, for legal accuracy.

Freedom of Information Act/Privacy Act

In keeping with our commitment to transparency, OIG reports, reviews, and testimony are posted on our public website. All of these documents first are examined by OC to ensure compliance with FOIA, the *Privacy Act*, and other legal and policy directives. In addition, OC processes FOIA and *Privacy Act* requests filed with OIG or referred from other DHS components or other agencies.

Ethics

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

Personnel

OC works closely with our office's Human Resources department and with individual supervisors on personnel issues, providing legal review, advice, and guidance on handling wide-ranging personnel issues, from the availability of accommodations for employees with disabilities to performance-based matters or disciplinary actions. OC represents our office in administrative proceedings before the Merit Systems Protection Board and 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 Inspector General is one of the few DHS officials with authority to issue administrative subpoenas. All administrative subpoenas, ordinarily issued through or in support of our Office of Investigations, undergo legal scrutiny prior to issuance.

Tort Claims

OC also handles or coordinates with Department of Justice on actions against 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 our office on a wide range of legal issues, including ethics, FOIA and *Privacy Act* matters, 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 our office, Inspector General authorities throughout the federal government, and matters in which our office 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 ensures a close liaison and ongoing working relationship with attorneys in DHS, the 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

OC attorneys play a leading role in CIGIE, the umbrella organization for all attorneys in OIGs throughout the federal government. OC attorneys have served on instructional panels regarding access to information, the *Freedom of Information Act* and *Privacy Act*, and 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 Council of Counsels to Inspectors General.

Appendix A – FY 2011 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.	Yes
1.2	Achieve at least 85% concurrence with recommendations contained in OIG audit and inspection reports.	96%
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).	40%
1.4	Achieve at least a 50% implementation rate for OIG recommendations that are more than 1 year old.	66%

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.	81%
2.2	At least 75% of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.	79%
2.3	Provide audit coverage of DHS' major grant programs. Provide audit coverage of $500 million in DHS grants.	Yes
2.4	Achieve at least 85% concurrence from DHS management with OIG recommendations on grant audits.	80%

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.	Partially Met
3.2	Ensure that 100% of DHS OIG employees have an annual Individual Development Plan.	100%
3.3	Ensure that 100% of all eligible DHS OIG employees have a performance plan and receive an annual Rating of Record.	100%

Appendix B – FY 2012 Performance Goals and Measures

The performance measures identified below were included in our FY 2011 performance plan. Each year, we reassess our goals and measures to ensure that we continue to use the most meaningful measures as a basis for assessing 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, 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).

1.4 Achieve at least a 50% implementation rate for OIG recommendations that are more than 1 year old. *[This rate will be based on the number of recommendations mutually closed by OIG and DHS.]*

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 DHS' major grant programs, such as FEMA, Public Assistance Grants, State Homeland Security and Urban Area Grant Audits.

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 a performance plan and receive an annual Rating of Record.

Appendix C
OIG Headquarters and Field Office Contacts

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

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

OIG Headquarters Senior Management Team

Charles K. Edwards	**……**	**Acting Inspector General**
Yvonne Manino	**……**	**Acting Chief of Staff**
Dorothy Balaban	**……**	**Special Assistant**
Richard N. Reback	**……**	**Counsel to the Inspector General**
Matthew Jadacki	**……**	**Assistant Inspector General/Emergency Management Oversight**
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**
Louise McGlathery	**……**	**Acting Assistant Inspector General/Management**
Philip D. McDonald	**.....**	**Acting Director, Office of Legislative Affairs**
Marta R. Metelko	**……**	**Director, Office of Public Affairs**

Appendix C (continued)
OIG Headquarters and Field Office Contacts

Locations of Audit 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
(312) 886-0100 alternate number

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

Houston, TX
Houston, TX 77057
(713) 212-4350 / Fax (713) 212-4361

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

Philadelphia, PA
Marlton, NJ 08053
(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 Office Field Offices

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

Biloxi, MS
Biloxi, MS 39531
(228) 822-0563 / Fax (228) 822-0296

Dallas, TX
Frisco, TX 75034
(214) 436-5200 / Fax (214) 436-5201

New Orleans, LA
New Orleans, LA 70114
(504) 762-2050 / Fax (504) 762-2388

Oakland, CA
Oakland, CA 94612
(510) 637-4311 / Fax (510) 637-1487

San Juan, PR
San Juan, PR 00918
(787) 294-2532 / Fax (787) 771-3617

Appendix C (continued)
OIG Headquarters and Field Office Contacts

Locations of Investigative Field Offices

Alpine, TX Alpine, TX 79830 (432) 837-7332 / Fax (432) 837-7449	**Detroit, MI** Detroit, MI 48126 (313) 226-2163 / Fax (313) 226-6405	**New York City, NY** Jersey City, NJ 07310 (201) 356-1800 / Fax (201) 356-4038
Atlanta, GA Atlanta, GA 30341 (404) 832-6730 / Fax (404) 832-6646	**El Centro, CA** Imperial, CA 92251 (760) 335-3900 / Fax (760) 335-3726	**Orlando, FL** Orlando, Fl 32822 (407) 506-1950 / Fax (407) 240-8104
Baton Rouge, LA Baton Rouge, LA 70803 (225) 334-4900 / Fax (225) 578-4982	**El Paso, TX** El Paso, TX 79925 (915) 629-1800 / Fax (915) 594-1330	**Philadelphia, PA** Marlton, NJ 08053 (856) 596-3800 / Fax (856) 810-3410
Bellingham, WA Bellingham, WA 98226 (360) 527-4400 / Fax (360) 671-0576	**Hattiesburg, MS** Hattiesburg, MS 39402-8881 (601) 264-8220 / Fax (601) 264-9088	**San Diego, CA** San Diego, CA 92101 (619) 235-2501 / Fax (619) 687-3144
Biloxi, MS Biloxi, MS 39531 (228) 385-9215 / Fax (228) 385-9220	**Houston, TX** Houston, TX 77027 (713) 212-4300 / Fax (713) 212-4363	**San Francisco, CA** Oakland, CA 94612 (510) 637-4311 / Fax (510) 637-4327
Boston, MA Boston, MA 02222 (617) 565-8705 / Fax (617) 565-8995	**Laredo, TX** Laredo, TX 78045 (956) 794-2917 / Fax (956) 717-0395	**San Juan, PR** San Juan, PR 00918 (787) 294-2500 / Fax (787) 771-3620
Buffalo, NY Buffalo, NY 14202 (716) 551-4231 / Fax: (716) 551-4238	**Los Angeles, CA** El Segundo, CA 90245 (310) 665-7320 / Fax: (310) 665-7309	**Seattle, WA** Kirkland, WA 98033 (425) 250-1360 / Fax (425) 576-0898
Chicago, IL Chicago, IL 60603 (312) 886-2800 / Fax (312) 886-2804	**McAllen, TX** McAllen, TX 78501 (956) 664-8010 / Fax (956) 618-8151	**Sierra Vista, AZ** Sierra Vista, AZ 85635 (520) 229-6420 / Fax (520) 742-7192
Dallas, TX Frisco, TX 75034 (214) 436-5250 / Fax (214) 436-5276	**Miami, FL** Miramar, FL 33027 (954) 538-7555 / Fax (954) 602-1033	**Tucson, AZ** Tucson, AZ 85741 (520) 229-6420 / Fax (520) 742-7192
Del Rio, TX Del Rio, TX 78840 (830) 298-2629 ext. 239 / Fax (830)298-3282	**Mobile, AL** Mobile, AL 36609 (251) 415-3278 / Fax (251) 219-3517	**Washington, DC** Arlington, VA 22209 (703) 235-0848 / Fax (703) 235-0854
Denver, CO Castle Rock, CO 80104 (303) 653-1627 / Fax (not available)	**New Orleans, LA** New Orleans, LA 70114 (504) 762-2202/ Fax (504) 762-2376	**Yuma, AZ** Yuma, AZ 85364 (928) 373-1620 / Fax (928) 783-0477

Appendix D
Acronyms/Abbreviations

AFR	Agency Financial Report
AIS	Automatic Identification System
ARRA	*American Recovery and Reinvestment Act of 2009*
AWA	alternative workplace arrangement
BEST	Border Enforcement Security Task Forces
CBP	Customs and Border Protection
CFO	Chief Financial Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CNCI	Comprehensive National Cybersecurity Initiative
COOP	Continuity of Operations
COTR	contracting officer's technical representative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DRF	Disaster Relief Fund
EMO	Office of Emergency Management Oversight
ESF	Emergency Support Function
FAMS	Federal Air Marshal Service
FAST	Free and Secure Trade
FECA	*Federal Employees Compensation Act*
FEMA	Federal Emergency Management Agency
FISMA	*Federal Information Security Management Act*
FLETC	Federal Law Enforcement Training Center
FOIA	*Freedom of Information Act*
FNS	Federal Network Security
FPS	Federal Protective Service
FY	fiscal year
GAO	Government Accountability Office
HPPG	high-priority performance goal
HM-TAP	Hazard Mitigation–Technical Assistance Program
HSPD	Homeland Security Presidential Directive
I&A	Intelligence and Analysis
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
IHP	Individuals and Households Program
INV	Office of Investigations

Appendix D
Acronyms/Abbreviations (continued)

IPA	independent public accounting
IPv6	Internet Protocol version 6
ISP	Office of Inspections
IT	information technology
ITA	Office of Information Technology Audits
NAIS	Nationwide Automatic Identification System
NCSC	National Cybersecurity Center
NCTC	National Counterterrorism Center
NDF	National Deployment Force
NFIP	National Flood Insurance Program
NLE	National Level Exercise
NPPD	National Policy and Programs Directorate
NRF	National Response Framework
OA	Office of Audits
OC	Office of Counsel
OCFO	Office of Chief Financial Officer
OFM	Office of Financial Management
OGS	Office of Global Strategies
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OM	Office of Management
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OPA	Office of Public Affairs
PA	Public Assistance
PAR	Performance and Accountability Report
P.L.	Public Law
PRISM	A department-wide (enterprise) contract management system
PTS	Project Tracking System
QHSR	Quadrennial Homeland Security Review
RAMP	Risk Assessment and Management Program
SAVE	Systematic Alien Verification for Entitlements
S&T	Directorate for Science and Technology
SBP	Secretary's Budget Priority

Appendix D
Acronyms/Abbreviations (continued)

SIDA	Security Identification Display Area
SLPO	State and Local Program Office
TECS	Traveler Enforcement Compliance System
TopOff	Top Officials
TPS	Temporary Protected Status
TSA	Transportation Security Administration
TTAC	Transportation Threat Assessment and Credentialing
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigration Status Indication Technology
VIPR	Visible Intermodal Prevention and Response
VTVPA	*Victims of Trafficking and Violence Protection Act*
VWP	Visa Waiver Program
WLC	Watchlisting Cell

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov, or visit our OIG websites at www.dhs.gov/oig or www.oig.dhs.gov.

OIG HOTLINE

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

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

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