ANNUAL PERFORMANCE PLAN
FOR FISCAL YEAR 2013

OFFICE OF INSPECTOR GENERAL

DEPARTMENT OF HOMELAND SECURITY

Homeland Security

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. Our annual performance plan (the plan) contains the goals that our agency will use to gauge its progress toward accomplishing its own strategic goals which align with the Department's strategic goals and to identify the performance measures our agency will use to assess its progress.

Photo Credits: DHS Photo Galleries, and other sources

A Message From the Acting Deputy Inspector General

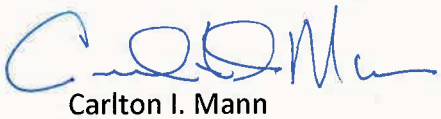
I am pleased to present the *Fiscal Year 2013 Annual Performance Plan* for the Office of Inspector General (OIG), Department of Homeland Security (DHS). The plan outlines the projects that we intend to undertake this fiscal year to evaluate DHS' programs and operations.

This year promises to be challenging as DHS continues to face 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 effort to reduce America's vulnerability to terrorism, and to minimize the impact of unforeseen events that may occur.

In developing the plan, we focused on aligning our planned projects with the mission areas and priorities identified in the Department's *Strategic Plan,* issued February 2012, and the nine major management challenges identified in our report, *Major Management Challenges Facing the Department of Homeland Security*, OIG-12-08. We 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). Finally, we built in enough flexibility into this plan to adjust planned work to adapt to new circumstances and requests that may occur.

In August 2012, we issued DHS OIG's second Strategic Plan, which covers fiscal years 2012 through 2016. This annual plan not only reflects the vision, mission, and goals outlined in our new Strategic Plan, it also reflects the risk based approach to planning independent and objective audits, inspections, and investigations that should help to promote economy, efficiency, and effectiveness in DHS' programs and operations, and prevent and detect fraud, waste, and abuse outlined in our Strategic Plan.

I look forward to keeping you abreast of our progress and that of the Department via our website, www.oig.dhs.gov, and on Twitter, @dhsoig.



Carlton I. Mann
Acting Deputy Inspector General

Table of Contents

Chapter **Page**

1. OIG Mission and Responsibilities 2

2. OIG Organizational Structure and Resources 3

3. Fiscal Year 2013 Planning Approach 6

4. Aligning Our Projects With DHS' Missions, Priorities, and Legislative Mandates 8

5. Project Narratives 12

Directorate for Management 12
Directorate for National Protection and Programs 22
Directorate for Science and Technology 25
Federal Emergency Management Agency 26
Federal Law Enforcement Training Center 35
Office of Health Affairs 35
Office of Intelligence and Analysis 36
Transportation Security Administration 37
United States Citizenship and Immigration Services 44
United States Coast Guard 47
United States Customs and Border Protection 51
United States Immigration and Customs Enforcement 55
United States Secret Service 59
Multiple Components 60
American Recovery and Reinvestment Act of 2009 66

6. Other OIG Activities Planned for FY 2013 67

Appendixes

Appendix A – Tables by DHS Components 81
Appendix B – FY 2012 Annual Performance Report on Goals, Measures, and Accomplishments 94
Appendix C – FY 2013 Annual Performance Plan Goals and Measures 95
Appendix D – OIG Headquarters and Field Office Contacts 98
Appendix E – Acronyms and Abbreviations 99

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.

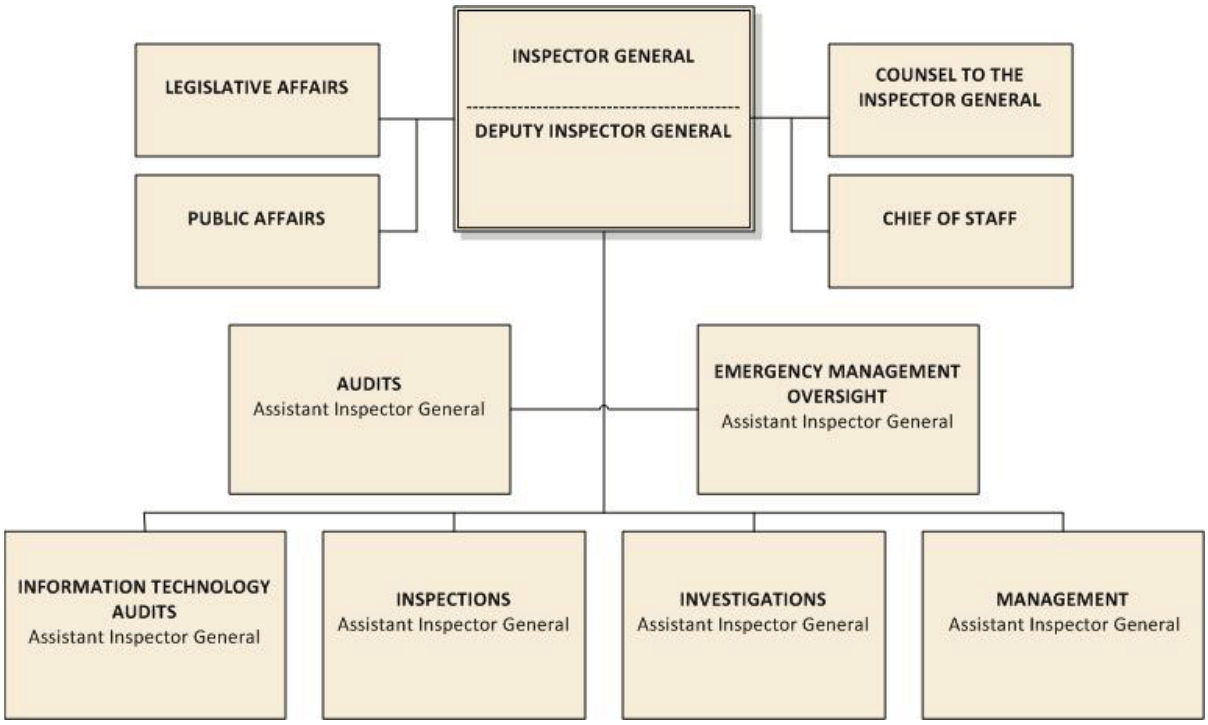
Our office's key legislated responsibilities are as follows:

- 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 683 full-time employees under the President's Budget for Fiscal Year 2013. 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



The OIG consists of the following components:

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

The **Office of Legislative Affairs** (OLA) is the primary liaison to members of Congress and their staffs. Specifically, OLA responds to inquiries from Congress; notifies Congress about OIG initiatives, policies, and programs; coordinates preparation of testimony, briefings, and talking points for Congress; and tracks legislation of interest to the Department and the Inspector General community. OLA tracks congressional requests, which are either submitted by a member of Congress or mandated through legislation. OLA also provides advice to the Inspector General and supports OIG staff as they address questions and requests from Congress.

The **Office of Public Affairs** (OPA) is OIG's principal point of contact for all media outlets and the public. OPA provides news organizations with accurate and timely information 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 communications strategy and helps promote understanding and transparency of OIG work products. In addition, OPA advises the Inspector General and others within OIG on complex programmatic and public affairs issues that affect OIG and its relationship with DHS; other Federal agencies; State and local government; 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 identifying and construing applicable laws and regulations; serves as OIG's designated ethics office; manages OIG's *Freedom of Information Act* (FOIA) and *Privacy Act* responsibilities; represents OIG in administrative litigation and assists the Department of Justice (DOJ) in Federal litigation affecting OIG; furnishes attorney services for the issuance and enforcement of OIG subpoenas; reviews OIG reports for legal sufficiency; reviews proposed legislation and regulations; proposes legislation on behalf of OIG, 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 that the Department, components, grantees, and contractors employ in carrying out essential programs or activities. Audits evaluate whether established goals and objectives are achieved, resources are used economically and efficiently, and intended and realized results are consistent with laws, regulations, and good business practice; and determine 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, the Administrator of the Federal Emergency Management Agency (FEMA), and others fully informed on 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. This allows EMO to stay current on all disaster relief operations and provide 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 Information Technology Audits** (ITA) conducts audits and evaluations of DHS' information technology (IT) management, cyber infrastructure, systems integration, and systems privacy activities protections. The office reviews the cost-effectiveness of acquisitions, implementation, and management of major systems and telecommunications networks across DHS. The office audits systems that affect privacy to assess whether the organizational

governance, culture, and safeguards comply with Federal privacy requirements. 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. The office also assesses DHS' cybersecurity program as mandated by the *Federal Information Security Management Act* (FISMA). In addition, the office conducts audits and provides technical forensics assistance to OIG offices in support of OIG's fraud prevention and detection program.

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 Investigations** (INV) investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and programs. These investigations can result in criminal prosecutions, fines, civil monetary penalties, administrative sanctions, and personnel actions. Additionally, INV provides oversight and monitors the investigative activity of DHS' various internal affairs offices. The office includes investigative staff working on gulf coast hurricane recovery operations.

The **Office of Management** (OM) provides critical administrative support functions, including OIG strategic planning; development and implementation of administrative directives; IT including OIG's information and office automation systems; budget formulation and execution; correspondence control; human resources; acquisitions; facilities; asset management; security; training and workforce development; and oversight of the travel and accounting services provided to OIG on a reimbursable basis by the Bureau of the Public Debt. The office also prepares OIG's annual performance plan and semiannual reports to Congress.

Chapter 3 – Fiscal Year 2013 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) 2013, 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 canceling some projects in this plan. Resource issues, too, may require changes to the plan. The plan includes projects initiated in a prior fiscal year that were not completed and projects that will start during FY 2013. Some projects initiated this year will carry over into FY 2014.

In establishing priorities, we placed particular emphasis on the major management challenges facing the Department, as described in our report, *Major Management Challenges Facing the Department of Homeland Security* (OIG-12-08), http://www.oig.dhs.gov/assets/Mgmt/OIG_12-08_Nov11.pdf. We identified the following as the most serious FY 2011 management challenges facing DHS:

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

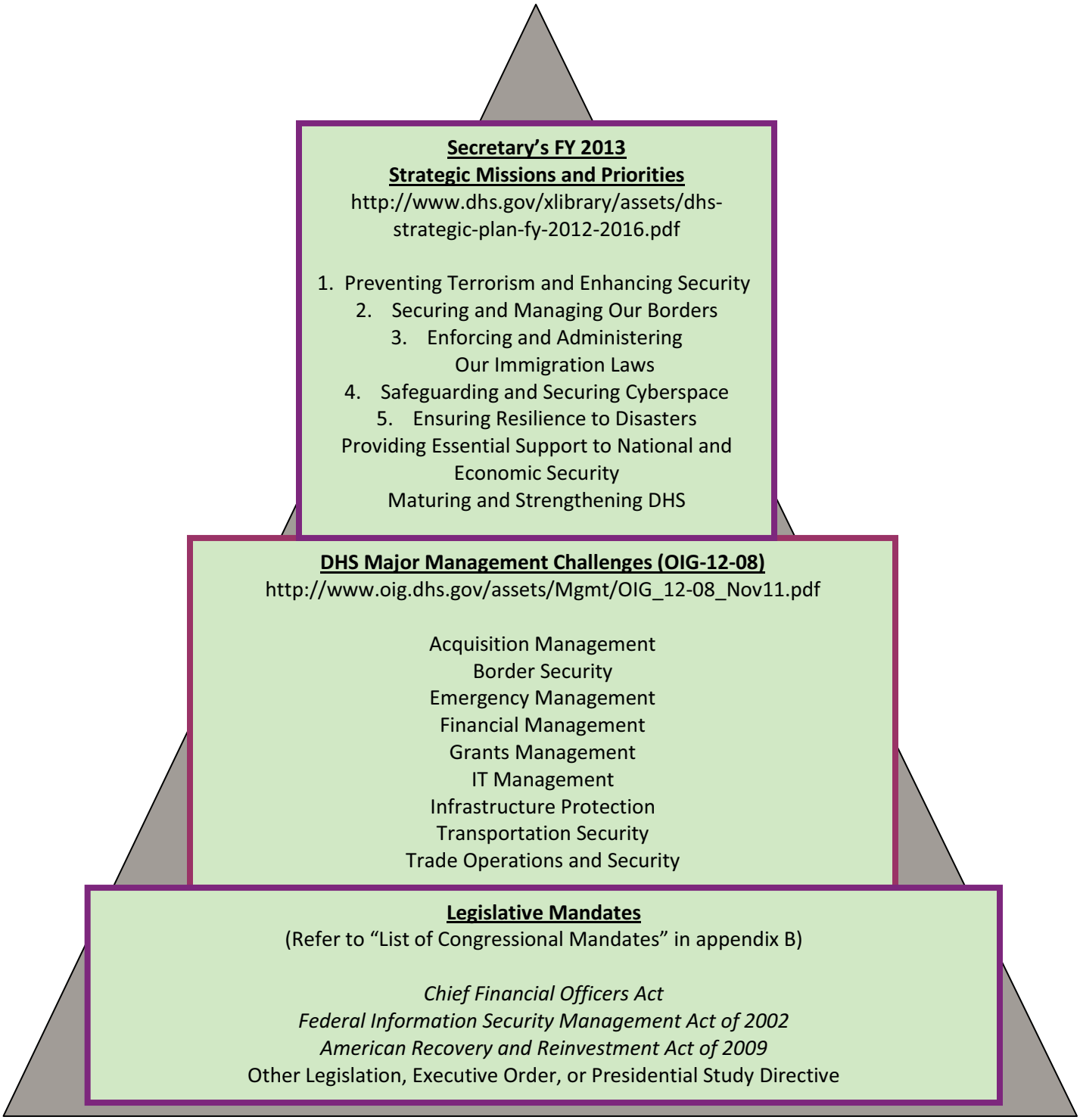
We placed emphasis on legislative mandates such as the *Chief Financial Officers Act* (P.L. 101-576), FISMA (44 U.S.C. §§ 3541, et seq.), and the *American Recovery and Reinvestment Act of 2009* (ARRA). We are also aware of congressional mandates through OLA. We focused on the Department's mission and priorities outlined in its Strategic Plan for Fiscal Years 2012 through 2016:

Mission 1: Preventing Terrorism and Enhancing Security	**Mission 4:** Safeguarding and Securing Cyberspace
Mission 2: Securing and Managing Our Borders	**Mission 5:** Ensuring Resilience to Disasters
Mission 3: Enforcing and Administering Our Immigration Laws	**Priorities:** Providing Essential Support to National and Economic Security; and Maturing and Strengthening DHS

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 these programs 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 is a snapshot of the Department's FY 2013 strategic missions and priorities—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 2013 Planning Priorities



Chapter 4 – Aligning Our Projects With DHS' Missions, Priorities, and Legislative Mandates

In February 2012, the Department issued its revised Strategic Plan for Fiscal Years 2012 through 2016. The Plan outlines the Department's vision, missions, and goals. The Plan also includes the Department's efforts to prioritize frontline operations while maximizing the effectiveness and efficiency of tax dollars. The following represents DHS' missions and priorities. OIG will align its projects and activities with the Department's stated missions and goals.

DHS Mission Areas and Priorities	Description
Mission 1 (M1): 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 threats to and vulnerability of critical infrastructure, key resources, essential leadership, and major events from terrorist attacks and other hazards.
Mission 2 (M2): Securing and Managing Our Borders	The protection of the Nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and other contraband while facilitating lawful travel and trade is vital to homeland security, as well as the Nation's economic prosperity. 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.

DHS Mission Areas and Priorities	Description
Mission 3 (M3): Enforcing and Administering Our Immigration Laws	The success of our Nation's immigration policy plays a critical role in advancing homeland security. 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.
Mission 4 (M4): Safeguarding and Securing Cyberspace	Cyberspace is highly dynamic, and the risks posed by malicious cyber activity often transcend sector and international boundaries. Today's threats to cybersecurity require the engagement of the entire society—from government and law enforcement to the private sector and most important, members of the public—to mitigate malicious activities while bolstering defensive capabilities. DHS is responsible for protecting the Federal executive branch civilian agencies and guiding the protection of the Nation's critical infrastructure. This includes the "dot-gov" world, where the government maintains essential functions that provide services to the American people, as well as privately owned critical infrastructure, which includes the systems and networks that support the financial services industry, the energy industry, and the defense industry.

DHS Mission Areas and Priorities	Description
Mission 5 (M5): Ensuring Resilience to Disasters	DHS coordinates comprehensive Federal efforts to prepare for, protect against, respond to, recover from, and mitigate a terrorist attack, natural disaster or other large-scale emergency, while working with individuals, communities, the private and nonprofit sectors, faith-based organizations, local, State, tribal, territorial, and Federal partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include fostering a Whole Community approach to emergency management nationally; building the Nation's capacity to stabilize and recover from a catastrophic event; bolstering information sharing and building unity of effort and common strategic understanding within the emergency management team; building plans and providing training to our homeland security partners; and promoting preparedness within the private sector.
Priorities (P): Providing Essential Support to National and Economic Security	Homeland security is an integral element of broader U.S. national security and domestic policy. It is not, however, the only element. The National Security Strategy clearly identifies national defense and economic security as other elements—along with homeland security—of overall U.S. national security. DHS leads and supports many activities that provide essential support to national and economic security, including, but not limited to, 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 in many ways to these elements of broader U.S. national and economic security while fulfilling its homeland security missions.

DHS Mission Areas and Priorities	Description
Priorities (P): Maturing and Strengthening DHS	Maturing and strengthening DHS and the entire homeland security enterprise—the collective efforts and shared responsibilities of Federal, State, local, tribal and 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, resilient communities; and fostering innovative approaches and solutions through cutting-edge science and technology, while continuing to foster a culture of efficiency, sustainability, and resilience.

Chapter 5 – Project Narratives

The following projects and the resulting reports should aid the Department in assessing its progress toward achieving its FY 2013 missions and priorities. We present projects under two broad categories: *Planned* or *In-progress*. *Planned projects* are defined as new projects that we should begin during FY 2013. *In-progress* projects are defined as projects that began in a prior fiscal year, but will continue in FY 2013. The projects are organized by Department component and include the objective, the origin of the project, and the related mission and priority area being assessed.

See appendix A for four tables grouping the projects by Department Component. The tables list the following:

1. **Mandatory** projects, which are legislatively required
2. **Congressionally Requested** projects, which are ***not*** legislatively mandated by statute, but requested by a member of Congress.
3. **ARRA** projects which specifically involve the Recovery Act
4. **Discretionary** projects, initiated by OIG

DIRECTORATE FOR MANAGEMENT

Planned Projects

<u>IT Matters Related to the FY 2012 Financial Statement Audit – DHS Consolidated</u>, Mandatory

We contract 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 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*

<u>Annual Evaluation of DHS' Information Security Program for FY 2013</u>, 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 of FISMA. FISMA includes provisions aimed at further strengthening the security of the Federal Government's information and computer systems by implementing an information security program and developing 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*

Telework Security, Discretionary

The *Telework Enhancement Act of 2010* was enacted on December 9, 2010, to improve telework across the Federal Government. As part of its telework program, agencies are required to implement adequate controls to protect their data and information systems. On July 15, 2011, OMB issued a memorandum highlighting the benefits of teleworking, citing increases in productivity and reduced overhead costs. However, OMB also emphasized the need for safeguards and reminded Federal agencies that if not properly implemented, telework might introduce new security vulnerabilities into agency systems and networks.

Objective: Determine whether DHS and its components have implemented effective controls as part of its telework program. *Office of IT Audits*

DHS' Implementation of HSPD-12 Compliant Cards for Logical Access, Discretionary

To improve cybersecurity, the President has identified "strong authentication" that requires the use of Homeland Security Presidential Directive 12 (HSPD-12)-compliant cards when accessing Federal information systems as one of his administration's priorities. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification smartcard credentials, including a standardized background investigation to verify employees' and contractors' identities.

Objective: Determine whether DHS has effectively managed the implementation of HSPD-12-compliant cards for logical access. *Office of IT Audits*

Cloud Computing at DHS, Discretionary

Cloud computing plays a key role in the President's initiative to modernize IT in the Federal Government by identifying enterprise-wide common services and solutions and adopting a new cloud-computing business model. Cloud computing is a way of computing, via the Internet, that broadly shares computer resources. Besides allowing data applications to be housed centrally and accessible anywhere, cloud computing offers tremendous potential for efficiency, cost savings, and innovation. The technology offers many advantages, but the main challenge in deploying cloud computing is to protect and secure sensitive data stored in the cloud.

Objective: Determine whether DHS has effectively managed the implementation of its cloud computing strategy to protect its sensitive data. *Office of IT Audits*

Homeland Security Presidential Directive 20 (HSPD-20) Compliance, Discretionary

HSPD-20 establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single national continuity coordinator responsible for coordinating the development and implementation of Federal continuity policies. Federal Continuity Directive 1 is the implementation guidance for HSPD-20. It provides guidance to the Federal agencies for developing continuity plans and programs. Agencies must designate and review their mission-essential and primary mission-essential functions. Additionally, agencies must identify the people, infrastructure, communications, transportation, and other resources needed to support the continuity program.

Objective: Determine whether DHS has identified the communication and IT systems to support connectivity among key Government leadership personnel, internal agency elements, other agencies, critical customers, and the public during crisis and disaster conditions. More specifically, determine whether DHS has identified the communication and IT systems (through procedures such as business impact assessments) that support its mission-essential and primary mission-essential functions. *Office of IT Audits*

Technical Security Evaluation of Dallas-Fort Worth International Airport (DFW), Discretionary

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 making this determination.

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

Human Resource IT Consolidation/Modernization, Discretionary

The DHS Human Resources Information Technology (HRIT) program aims to consolidate and modernize the Department's HR IT systems. The DHS Office of the Chief Human Capital Officer began working on HRIT in 2005 with the goal of consolidating DHS component HR systems into five enterprise-wide solutions.

Objective: Determine the progress made in consolidating and modernizing the Department's HR IT systems. *Office of IT Audits*

DHS Financial Systems, Discretionary

DHS plans to upgrade its current component financial systems to provide better consolidated financial reporting. These upgrades will improve the quality of the information included in the

financial data used to prepare DHS' annual financial statements. DHS has developed an approach to reengineer its financial systems and to consolidate them across DHS platforms.

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

DHS' Use and Oversight of Other Transaction Agreements, Discretionary

Several DHS components have authority to use Other Transaction Agreements (OTAs) as a procurement method. An OTA is not a contract, grant, or cooperative agreement and is not subject to many of the traditional procurement rules and regulations. The following regulations and statutes are among those that do not apply to OTAs: Federal Acquisition Regulation, *Competition in Contracting Act*, *Small Business Act*, *Prompt Payment Act*, *Contract Dispute Act*, and *Single Audit Act*.

Objectives: Determine whether DHS is (1) appropriately using OTA authority in lieu of traditional procurement contracts or other financial assistance methods, and (2) providing sufficient oversight of the agreements. *Office of Audits*

DHS' Competition in Contracts With One Bid Received, Discretionary

Analysis performed by DHS indicates that during FY 2010, the Department awarded 1,256 new competitively negotiated contracts and orders that exceeded $700,000 in value, totaling $4.8 billion. Out of the 1,256 new contracts and orders, 30 percent resulted from the receipt of only one offer. In February 2011, DHS' Chief Procurement Officer issued a memorandum on procedures for improved competition when only one offer is received on a solicitation that uses competitive negotiation and exceeds $700,000. The memorandum provides required actions to take when (1) the solicitation period is less than 30 days, and (2) price negotiations are conducted (regardless of solicitation period).

Objective: Determine the effectiveness of the Department's efforts to increase competition and ensure a fair and reasonable price when only one offer is received in response to a solicitation that uses competitive negotiation and is expected to result in a contract or order exceeding $700,000. *Office of Audits*

Survey of Acquisition, Operation, and Maintenance of DHS' Aviation Assets, Discretionary

In the Secretary's February 2012 congressional testimony on the Department's budget, she stated that DHS is examining how to leverage joint requirements for aviation assets. DHS' Efficiency Review Initiative mandates increased cross-component collaboration for aviation-related equipment and maintenance, to include cross-component transfer of excess aviation equipment and establishment of cross-component maintenance teaming agreements for aviation assets. Since FY 2005, Congress has appropriated more than $3.39 billion to aviation asset-related accounts.

Objective: Determine whether DHS is effectively managing its aviation assets to achieve efficiencies through cross-component coordination and collaboration. *Office of Audits*

DHS' Oversight of Fleet Management and Fuel Expenses, Discretionary

DHS attempts to promote energy efficiency and reduction of petroleum consumption and greenhouse gas emissions through vehicle fuel efficiency, timely vehicle maintenance, minimized idling, and acquisition of alternative fueled vehicles and hybrid electric vehicles. The mission of DHS' Mobile Assets Division is to formulate, promulgate, and interpret policy; provide subject matter expertise; and conduct oversight of fleet management activities for the Department. In April 2011, DHS issued the *Motor Vehicle Fleet Program Acquisition Guide* to provide a single, comprehensive source of processes to assist Fleet Managers in administering the DHS vehicle acquisition program.

Objective: Determine whether DHS provides effective oversight of fleet management activities to ensure that components purchase vehicles and track fuel purchases to achieve higher fuel economy. *Office of Audits*

FY 2013 *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 2013 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting. Final Report November 2013.
- DHS Consolidated Audit Report – Management Letter for DHS FY 2013 Consolidated Financial Statements Audit. Final Report January 2014.
- U.S. Customs and Border Protection (CBP) Audit Report – Independent Auditors' Report on CBP's FY 2013 Consolidated Financial Statements. Final Report January 2014.
- CBP Audit Report – Management Letter for CBP's FY 2013 Consolidated Financial Statements Audit. Final Report March 2014.
- National Flood Insurance Program (NFIP) Audit Report – Independent Auditors' Report on NFIP's FY 2013 Consolidated Financial Statements. Final Report January 2014.
- NFIP Audit Report – Management Letter for NFIP's FY 2013 Consolidated Financial Statements Audit. Final Report March 2014.
- FEMA Audit Report – Management Letter for FEMA's FY 2013 Consolidated Financial Statement Audit. Final Report February 2014.
- Immigration and Customs Enforcement (ICE) Audit Report – Management Letter for ICE's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.

- United States Citizenship and Immigration Services (USCIS) Audit Report – Management Letter for USCIS' FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- Federal Law Enforcement Training Center (FLETC) Audit Report – Management Letter for FLETC's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- United States Coast Guard (USCG) Audit Report – Management Letter for USCG's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- Transportation Security Administration (TSA) Audit Report – Management Letter for TSA's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- Office of Financial Management (OFM) Audit Report – Management Letter for OFM's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- National Protection and Programs Directorate (NPPD) Audit Report – Management Letter for NPPD's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- United States Secret Service (USSS) Audit Report – Management Letter for USSS' FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- Management Directorate Audit Report – Management Letter for Management Directorate's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.
- Science and Technology (S&T) Audit Report – Management Letter for S&T's FY 2013 Consolidated Financial Statements Audit. Final Report February 2014.

***Objectives**:* Determine the fairness of presentations of DHS general and individual component FY 2013 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*

DHS' FY 2013 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 3 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 percent 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: For FY 2013, determine whether 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 2013, 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 required 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 2013 fiscal year appropriations bill.

Prior Inspector General reports showed that the Department improved acquisition management oversight, 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*

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 2013 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*

***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 than $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: Review the work performed by the nonfederal auditors for compliance with OMB Circular A-133 requirements and applicable auditing standards and regulations. *Office of Audits*

Projects In-progress

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*

Homeland Security Information Network Review

The *Homeland Security Act of 2002* mandates that the Department establish a secure communications and IT infrastructure to share data with other Federal agencies, State or local governments, and private entities. In response, DHS created the Homeland Security Information Network (HSIN). In two previous reports, we identified planning and implementation issues regarding DHS' systems approach and found that HSIN did not effectively support State and local information sharing. In this followup audit, we will examine progress made in addressing these planning and implementation issues as well as assess the current state of information sharing over HSIN.

***Objective*:** Determine progress made since our previous audit, *DHS' Efforts to Improve the Homeland Security Information Network* (OIG-09-07), by assessing the status of information sharing among HSIN stakeholders, to include Intelligence, Law Enforcement, and various State, Local, and Tribal stakeholders. *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. National Cybersecurity Center 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*

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.
- CBP Audit Report – Independent Auditors' Report on CBP's FY 2012 Consolidated Financial Statements. Final Report January 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, we will determine the effectiveness of DHS' internal controls over financial reporting. *Office of Audits*

DHS' Internal Controls Over Travel, Conferences, and Employee Awards Programs, Congressionally Requested

The House Appropriations Committee directed OIG to report on whether DHS has effective procedures in place to ensure compliance with all applicable Federal laws and regulations on travel, conferences, and employee awards programs.

Objective: Determine whether the Department has effective procedures in place to ensure compliance with applicable Federal laws and regulations on travel, conferences, and employee awards programs. *Office of Audits*

Radio Communication Inventory, Discretionary

This project is a continuation of the DHS Interoperable Communications audit and will assess DHS and component management of radio communication assets (i.e. equipment and infrastructure.

Objective: Determine whether DHS and its components have effective oversight of inventory management of tactical communication equipment to improve efficiencies within the Department. *Office of Audits*

DHS Compliance With Federal Acquisition Regulation Revisions for the Proper Use and Management of Cost Reimbursement Contracts, Mandatory

This audit is being conducted pursuant to the *Duncan Hunter National Defense Authorization Act for FY 2009* (Public Law 110-417). The act required that the Federal Acquisition Regulation (FAR) be revised to address the use of cost reimbursement contracts. The interim rule amending the FAR was promulgated on March 16, 2011. The act requires that not later than 1 year after the regulations (revisions) are promulgated, the Inspector General for each executive agency shall review the use of cost reimbursement contracts by such agency for compliance with such regulations and shall include the results of the review in the Inspector General's next semiannual report.

Objective: Determine whether DHS complied with the revisions to the FAR for the use and management of cost reimbursement contracts. *Office of Audits*

DIRECTORATE FOR NATIONAL PROTECTION AND PROGRAMS

Planned Projects

Controls Over the Fraudulent Use of Documents To Obtain Entrance Into the United States, Discretionary

To support DHS' mission of protecting our Nation, U.S. Visitor and Immigrant Status Indicator Technology (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. One way that US-VISIT deters fraud is to identify multiple individuals (as indicated by their biometrics) who use the same documents (e.g., passports, visas) to enter the United States.

Objective: Determine the extent to which multiple individuals use the same documents to enter the United States, and actions US-VISIT take to identify and refer these individuals for additional investigations. *Office of IT Audits*

DHS' Implementation of Its Additional Cybersecurity Responsibilities, Discretionary

To improve the national security posture and emergency response of Federal agencies, the OMB has delegated additional cybersecurity responsibilities to DHS. For example, DHS has been tasked with improving cybersecurity throughout the Federal Government by providing FISMA support management, establishing network and infrastructure security capabilities, and overseeing the Federal Trusted Internet Connection initiative. In addition, on July 6, 2012, the President issued Executive Order 13618—Assignment of National Security and Emergency Preparedness Communications Functions, which assigns DHS the responsibilities of developing, testing, implementing, and sustaining National Secure/Emergency Preparedness (NS/EP) communications throughout the Federal Government. DHS is tasked with developing and submitting a detailed plan within 60 days of the date of this order that describes the Department's organization and management structure for its NS/EP communications functions, including all relevant supporting services and entities.

Objective: To determine whether DHS has effectively implemented its additional cybersecurity responsibilities to improve the security posture of the Federal Government. *Office of IT Audits*

National Cybersecurity Center's Effort To Coordinate Cyber Operations Centers Across the Government, Discretionary

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 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 National Cybersecurity Center has made in coordinating DHS cyber operations across the Government. *Office of IT Audits*

NPPD Privacy Stewardship, Discretionary

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 to lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure through Infrastructure Protection, Cybersecurity and Communications, Federal Protective Service, and US-VISIT's advanced biometric identification and analysis, NPPD collects, shares, and uses sensitive personally identifiable information. To promote compliance with Federal privacy requirements, the NPPD Privacy Office works with NPPD's components to instill and maintain an effective culture of privacy.

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

National Cyber Security Review Status, Discretionary

The National Cyber Security Division (NCSD), within the Office of Cybersecurity and Communications, serves as the single national point of contact for the public and private sector regarding cyber security issues. It is also charged with identifying, analyzing, and reducing cyber threats and vulnerabilities; disseminating threat warning information; coordinating incident response; and providing technical assistance in continuity of operations and recovery planning.

Objective: Determine whether NCSD has taken adequate actions to implement new White House and OMB cybersecurity initiatives to address evolving cybersecurity threats. *Office of IT Audits*

Effectiveness of the Federal Protective Service in Providing Security at Federal Facilities, Discretionary

Federal facilities remain a primary terrorist target. The Federal Protective Service (FPS) secures approximately 9,000 Federal facilities across the country with varying security levels. FPS officers and contracted security guards use x-ray technology, magnetometers, and canine patrols to identify threats. FPS has refocused its training and screening procedures in response to attacks on Federal facilities as recently as 2010, as well as audits conducted by OIG and Government Accountability Office (GAO). Additionally, within DHS, FPS has been transferred from ICE to NPPD.

Objectives: Through the use of penetration testing, determine whether FPS effectively identifies threats at visitor entrances of Federal buildings. We will also determine whether Federal Protective Officers and FPS-contracted security guards are following established policies and procedures. *Office of Audits*

Project In-progress

Review of DHS's Disaster Recovery Program, Discretionary

On June 29, 2012, the East Coast experienced a set of major thunderstorms that included strong winds, hail, heavy downpours, and dangerous thunder and lightning. These storms caused not only major power outages to the Mid-Atlantic region but they also downed large trees and pulled down power lines leaving over 1 million people without power in the Washington, D.C., area. DHS relies on a variety of critical IT systems and technologies to support its wide-ranging missions. DHS' IT systems also allow employees to communicate internally and for the American public to communicate with the Department. Following a service disruption or disaster, DHS must be able to recover its IT systems quickly and effectively in order to continue performing these mission essential functions.

Objective: To determine the progress that DHS has made in developing plans for routine backups of critical data, programs, documentation, and personnel for the recovery of these items after an interruption of processing. *Office of IT Audits*

Effectiveness of the Infrastructure Security Compliance Division's Management Practices To Implement the Chemical Facilities Anti-Terrorism Standards Program, Congressionally Requested

We are initiating a review of the Infrastructure Security Compliance Division's (ISCD) management practices to implement the Chemical Facilities Anti-Terrorism Standards (CFATS) program. This review is being conducted pursuant to a February 2012 request from Representative Daniel Lungren, Chairman of the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection & Security Technologies. In April

2012, we received a separate request from Congressman Henry Waxman, Ranking Member of the House Committee on Energy & Commerce, which we incorporated into our review.

Objectives: Determine whether (1) management controls are in place and operational to ensure that the CFATS program is not mismanaged; (2) NPPD and ISCD leadership misrepresented CFATS program progress; and (3) nonconforming opinions of CFATS program personnel have been suppressed or met with retaliation. *Office of Inspections*

DIRECTORATE FOR SCIENCE AND TECHNOLOGY

Planned Projects

S&T's Research and Development Efforts to Detect Cyber Attacks Against the DHS' Network Systems, Discretionary

The S&T Cyber Security Division conducts a wide range of research, development, testing, evaluation, and transition activities to ensure the continuity of DHS operations. As part of the Cyber Security Division Research and Development Center, the Cyber Infrastructure & Emerging Threats Project (Distributed Environment for Critical Infrastructure Decision-Making Exercises, or DECIDE) has been developing programs to address potential cyber disruptions. Integrating these advanced programs into DHS' network, as well as dispersing them to other Federal agencies, private-sector entities, and even transit systems, will deter cyber-terrorists from obliterating critical infrastructure information and personally identifiable information that could compromise our Nation's security.

Objectives: Determine (1) how S&T assesses which sectors are most vulnerable to cyber attacks, (2) the effectiveness of S&T's new technological programs that are being researched and developed to detect potential threats to network systems, and (3) how S&T is collaborating with NPPD in efforts to implement response and restoration plans if a cyber attack were to occur. *Office of Inspections*

Effects of Recent Portfolio Balancing Reviews and Budgetary Constraints on S&T's Workforce and Ability To Carry Out Its Mission, Discretionary

S&T's mission is to strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise. In 2010 and 2011, the Under Secretary for Science and Technology conducted portfolio balancing reviews to review and balance its research and development portfolio. The reviews were conducted to enhance S&T management's perspective on its entire research and development portfolio and on each project within the portfolio, to see linkages between projects both within

S&T and with other agencies, and to inform decisions, including identifying projects to retain and projects to discontinue. Although S&T has moved ahead with reprioritizing its project portfolio, it has been challenged by budget constraints, employee turnover, and declining morale. For example, S&T's research and development budget was cut by 43 percent in FY 2012, which eliminated more than 100 ongoing projects. In 2011, the Office of Personnel Management determined through a survey of Federal employees that S&T ranked 238 out of 240 subcomponents in employee satisfaction.

Objectives: Determine (1) the effectiveness of recent organizational changes within S&T as a result of the portfolio balancing reviews and budget cuts; (2) how S&T is prioritizing its resources to carry out its mission; and (3) what actions S&T has taken to strengthen its workforce. *Office of Inspections*

Goals and Metrics for S&T's Research Projects, Discretionary

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

Planned Projects

Information Technology Matters Related to the FEMA Component of the FY 2012 DHS Financial Statement Audit, Mandatory

We contract with an IPA firm to conduct DHS' annual financial statement audit. As part of this annual audit, the IPA firm's IT auditors review general and application controls 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*

Capping Report: FY 2012 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits, Discretionary

This report will summarize the results of Public Assistance (PA) program and Hazard Mitigation Grant Program (HMGP) grant and subgrant audits performed during FY 2012. We will review audit findings and recommendations made to officials as they relate to PA and HMGP program funds awarded to State, local, and tribal governments FEMA and eligible nonprofit organizations.

***Objective*:** Summarize the results of PA and HMGP grant and subgrant audit reports issued in FY 2012, identify frequently occurring audit findings, and quantify the financial impact of these findings. *Office of Emergency Management Oversight*

Disaster Assistance Grants – Regional Offices, Discretionary

FEMA awards disaster assistance grants from the Disaster Relief Fund to individuals, States, local governments, and certain nonprofits. For the last 3 years, grant expenditures have averaged more than $10 billion. In FY 2011, we issued 54 grant reports disclosing more than $300 million in questioned costs. We will continue conducting 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*

Management Cost of FEMA's Area Field and Long-Term Recovery Offices, Discretionary

In the aftermath of a disaster, FEMA deploys resources and establishes offices to assist local and State governments with disaster response and recovery activities and coordinate the Federal activities. In most cases, FEMA moves its disaster recovery assistance activities to its regional office after an initial period. However, FEMA sometimes chooses to maintain a long-term recovery or area field office to continue providing disaster recovery assistance to local and State governments.

***Objective*:** Determine (1) to what extent FEMA is working toward closing long-term recovery and area field offices and (2) the cost savings that closures of these offices will provide to the Federal Government. *Office of Emergency Management Oversight*

Duplication of FEMA Benefits From Hurricane Irene and Tropical Storm Lee, Discretionary

FEMA has distributed more than $100 million in individual assistance and PA following Hurricane Irene and Tropical Storm Lee. Because some locations were affected by both of these disasters, it is possible that individuals and local governments received duplicate benefits

for damages sustained. In addition, it is possible that duplicate FEMA benefits were received for damage that is covered by insurance benefits. Duplication of payments is prohibited.

***Objective*:** Determine whether individuals and local governments have received duplicate payments following Hurricane Irene and Tropical Storm Lee. Identify systemic weaknesses that permitted such duplicate payments and changes needed to prevent future occurrences. *Office of Emergency Management Oversight*

FEMA's Decisions To Repair or Replace Damaged Facilities, Discretionary

One of the most important decisions FEMA makes following a declared disaster is whether to fund the repair or replacement of damaged buildings; the wrong decisions, either way, can cost taxpayers millions of dollars.

Objective: Determine whether (1) FEMA's policies and procedures are adequate to decide to repair or replace damaged facilities and (2) FEMA makes cost-effective decisions and complies with existing policies and procedures. *Office of Emergency Management Oversight*

Mission Assignment Eligibility and Closeout Activities, Discretionary

FEMA mission assignments are work orders to other Federal agencies immediately following an emergency or major disaster declared by the President to (1) support FEMA activities, (2) provide technical assistance to States, or (3) provide direct operational support to the States. When there is a need for a mission assignment, FEMA will task another Federal agency and obligate funds to fund the directed activities. In general, mission assignments are supposed to be completed within 60 days after the declaration or emergency, although FEMA can extend this timeframe based on extenuating circumstances or unusual project requirements. Additionally, FEMA is supposed to adjust funding levels throughout the life cycle of the mission-assigned activity, as needed. Federal operations support and technical assistance mission assignments are 100 percent federally funded. Therefore, in order to close these mission assignments, the assigned Federal agency must submit to FEMA its cost of performing the assigned mission. Disaster Federal assistance mission assignments are cost shared unless the disaster declaration authorizes 100 percent for these types of mission assignments. With disaster Federal assistance mission assignments, the assigned Federal agency must submit to FEMA its cost of performing the assigned mission, and FEMA must bill the receiving State for the nonfederal cost share.

Objectives: Determine whether FEMA (1) mission-assigned activities are eligible according to Federal regulations and FEMA guidelines, (2) funded activities were the statutory responsibility of another Federal agency, (3) closed out mission assignments in a timely manner so that unliquidated obligations are returned to the disaster relief fund, (4) recouped the nonfederal cost share of direct Federal assistance mission assignments from the States in a timely manner, and (5) had adequate legal authority to ensure that the above activities are performed within an expected timeframe. *Office of Emergency Management Oversight*

FEMA's Oversight of the Mission Assignment Process, Discretionary

Emergency Support Function 5 executes mission assignments during disaster response. To facilitate these assignments, FEMA, in partnership with other Federal agencies, has developed several hundred pre-scripted mission assignments. These assignments are developed and agreed to before a disaster, so that at the time of the disaster, the needed deployments can be accomplished quickly. Although not every need for disaster response has been anticipated, the assignments do cover most deployments.

FEMA reimburses other agencies for their disaster response. For disasters declared in FY 2011 and the first 6 months of 2012, FEMA obligated $558 million for mission assignments.

Objectives: Determine whether FEMA (1) is effectively using the prescripted mission assignments and (2) is effectively monitoring the goods and services received. *Office of Emergency Management Oversight*

Grantee Policies and Procedures for Evaluating Procurements Associated With Public Assistance Grant Funds, Discretionary

In FY 2009, we questioned almost $30 million in improper contracts. In FY 2010, we reported 11 instances where subgrantees awarded $72.7 million in contracts that did not comply with Federal procurement regulations. In FY 2011, we questioned more than $100 million in contracts, and that number may be surpassed in FY 2012. We previously reported that FEMA did not hold grantees adequately accountable for noncompliance with procurement regulations. Proper contracting and full and open competition ensure reasonable pricing from qualified contractors and discourage favoritism, collusion, fraud, waste, and abuse.

Objective: Determine FEMA policies and procedures for reviewing grantee and subgrantee procurements and the actions being taken to ensure compliance with Federal procurement regulations, as required by the grant agreements. *Office of Emergency Management Oversight*

FEMA Public Assistance Grant Funds (Single Settlement Request) Awarded to Recovery School District (Master Plan), New Orleans, Louisiana, Discretionary

The Recovery School District is tasked with rebuilding the primary and secondary schools in New Orleans, Louisiana. Many schools were damaged beyond repair by Hurricane Katrina. Families displaced by the storm have not returned to the neighborhoods some schools once serviced. To rebuild the educational system for the 21st century, FEMA and the Recovery School District have agreed to the 'Master Plan', with the goal of rebuilding smarter. Schools will be built where they are needed, not necessarily their original location. To fund this rebuilding, the Recovery School District submitted a Single Settlement Request for building 87 schools.

Objective: Determine whether the Single Settlement Request was developed according to Federal regulations and FEMA guidelines and whether the Recovery School District is managing the rebuilding projects in line with this *Office of Emergency Management Oversight*

Hurricane Wilma Insurance Settlements to FEMA Subgrantees by the Florida League of Cities-Florida Municipal Insurance Trust, Discretionary

Section 312 of the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, as amended, prohibits the use of public assistance funds for damages covered by insurance. Further, 44 CFR 206.250 (c) requires that actual and anticipated insurance recoveries be deducted from otherwise eligible costs. We have identified two instances in recent audits of FEMA subgrantees in Florida where the Florida League of Cities-Florida Municipal Insurance Trust has incorrectly applied casualty property insurance coverage to insured properties damaged by Hurricane Wilma in 2005. At least 130 FEMA applicants that have received public assistance funding for properties damaged by Hurricane Wilma have unresolved insurance settlements with Florida Municipal Insurance Trust, with millions of dollars of damages at risk of being improperly denied by the trust.

Objective: Determine whether the Florida Municipal Insurance Trust properly applied insurance coverage to insured properties of FEMA Florida subgrantees that received public assistance funding for property damaged by Hurricane Wilma. This is a follow-on audit to the audit at Vero Beach. *Office of Emergency Management Oversight*

FEMA's Logistics Supply Chain Management System, Discretionary

The Logistics Supply Chain Management System manages FEMA's end-to-end supply chain of critical disaster assets and commodities. FEMA's previous supply chain management system, Total Asset Visibility, cost FEMA $117.3 million over 4 years and was never fully implemented. In 2007 FEMA transitioned the program into the Logistics Supply Chain Management System, or Phase II, which is designed to address earlier shortcomings such as information transfer, systems interaction, data entry, and data accuracy issues while providing data access to Federal, State, tribal, and local logistics partners. Phase II is expected to cost $93.8 million.

Objective: Determine whether FEMA's new Logistics Supply Chain Management System has the ability to effectively support Federal disaster logistics operations in the event of a catastrophic disaster. *Office of Audits*

Assistance to Firefighter Grants, Discretionary

Assistance to Firefighter Grants have provided more than $2 billion to more than 20,000 grantees over the past 5 years. DHS OIG has received more than 100 complaints of waste, fraud, or abuse related to Assistance to Firefighter Grants. A prior audit reviewed 30 Assistance to Firefighter Grants from FY 2003 and determined that 30 percent of grants were not in compliance with grant requirements, and questioned 1.1 percent of total grant costs.

Objective: Determine the extent to which Assistance to Firefighter Grant recipients comply with grant requirements and guidance precluding waste, fraud, and abuse of grant funds. *Office of Audits*

State Homeland Security and Urban Area Grant Audits, Mandatory

P.L. 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007* (August 3, 2007), requires OIG 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 12 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 Management of the Temporary Housing Unit Program, Discretionary

Actual provision of temporary housing units at disaster sites is only part of FEMA's overall temporary housing unit program. FEMA acquires, stores, maintains, deploys, and disposes of units in an ongoing program that has presented major management challenges in past years. At any one time, FEMA has more than $200 million in temporary housing unit inventory stored in long-term storage facilities in three States. This review will examine the overall program management effort and plans for the temporary housing unit program.

Objectives: Evaluate the effectiveness and potential for cost savings in FEMA's acquisition, storage, maintenance, deployment, and disposal practices and processes for the temporary housing unit program and make recommendations for improvements. Examine and evaluate the program's goals, structure, and long-term planning. *Office of Emergency Management Oversight*

Projects In-progress

FEMA Privacy Stewardship, Discretionary

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*

FEMA's Temporary Housing in 2011, Discretionary

Quickly providing temporary housing units is critically important for survivors during recovery from a disaster. These units, most often trailers, have been problematic for FEMA in past years. In some cases, housing units have been unnecessarily expensive, housing sites have proven to be unusable, and many units have proven unacceptable in terms of air quality, water leaks, and other shortcomings. FEMA officials have committed to specific corrective action plans to address many of these issues. In response to disasters during 2011, FEMA has deployed hundreds of units at an estimated cost of $20 million. These recent unit deployment experiences of FEMA staff, local governments, and unit occupants can demonstrate FEMA's improvements in this critical operation.

***Objective*:** Determine whether temporary housing unit deployments in 2011 were managed to provide safe, satisfactory, and cost-effective housing for disaster victims. The review will include the procurement, quality control, transportation, safety, and features of units, as well as the selection and preparation of sites for units. It will also evaluate FEMA's exit strategy for terminating unit provisions and disposing of units. *Office of Emergency Management Oversight*

FEMA's Policy for Land Acquisition Costs of Permanently Relocated Damaged Facilities, Discretionary

Title 44 CFR 206.226(g) authorizes FEMA to approve funding for and require restoration of a destroyed facility at a new location when (1) the facility is and will be subject to repetitive heavy damage; (2) the approval is not barred by other provisions of Title 44 CFR; and (3) the overall project, including all costs, is cost effective. When relocation is required, eligible work includes land acquisition and the construction of ancillary facilities such as roads and utilities, in addition to work normally eligible as part of a facility reconstruction. If the applicant sells the original property, FEMA will reduce the grant for the relocated project by the net proceeds from the disposition of property. A cursory review of relocated properties in Mississippi damaged by Hurricane Katrina shows that FEMA has reimbursed applicants millions of dollars for land purchases for relocation of damaged facilities. FEMA's current policy does not provide incentives for the applicant to sell the original property, thus offsetting grant costs, before the applicant's grant is closed out.

Objective: Determine whether FEMA's land acquisition policies and procedures for permanently relocated damaged projects can be strengthened to ensure that proceeds from the sale of the original property are used to reduce Federal funding, whether the property is sold before or after the grant is closed out. *Office of Emergency Management Oversight*

FEMA's Deployment of Disaster Assistance Employees in Response to Hurricane Irene and Tropical Storm Lee, Discretionary

In the aftermath of a federally declared disaster, FEMA deploys staff and resources to assist in disaster response and recovery. Joint Field Offices directed by a Federal Coordinating Officer manage this process. At each Joint Field Office, the Federal Coordinating Officer is responsible for minimizing costs by closely managing staffing levels and striving to hire temporary employees from the local area rather than utilizing higher-cost FEMA Disaster Assistance Employees. However, in some cases Federal Coordinating Officers receive, unrequested, a surplus of Disaster Assistance Employees, who drive up costs and reduce program efficiency. It is possible that that excessive numbers of Disaster Assistance Employees were sent out to Joint Field Offices in the aftermath of Hurricane Irene and Tropical Storm Lee.

Objective: Determine the cost-effectiveness of FEMA's deployment of Disaster Assistance Employees to Joint Field Offices in response to Hurricane Irene and Tropical Storm Lee. *Office of Emergency Management Oversight*

Personal Property at FEMA Joint Field Offices, Discretionary

In the aftermath of disasters, FEMA establishes Joint Field Offices to manage the recovery process. These Joint Field Offices frequently purchase and hold significant amounts of personal property items, including furniture, vehicles, and computers. Such property purchases involve major budget amounts every year. In emergencies, it is possible that unnecessary amounts or types of personal property have been purchased or that appropriate property management procedures have not been followed.

Objective*:* Determine whether personal property for Joint Field Offices is purchased in the approximate quantities needed; appropriate sources are used; and property is accounted for, tracked, and disposed of in accordance with applicable regulations. *Office of Emergency Management Oversight*

State Homeland Security and Urban Area Grant Audits (North Carolina, Kentucky, Rhode Island, Massachusetts, American Samoa, Northern Mariana Islands, Guam, Indiana, Virginia, Mississippi, Connecticut, Nebraska), Mandatory

P.L. 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007* (August 3, 2007), requires OIG 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 12 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, Discretionary

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 oversight of grantees with increased risk. *Office of Audits*

Planned and Project In-progress*

FEMA's Efforts To Recoup Improper Payments in Accordance With the *Disaster Assistance Recoupment Fairness Act of 2011*, Congressionally Requested

The *Disaster Assistance Recoupment Fairness Act* (DARFA) *of 2011* provides a limited-time, discretionary authority for the Administrator of FEMA to waive debts arising from improper payments provided for disasters declared between August 28, 2005, and December 31, 2010. DARFA directs the DHS Inspector General to report periodically on the cost-effectiveness of FEMA's efforts to recoup improper payments.

Objective: Provide quarterly reports to Congress on the cost-effectiveness of FEMA's efforts to recoup improper payments in accordance with DARFA. *Office of Emergency Management Oversight*

**Note: Three reports will be issued. One report is currently in-progress. Two additional reports are planned for FY 2013*.

FEDERAL LAW ENFORCEMENT TRAINING CENTER

Planned Projects

Information Technology Matters Related to the FLETC Component of the FY 2012 DHS Financial Statement Audit, Mandatory

We contract with an IPA firm to conduct DHS' annual financial statement audit. As a part of this annual audit, the IPA firm's IT auditors review general and application controls over FLETC's critical financial systems.

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

OFFICE OF HEALTH AFFAIRS

Planned Project

National Bio-surveillance Integration System, Discretionary

In early January 2012, the National Bio-surveillance Integration Center released a request for information on ways to enhance the current IT system and to reduce barriers for integrating bio-surveillance information. Due to this request and acknowledged barriers, it is critical to assess whether the National Bio-surveillance Integration System (NBIS) meets user needs and to examine system requirements gathering, planning, and compliance with standard IT management policies.

Objective: Determine how effectively the NBIS program is meeting the Department's mission of detecting and sharing biological and chemical threat information. *Office of IT Audits*

OFFICE OF INTELLIGENCE AND ANALYSIS

Planned Projects

Annual Evaluation of DHS' Information Security Program (Intelligence Systems-IC IG) for FY 2013, 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 Chief Information Officer (CIO), and OMB, requires an annual evaluation and reporting of the security program over agencies' intelligence systems. 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: 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*

Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2013, 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. 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: 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*

Insider Threat at the DHS Office of Intelligence and Analysis, Discretionary

Despite the classified and high-tech nature of DHS systems and the technological expertise required to develop and maintain them, the emphasis on adequate attention by experts to safeguard them against technological vulnerabilities has not always followed suit. The trusted insider, given access and status within the organization, poses the biggest threat to the protection of life, property, and information for the component.

The Office of Intelligence and Analysis (I&A) has been designated as the entity within DHS responsible for developing an agency-wide insider threat program, standardizing agency-wide counterterrorism insider threat training, and enabling IT audit and monitoring capabilities for classified systems.

Objective: Determine the adequacy of the steps I&A has taken to address the insider threat risk to classified systems. *Office of IT Audits*

Project In-progress

DHS' Watchlisting Cell Efforts To Coordinate Departmental Nominations, Discretionary

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 I&A 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*

TRANSPORTATION SECURITY ADMINISTRATION

Planned Projects

IT Matters Related to the TSA Component of the FY 2012 DHS Financial Statement Audit, Mandatory

We contract with an IPA firm to conduct DHS' annual financial statement audit. As a part of this annual audit, the IPA firm's IT auditors review general and application controls 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*

Covert Testing of TSA's Law Enforcement Officer Screening Procedures, Mandatory

Prior audit work, congressional testimonies and news reports have suggested vulnerabilities in the aviation security system, including unauthorized access to secure areas of airports. The *Aviation and Transportation Security Act* requires TSA to prescribe requirements for screening or inspecting all passengers before they enter sterile areas of an airport. Armed law enforcement officers (LEOs) are exempt from regular passenger screening procedures, and TSA has established a specialized screening process for LEOs which entails a series of document verification procedures.

Objectives: Determine whether TSA has established policies and procedures, and if so, whether Transportation Security Officers are following established policies and procedures to prevent armed individuals posing as law enforcement officers from unauthorized access to sterile areas and passenger aircraft. *Office of Audits*

Access to Secured Airport Perimeter Areas, Discretionary

Persons with unescorted access to secured areas of the airport, including the external perimeter areas, are required to undergo a TSA security threat assessment. While airport operators generally have direct operational responsibility for airport perimeter security and implementing access controls for secure areas, TSA has responsibility for establishing and implementing measures to improve security in these areas. Accessing airports from the perimeter and surrounding areas may circumvent passenger screening and allow individuals to carry prohibited items aboard aircraft. Flights at Philadelphia International Airport were briefly halted in March 2012 after a man drove a vehicle onto the airfield through a construction fence on the airport's perimeter. Prior audit work identified vulnerabilities when truck drivers easily gained access to secured areas after minimal background checks. Without inspections or stringent security requirements, vehicles could be used to deliver tons of explosives or chemicals directly onto the tarmac.

Objective: Determine the effectiveness TSA's implementation and enforcement of policies and procedures to prevent unauthorized individuals and vehicles from gaining access to secured airport perimeter areas. *Office of Audits*

TSA's Airport Screening Equipment Maintenance Program, Discretionary

One of TSA's key responsibilities is to ensure the effective and efficient screening of all passengers, baggage, and cargo on passenger aircraft. In FY 2011, TSA screened approximately 640 million people and their carry-on items, as well as more than 425 million checked bags. To fulfill its screening responsibilities, TSA must ensure that screening equipment is operating effectively and efficiently. This can only be accomplished through regular maintenance of equipment. Prior audit reports identified issues with equipment maintenance.

Objective: Determine whether routine and periodic maintenance is being performed on airport screening equipment in accordance with contractual requirements and manufacturers' specifications. *Office of Audits*

Effectiveness of Automated Target Recognition in Passenger Screening, Discretionary

TSA currently has 486 advanced imaging technology (AIT) units deployed at 78 airports across the Nation. Automated target recognition software is being added to the AIT units to enhance screening by removing the human element of image analysis from the screening process. This technology, which automatically indicates whether additional screening is needed, detects potential threats that may be hidden on a passenger. Prior covert testing by DHS OIG identified weaknesses in AIT and automated target recognition algorithms to detect anomalies. TSA is allocating more than $6 million to upgrade AIT units with the automated target recognition software and plans to continue the investment with additional units.

Objective: Determine the effectiveness of automated target recognition software used with TSA's AIT units. *Office of Audits*

TSA's Preclearance Aviation Security Operations Program, Discretionary

A recent DHS OIG review concluded that TSA's Preclearance Aviation Security Operations program had not been effectively managed and that a number of preclearance airports had never been assessed.

DHS operates customs preclearance services at 14 international airports. CBP has primary responsibility for preclearance operations. At designated preclearance airports, CBP inspectors use customs procedures comparable to those conducted at U.S. ports of entry to clear passengers and their belongings for entry into the United States. At these airports, TSA is responsible for assessing passenger checkpoint screening to determine whether the foreign airport's screening procedures are comparable to aviation security standards for U.S. airports. However, many of these airports have not had a TSA assessment in years, while some preclearance airports have never been assessed. As a result, security vulnerabilities may exist because passengers arriving from international preclearance airports operating with security procedures that may be less stringent than U.S. domestic standards are deplaning and then connecting to domestic flights without undergoing additional TSA security screening.

Objectives: Determine (1) the extent to which TSA's revised preclearance policies and procedures have been implemented, (2) the rate at which TSA is conducting assessments at the various international preclearance airports, (3) the results of the assessments conducted to date, and (4) the actions being taken with regard to preclearance airports that do not pass the TSA assessments. *Office of Inspections*

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

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*

Projects In-progress

TSA's Office of Inspections Efforts, Discretionary

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 DHS OIG and 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 the efforts of TSA's Office of Inspection enhance transportation security. *Office of Audits*

Management and Oversight of Transportation Security at Honolulu International Airport, Congressionally Requested

Representatives John Mica and Jason Chaffetz 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 K. Edwards, the two congressmen 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 that had not been properly screened for explosive devices to pass through security. 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*

TSA Procurement of Security Badge Vetting Services, Congressionally Requested

Honorable Bennie G. Thompson requested that the DHS OIG review TSA's arrangement for the Aviation Channeling Service Provider project. In 2011, TSA selected three vendors to vet security badges for access to secured airport areas. The ACSP project was expanded by TSA to address the Congressional concerns that airports and airlines be given a choice of contractors when acquiring services for airport employees that will work in secured aviation environments. The ACSP project is administered by TSA's Office of Security Policy and Industry Engagement (OSPIE) and I&A. I&A, under the Office of Technology Solutions, has the Credentialing Systems Division, Vetting Operations Technology Division. OSPIE, under the Program Management Office has the Transportation Workers Vetting Division as well the Industry Programs Division. Despite TSA's utilization of various vendors to vet security badges, ultimately it is the TSA's responsibility to ensure that only airport workers who do not pose a threat to national security obtain access to secured airport areas.

Objective: Review the selection process for the three vendors and the deployment and implementation of the program, including the implementation plans, what costs will be passed on to the users, and the measures TSA has established to evaluate the vendors' performance. *Office of Audits*

Transportation Security Administration's Screening Partnership Program, Congressionally Requested

This audit is being conducted pursuant to a request from Senator Roy Blunt and Senator Bob Corker we requested a review of the Screening Partnership Program (SPP) and how it is being administered. According to the *Aviation Transportation Security Act* (ATSA), an

operator of an airport may submit to the Under Secretary an application to have the screening of passengers and property at the airport to be carried out by the screening personnel of a qualified private screening company under a contract entered into with the Under Secretary. The ATSA pilot was conducted from 2002 to 2004 with five airports. At the conclusion of the pilot, TSA created the SPP which provides airports the opportunity to not use an all-Federal screening program and instead have screening services provided by private companies under Federal supervision. The five pilot airports transitioned to SPP. After several years and some controversy, Congress passed the *Federal Aviation Administration (FAA) Modernization and Reform Act of 2012*. This act requires TSA to approve an airport's application to participate in SPP if the approval will not compromise security, detrimentally affect cost efficiency, or detrimentally affect screening effectiveness of passengers or property. As of September 2012, 22 airports, including the five pilot airports and five recent applicants, have been approved for participation in the program.

Objectives: Determine whether TSA is properly administering the SPP by (1) complying with Federal procurement practices and (2) promoting cost-effectiveness when making opt-out decisions. *Office of Audits*

TSA Deployment and Use of Advanced Imaging Technology, Congressionally Requested

TSA is responsible for conducting checkpoint and checked baggage screening operations at all federalized airports. AIT enables TSA to screen passengers for prohibited items, including weapons, explosives and other metallic and nonmetallic threat items concealed under layers of clothing without physical contact. TSA introduced AIT units at airport security checkpoints in 2007 and has approximately 700 AIT units at 180 airports. Representative John Mica, Chairman of the House Transportation and Infrastructure Committee, requested the DHSOIG conduct an audit on TSA processes related to deployment and utilization AIT. Chairman Mica was concerned with reports of TSA buying AIT units that it is not using; TSA deploying AIT units that it is not operating; and TSA not appropriately planning for the deployment and use related to future purchases of AIT units.

Objective: To determine whether TSA effectively planned for deployment and use of AIT. *Office of Audits*

TSA's Screening of Passengers by Observation Techniques (SPOT) Program, Congressionally Requested

TSA's SPOT program uses observation and behavioral-based profiling techniques to identify persons who may pose a potential security risk at TSA-regulated airports. According to TSA, the SPOT program is a derivative of other behavioral analysis programs that have been successfully employed by law enforcement and security personnel both in the United States and around the world, particularly those of Israel's airline EL AL. The program, which began operational testing in 2003, employs an estimated 3,000 certified Behavioral Detection Officers at 161 airports nationwide at an annual cost of $212 million.

TSA has been criticized for the way it developed, deployed, and executed the SPOT program. Specifically, TSA has been criticized for deploying SPOT nationwide without first validating the scientific basis for identifying suspicious passengers in an airport environment and for utilizing profiling techniques that are identifying a disproportionate number of racial and ethnic minorities.

Objective: Determine to what extent TSA's SPOT program is screening passengers at U.S. airports in an objective and cost-effective manner to identify potential terrorism and/or criminal activity. *Office of Audits*

Personnel Security and Internal Control at TSA's Legacy Threat Assessment and Credentialing Office, Congressionally Requested

Representative Bennie G. Thompson, Ranking Member of the House Committee on Homeland Security, requested that DHS OIG review the background investigations and suitability determinations conducted for TSA Transportation Threat Assessment and Credentialing (TTAC) personnel. Specifically, Representative Thompson requested that OIG review the quality, fairness, and impartiality of the clearance and suitability system at TTAC, and determine how TTAC evaluates judgment, reliability and trustworthiness. DHS' TTAC office was established as the lead entity for conducting security threat assessments and credentialing initiatives for domestic passengers on public and commercial modes of transportation, transportation industry workers, and individuals seeking access to critical infrastructure.

Objectives: (1) Assess the quality, fairness, and impartiality of the clearance and suitability system at TTAC and (2) determine how TTAC evaluates judgment, reliability and trustworthiness. *Office of Inspections*

TSA Information Technology Management, Discretionary

TSA is composed of more than 50,000 security officers, inspectors, directors, air marshals, and managers who protect the Nation's transportation systems. The organization maintains an IT budget of nearly $800 million, the second largest IT budget within DHS. Due to the nature of TSA's mission, TSA must share information across components, with other Federal agencies, and with State and local partners. This is a followup audit of an October 2007 report that highlighted ongoing inefficiencies in TSA's operational environment and IT infrastructure. Since our previous review, TSA has begun testing and advancing a variety of new systems and technologies, which should be reviewed for alignment with DHS and Federal standards.

Objective: Determine whether TSA's IT approach includes adequate planning, implementation, and management to support efficient and effective protection of the Nation's transportation systems. *Office of IT Audits*

Controls Over TSA's Vetting of Secure Identification Display Area Badges, Discretionary

The *Aviation and Transportation Security A*ct directs TSA to improve the security of airports, including security related to airport workers. TSA has the statutory responsibility for issuing Secure Identification Display Area (SIDA) badges, which are identification devices that establish which areas of the airport an employee is authorized to access. Employment investigations, including a criminal history record check, fingerprint-based checks, vetting against terrorist databases, and a review of available law enforcement databases and other records, are required for issuance. TTAC is responsible for vetting SIDA badges.

Objective: Determine (1) the accuracy and reliability of data TSA uses to vet SIDA badge workers and (2) identify enhancements to the TSA vetting process. *Office of IT Audits*

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

Planned Projects

Information Technology Matters Related to the USCIS Component of the FY 2012 DHS Financial Statement Audit, Mandatory

We contract with an IPA firm to conduct DHS' annual financial statement audit. As a part of this annual audit, the IPA firm's IT auditors review 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*

USCIS Controls To Ensure That Employers With 50 Percent or More H1B Employees Properly Declare Their Status, Discretionary

According to P.L. 111-230, employers petitioning for H1-B workers must identify themselves if they have 50 or more employees, and if their workforce consists of 50 percent or more H1-B or L status employees. These employers have to pay an additional $2,000 application fee. These requirements apply to applications submitted after August 14, 2010.

Objective: Perform data analysis to determine whether employers meeting the requirements of P.L. 111-230 are correctly self-identifying themselves. *Office of IT Audits*

USCIS Transformation, Discretionary

Effective use of IT, coupled with updated processes, is vital to increase efficiency and address demands in processing immigration benefits. In our 2011 report, we found that the implementation of the transformation program was delayed because of changes in the deployment strategy and insufficiently defined system requirements. These inefficiencies and delays have resulted in USCIS' continued reliance on paper-based processes to support its mission, which hinders USCIS' ability to process immigration benefits efficiently, combat identity fraud, and provide other government agencies with the information required to identify criminals and possible terrorists.

Objective: Assess progress made in implementing transformation program initiatives, as well as addressing our prior recommendations. *Office of IT Audits*

Projects In-progress

Adjudication of I-130 Marriage-based Petitions, Discretionary

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 is 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 percent. 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*

Security and Monitoring of U.S. Citizenship and Immigration Services' EB-5 Immigrant Investor Pilot Program, Discretionary

Through the EB-5 Immigrant Investor program, USCIS offers 10,000 green cards per year to foreigners who invest $1,000,000 in any qualifying U.S. business, or $500,000 in a targeted or underperforming employment sector. During prior audit work, a USCIS employee raised concerns to DHS OIG about the program's vulnerability to fraud and national security threats. Media sources have also raised concerns about the program's vulnerability to fraud and victimization, and about USCIS's qualifications to evaluate and monitor investment justifications and outcomes.

Objectives: Determine whether USCIS's management of the EB-5 Immigrant Investor Pilot program (1) detects and resolves potential immigration fraud and national security threats, and (2) effectively evaluates and monitors investment justifications and outcomes. *Office of Audits*

Followup Review of the L Intracompany Transferee Visa Program, Congressionally Requested

Senator Charles E. Grassley requested that DHS OIG conduct a followup 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 in our 2006 report. *Office of Inspections*

Iraqi Refugees Wrongfully Admitted to the United States, Congressionally Requested

This review is a request from Senator Charles E. Schumer, Chairman, Senate Judiciary Subcommittee on Immigration, Refugees and Border Security; and Senator Rand Paul, asking that we determine how two Iraqi refugees, Waad Ramadan Alwan and Mohmad Shreef Hammadi, who were charged with terrorism-related offenses, gained admission into the United States.

Objectives: Determine whether (1) DHS had information that could have been used to deny Alwan's and Hammadi's admission into the United States and (2) there are safeguards in the Department's refugee program that will eliminate flaws and vulnerabilities. *Office of Inspections*

DHS Administration of the T and U Visa Process, Discretionary

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 COAST GUARD

Planned Projects

Information Technology Matters Related to USCG Component of the FY 2012 DHS Financial Statement Audit, Mandatory

We contract with an IPA firm to conduct DHS' annual financial statement audit. As a part of this annual audit, the IPA firm's IT auditors review 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, Discretionary

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 11 missions related to 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 requirements, the USCG Privacy Office works with programs to steward and instill an effective 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 laws, regulations, and policies. *Office of IT Audits*

USCG Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Modernization, Discretionary

USCG's C4ISR project will provide an integrated group of systems that are interoperable across all USCG ships, aircraft, and shore sites. The purpose is to supply the tools, intelligence, and common operating picture necessary to detect, identify, and prosecute intended targets. These technologies will also provide the foundation for interoperability with USCG's partners within DHS, the Department of Defense, and other law enforcement and emergency services agencies.

***Objective*:** Evaluate the progress USCG has made with C4ISR systems and determine how well these systems support the integration of USCG and DHS. *Office of IT Audits*

USCG Laptop Security, Discretionary

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 USCG has implemented an effective program to protect the security and integrity of its laptop computers. *Office of IT Audits*

USCG Information Technology Insider Threat, Discretionary

As the agency becomes increasingly dependent upon complex information systems, the inherent risk to these systems by computer crimes and security attacks increases. Despite the classified and high-tech nature of these DHS systems and the technological expertise required to develop and maintain them, the emphasis on adequate attention by experts to safeguarding them against technological vulnerabilities has not always followed suit. The trusted insider, given access and status within the organization, poses the biggest threat to the protection of life, property, and information for the component.

Objective: Determine the effectiveness of the steps USCG has taken to address the insider threat risk on IT systems. This includes determining whether (1) an Insider Threat Program Office has been established, (2) an insider threat-specific security awareness program exists, and (3) USCG is prepared to detect and resolve insider attacks. *Office of IT Audits*

USCG Operations on the Rio Grande, Discretionary

There has been a significant increase in drug importation and drug-related violence along the Rio Grande portion of the U.S. border with Mexico. This endangers the lives of Federal and

local law enforcement officials, as well as the lives and property of U.S. citizens who live near the border. Failing to secure the Rio Grande adequately also risks an increase in the nationwide distribution of narcotics and the establishment of Mexican drug cartels on U.S. soil. A recent USCG assessment concluded that the current use of resources and personnel along the Rio Grande is sufficient; however, the increasing level of violence on both sides of the border and the volume of illegal drugs involved justifies an independent review.

Objective: Determine whether USCG operations and resources along the Rio Grande border between the United States and Mexico adequately support its mission as the lead Federal agency for maritime drug interdiction. *Office of Audits*

USCG's Implementation of Recommendations in Deepwater Horizon After-Action Reports, Discretionary

The Deepwater Horizon oil spill was the first spill of national significance and the first time a National Incident Commander was named. Organizing and directing the response to the Deepwater Horizon oil spill required uniting the efforts of more than 47,000 Federal, State, and local responders, including more than 6,600 active and reserve USCG members. The response employed more than 835 oil skimmers, 11 million feet of boom, more than 6,100 response boats and 3,190 vessels of opportunity, and more than 120 aircraft. A number of after-action reports, containing numerous recommendations, have been or are scheduled to be issued.

Objective: Determine whether USCG has implemented recommendations in Deepwater Horizon Oil Spill After-Action Reports, including those issued by the National Incident Commander, the Presidential Oil Spill Commission, the Joint Industry Oil Spill Preparedness & Response Task Force, and the British Petroleum Deepwater Horizon Oil Spill Incident Specific Preparedness Review. *Office of Audits*

Projects In-progress

Marine Accident Reporting to the USCG, Discretionary

To aid in identifying, preventing, and minimizing marine accidents and casualties, 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 these specific categories require the filing of an CG-2692 form, Marine Accident Report, it is unclear how USCG enforces this requirement.

If the feedback loop in the report-filing process is not adequately enforced, 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 fail to identify serious hazardous conditions, be unnecessary, or not be implemented due to the lack of information or erroneous information. If crew personal injury accidents are underreported,

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 USCG.

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 nonhomeland security missions. Homeland security missions consist of Illegal Drug Interdiction; Undocumented Migrant Interdiction; Foreign Fish Enforcement; Ports, Waterways, and Coastal Security; and Defense Readiness. Nonhomeland 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 nonhomeland security missions. *Office of Audits*

USCG's Annual Mission Performance (FY 2012), Mandatory

The *Homeland Security Act of 2002* directs the Inspector General to review annually the performance of all USCG missions, with particular emphasis on nonhomeland security missions. Homeland security missions consist of Illegal Drug Interdiction; Undocumented Migrant Interdiction; Foreign Fish Enforcement; Ports, Waterways, and Coastal Security; and Defense Readiness. Nonhomeland 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 nonhomeland security missions. *Office of Audits*

USCG Reutilization and Disposal Program, Discretionary

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*

UNITED STATES CUSTOMS AND BORDER PROTECTION

Planned Projects

Information Technology Matters Related to the FY 2012 Financial Statement Audit of CBP, Mandatory

We contract 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 review 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*

CBP Controls To Ensure Fingerprinting of All International Travelers Seeking Admission Into the United States, Discretionary

To support DHS' mission of protecting our Nation, CBP fingerprints international travelers at U.S. air ports of entry and validates travelers against information in a number of systems to which CBP has access. CBP uses the biographic and biometric information to determine whether to admit the travelers, and transmits such information to the Arrival and Departure Information System (ADIS) maintained by US-VISIT to perform analysis aimed at detecting and deterring identity fraud.

Objectives: Determine whether CBP properly captures all biometric and biographic information from international travelers, and transmits this information to ADIS. *Office of IT Audits*

Extent of Fraud in the Uncollectible Amounts Related to Anti-Dumping/Countervailing Duties, Discretionary

In its Annual Financial Report for Fiscal Year 2010, CBP estimated that the uncollectible amount for anti-dumping (AD)/countervailing (CV) duties totaled more than $487 million. This amount represented more than 88 percent of the $551 million in gross receivables. The agriculture and aquaculture industry represents 87 percent of all uncollected AD/CV duties. Four products, all from China, are responsible for approximately 84 percent of all uncollected AD/CV duties. CBP

faces difficulties with these receivables, in part because some parties never intended to pay the duties. CBP had indicated that its ability to collect from certain importers is limited because the importers have no attachable assets in the United States.

Objective: Determine whether indicators exist that companies with uncollectible AD/CV duties that disappeared, ceased business operations, or declared bankruptcy subsequently open the same type of business under a different name. *Office of IT Audits*

Automated Targeting System, Discretionary

The Automated Targeting System (ATS) is an information system that captures and stores personally identifiable information. It is one of the most advanced targeting systems in the world. CBP officers use the system to identify cargo, individuals, or conveyances that may present a risk to the United States and its citizens.

Objective: Determine the effectiveness of CBP's system controls to protect the information collected, transmitted, and stored in the ATS. *Office of IT Audits*

CBP's Use of Unattended Ground Sensors To Secure U.S. Land Borders, Discretionary

Unattended ground sensors are part of CBP's multilayered approach to secure U.S. land borders. These sensors come in three main forms and are used by CBP to detect ground movement, recognize metal in passing vehicles, and sense breakage of spatial planes. As of June 2012, CBP has deployed 12,848 unattended ground sensors along the southern border with plans to acquire an additional 450 during the year. CBP faces various challenges regarding the effective use and proper performance of unattended ground sensors. The functionality of these devices is affected by physical and environmental challenges such as frozen ground on the northern border, battery life, and electromagnetic energy.

Objective: Determine whether CBP is effectively deploying, maintaining, and utilizing unattended ground sensors at U.S. land borders. *Office of Audits*

CBP's Ability To Respond to Incursion on the Southwest Border, Discretionary

CBP's Office of Border Patrol is the primary organization responsible for preventing the entry of aliens, terrorists, and terrorist weapons into the United States between official ports of entry. On the southern border, Office of Border Patrol is responsible for securing 2,000 miles of the border with Mexico. Gaps in coverage can occur when Border Patrol agents seize drugs or apprehend aliens and are required to provide transportation to the nearest Border Patrol station for processing, potentially leaving border zones unmanned.

Objective: Determine whether CBP's operational strategy and agent deployment provide adequate zone coverage to respond to incursions on the southwest border. *Office of Audits*

Ensuring the Integrity of CBP's Secure Electronic Network for Travelers Rapid Inspection Program, Discretionary

The Secure Electronic Network for Travels Rapid Inspection (SENTRI) program provides expedited processing for low-risk travelers. SENTRI applicants must voluntarily undergo a thorough biographical background check against law enforcement, customs, immigration, and terrorist indexes; a 10-fingerprint law enforcement check; and a personal interview with a CBP Officer. After approval, participants are issued a decal for their legally registered vehicle and a Radio Frequency Identification Document that transmits information to CBP's databases when the travelers pass through a SENTRI inspection line. Inspection time for SENTRI participants is reduced from 30 to 40 seconds to approximately 10 seconds. The program has expanded to 10 southwest border ports of entry and has more than 175,000 participants.

Smugglers and drug traffickers have used SENTRI participants to transit illegal persons, contraband, and drugs across the border. As a result, effective internal controls are essential for the program to deter and detect illegal activity.

***Objectives*:** Determine (1) the adequacy of CBP's internal controls to detect and deter smugglers and drug traffickers from using SENTRI participants to transport illegal persons, contraband, or drugs; (2) to what extent has CBP established redress procedures for participants who believe they were wrongfully terminated from the SENTRI program; and (3) to what extent CBP is using and sharing data collected from the SENTRI, NEXUS,[1] and Future Attribute Screening Technology (FAST)[2] programs to identify illegal activities and trends associated with these programs. *Office of Inspections*

Projects In-progress

CBP's 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. CBP employs radiation portal monitors to assist in identification of dangerous cargo. Radiation portal monitors provide an efficient means of scanning cargo—it takes seconds for one of the 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 they 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 the machines are performing at the same level as those in the GAO test sample, there is a potential for cargo security breaches.

[1] NEXUS is a joint program with the Canada Border Services Agency that allows prescreened, approved travelers faster processing.

[2] The FAST Mobile Modular project seeks to develop people-screening technologies that will enable security officials to test the effectiveness of current screening methods at evaluating suspicious behaviors and judging the implications of those behaviors.

Objective: Determine whether CBP and the Department are deploying and using radiation portal monitors to maximize cargo screening efforts, focusing resources on the highest risk cargo and entry ports. *Office of Audits*

Efficacy of CBP's Penalties Process, Congressionally Requested

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 of 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 consistently and is an effective deterrent. *Office of Audits*

Developing Efficiencies for the Acquisition, Conversion, and Maintenance of CBP and USCG H-60 Helicopters, Discretionary

DHS supports the world's largest law-enforcement aviation organization. Both CBP and USCG utilize H-60 helicopters; however, they have no common H-60 acquisition, conversion, or maintenance programs. To streamline efforts and potentially save money, on March 11, 2010, the Deputy Secretary signed an Acquisition Decision Memorandum that required CBP and USCG to coordinate, prepare, and present a review of joint aircraft requirements and capabilities, including H-60 helicopters. On January 6, 2011, the Under Secretary for Management signed another Acquisition Decision Memorandum for the H-60 projects, stating that it is time to explore alternatives for leveraging logistics functions so that future contracts can be affected.

Objective: Determine whether DHS and its components have developed efficiencies for the acquisition, conversion, and maintenance of CBP and USCG H-60 helicopters. *Office of Audits*

CBP's Use of Force, Congressionally Requested

This review originated as a request from Senator Robert Menendez and 15 members of the U.S. House of Representatives, who expressed concern about the death of Anastasio Hernandez Rojas, who was in CBP's custody at the time of his death. The members of Congress requested that DHS OIG determine whether the Rojas incident is emblematic of a broader cultural problem within CBP.

Objectives: (1) Examine and summarize reports of investigation alleging brutality or use of excessive force by CBP employees; (2) determine what reforms DHS has implemented to

address the number of incidents involving the use of force by CBP employees; and (3) determine whether adding more agents and officers to the workforce has had an effect on training and professionalism. *Office of Inspections*

The IT Insider Threat at CBP, Discretionary

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*

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

Planned Projects

Information Technology Matters Related to the ICE Component of the FY 2012 DHS Financial Statement Audit, Mandatory

We contract with an IPA firm to conduct DHS' annual financial statement audit. As a part of this annual audit, the IPA firm's IT auditors review 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*

ICE's Management of Its *Federal Employees' Compensation Act* Program, Discretionary

The *Federal Employees' Compensation Act* (FECA) provides wage loss compensation, medical care, and survivors' benefits to Federal and postal workers for employment-related traumatic injuries and occupational diseases. FECA is a self-insured program administered by the U.S. Department of Labor. FECA benefits are financed by the Employees' Compensation Fund, which is replenished annually through chargeback to employing agencies. In FY 2010 ICE's unaudited actuarial FECA liability was $211 million, which was the third highest liability within the Department. Overall DHS's unaudited actuarial FECA liability was $1.94 billion for FY 2010.

Objectives: Determine whether ICE (1) is effectively managing its FECA program to minimize lost workdays and FECA-related compensation costs by returning work-capable employees to work at the earliest date suggested in a medical report and (2) utilizes an effective process to validate its workers' compensation chargeback reports to ensure that the billing is correct. *Office of Audits*

ICE's Management of Medical Care for Detained Aliens, Discretionary

ICE apprehends, detains, and removes illegal aliens from the United States. Aliens in custody must be given appropriate medical treatment and care. In 2011, ICE revised its Performance-Based National Detention Standards, which include standards for medical care. Under the revised standards, detainees should have access to appropriate and necessary medical, dental, and mental health care, including emergency services. In prior audit work, DHS OIG evaluated and made numerous recommendations to improve the management of mental health care.

Objective: Determine whether ICE has developed and implemented policies, procedures, and controls to provide medical care to detainees in accordance with the 2011 Performance-Based National Detention Standards. *Office of Audits*

Detention and Deportation of U.S. Citizens, Discretionary

ICE cannot assert its civil immigration enforcement authority to arrest, detain, or deport an individual unless the person arrested is an alien. Nonetheless, ICE has arrested and in some instances deported U.S. citizens. ICE attempted to clarify its efforts to prevent the detention and deportation of U.S. citizens in a November 2009 memorandum. Despite this effort, detention and deportation of U.S. citizens have continued, which calls into question ICE's ability to oversee and monitor encounters with U.S. citizens.

Objectives: Determine the (1) circumstances surrounding the arrest, detention, and deportation of U.S. citizens; (2) methods ICE uses to establish U.S. citizenship; (3); effectiveness of the Public Advocate Office; and (4) efficacy of the November 2009 memorandum. *Office of Inspections*

Effectiveness of Alternatives to Detention, Discretionary

The Federal Government has been exploring alternatives to immigration detention for more than a decade. In 2009, ICE restructured its Intensive Supervision Appearance Program (ISAP). ICE awarded a contract to a single provider that conducts home and office visits, verifies employment, and monitors curfews. The contractor also relies on technologies such as global positioning satellite monitoring devices and telephonic reporting to increase oversight and reduce costs. In budget negotiations on the DHS appropriations bill, both the House and Senate approved at least $90 million to continue the program.

ISAP is a less expensive alternative to detention. However, lengthy and complex immigration proceedings can make it difficult to measure the program's effectiveness in the short term. Individuals in removal proceedings may cooperate until they receive a final order of removal. This risk also exists for individuals who are not in ISAP but are released on parole or a bond during immigration proceedings. Understanding the risks and benefits of ISAP would enable ICE to restructure the program as necessary before it awards another contract in 2014.

Objectives: Determine (1) the effectiveness of the risk matrix ICE completes for release from custody; (2) the rate at which individuals in the program have committed criminal acts or absconded has been reduced since 2009; and (3) what measures ICE could take to make the program more effective. *Office of Inspections*

The Performance of 287(g) Agreements Report - FY 2013 Update, Mandatory

Section 287(g) of the *Immigration and Nationality Act* empowers DHS to delegate immigration enforcement authorities to State and local government agencies through formal written agreements and supervise the immigration enforcement activities of participating officers in these jurisdictions. The FY 2013 *DHS Appropriations Act* (H.R. 585) mandates that we review the delegation of law enforcement authority agreements that ICE enters into pursuant to section 287(g). The bill further requires that ICE cancel any 287(g) agreements where the Inspector General determines that the terms of the agreement have been violated.

Objective: We will review 287(g) agreements for any violation of the terms of such agreements. Specifically, we will determine whether ICE and law enforcement agencies with active 287(g) agreements are complying with the terms of respective agreements. *Office of Inspections*

Foreign Terrorist Organizations (FTOs), Congressionally Requested

We received an inquiry from Representative Peter T. King, who requested a review of DHS' actions and processes related to allowing members of foreign terrorist organizations to enter the United States.

Objectives: (1) Determine what DHS policies and procedures are in place for admitting members of FTOs into the United States, and evaluate whether the current policies and procedures present national security vulnerabilities; (2) assess the level of coordination between DHS and the Department of State when waivers for admission into the United States are granted to members of FTOs; (3) assess whether the admittance of specific individuals was in compliance with applicable Federal laws, DHS policies and procedures, or other requirements; and (4) establish whether DHS has a role in custodial transfers of foreign nationals who are in the Department of Justice custody on terrorism charges. *Office of Inspections*

Projects In-progress

ICE Worksite Enforcement Strategy, Discretionary

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 had conducted the required verification. ICE is the DHS component responsible for worksite enforcement. Stakeholders have criticized ICE's overall worksite enforcement program/strategy as either "too tough" or "not tough enough" when 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 to, and deterring U.S. employers and workers from violating *Immigration Reform and Control Act* requirements. *Office of Audits*

ICE Enforcement and Removal Operations Contract Funding and Payment Processes, Discretionary

ICE's Enforcement and Removal Operations (ERO) identifies and apprehends removable aliens, detains these individuals when necessary and removes illegal aliens from the U.S. ERO prioritizes the apprehension, arrest and removal of convicted criminals, those who pose a threat to national security, fugitives and recent border entrants.

During the FY 2011 and FY 2010 audits of the DHS financial statements, the independent public accounting firm KPMG LLP (KPMG), under contract with DHS OIG, reported that ICE ERO did not record a dollar value for obligations in the financial systems prior to incurring costs on various contracts. KPMG concluded that these conditions resulted in an increased risk of *Anti-Deficiency Act* violations at ICE.

Objective: To determine whether the ICE's ERO department is appropriately managing its contract funding and payments processes.

UNITED STATES SECRET SERVICE

Planned Projects

USSS IT Modernization, Discretionary

USSS is implementing a multiyear modernization program of its IT infrastructure and related systems. This program is estimated to cost more than $1.1 billion over 10 years.

Objective: Determine the progress made in modernizing USSS IT systems. *Office of IT Audits*

USSS' Network Security, Discretionary

DHS has issued Department-wide information security policies, guidance, and best practices to protect its network-connected resources against unauthorized disclosure, modification, or destruction. In September 2005, we identified deficiencies in USSS networks, such as a lack of policies and procedures on security testing, network monitoring, and configuration and patch management. Additionally, the results of our vulnerability assessments identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices, and weaknesses in configuration management.

Objective: To determine whether USSS has implemented effective controls to protect its networks. *Office of IT Audits*

USSS Administration of Workplace Programs, Discretionary

This is a self-initiated review of the effectiveness of USSS' administration of various workplace programs.

An advance team of Secret Service agents work with the host city, State and local law enforcement, and public safety officials to implement the necessary security measures, when the United States President travels. On April 11, 2012, 2 days prior to the President's arrival in Cartagena, Colombia, several members of an Advance Team allegedly drank alcohol excessively, visited strip clubs, and brought Colombian women to their hotel rooms. In response to allegations of misconduct, the USSS immediately recalled 11 agents to the United States and replaced them with agents from its Miami Field Office. The USSS conducted an internal investigation of this incident. In addition, as requested by the Senate committee on Homeland Security and Governmental Affairs, our office conducted an independent investigation into this matter.

Based on additional concerns by members of Congress, we will review how effectively the USSS administers workplace programs to determine whether the administration of these programs contribute in any way to the type of misconduct as reported in the Cartagena incident. We will also review the Memorandum of Understanding between the USSS and the DHS OIG for sharing/reporting information and conducting investigations.

Objectives: Determine (1) how effectively USSS is administering workplace programs, and (2) whether updates or revisions are needed to the 2003 Memorandum of Understanding between our office and the USSS regarding coordination on investigative matters. *Office of Inspections*

Projects In-progress

USSS After-Action Review of the Advance Team Incident in Cartagena, Colombia, Discretionary

This is a self-initiated review of USSS' investigation of allegations of misconduct by several members of an advance team in Cartagena, Colombia, prior to a scheduled presidential visit.

Objectives: Determine (1) the adequacy of the USSS' response to the incident in Colombia; (2) the adequacy of the scope, methodology, and conclusions of its ongoing investigation; and (3) the sufficiency of corrective actions taken or planned. *Office of Inspections*

MULTIPLE COMPONENTS

Planned Projects

The Use of Radio Frequency Identification Technology at DHS, Discretionary

Radio frequency identification (RFID) is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The main technology components of an RFID system are a tag, reader, and database. DHS uses RFID to track and identify trusted passengers or preregistered travelers, assets, weapons, and baggage on flights.

Objective: Determine whether DHS has effectively managed the implementation of RFID technology. *Office of IT Audits*

DHS Controls Over Foreign Military Sales and International Agreements, Discretionary

DHS components may sell excess assets to other countries through the Foreign Military Sales program or transfer assets under international agreements when they replace assets in their

inventory. These activities are governed by the FAR, Department of Defense Letters of Offer and Acceptance Guidance, as well as USCG and CBP policies and procedures for Foreign Military Sales activities.

Objective: Determine whether DHS has adequate policy, oversight, and controls in place for transfers of assets under the Foreign Military Sales program and international agreements. *Office of Audits*

FY 2012 Office of National Drug Control Policy 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*, DHS OIG is required to review assertions made by management related to FY 2012 obligations for the National Drug Control Program. We will contract with IPA firms to review CBP, USCG, and ICE ONDCP assertions. This review will address, 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
- FLETC Audit Report – Review of FY 2012 ONDCP Management Assertions
- FLETC Audit Report – Review of FY 2012 ONDCP Performance Summary Report
- FEMA Audit Report – Review of FY 2012 ONDCP Management Assertions
- FEMA Audit Report – Review of FY 2012 ONDCP Performance Summary Report

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

FY 2013 Office of National Drug Control Policy Reviews at CBP, ICE, and USCG, Mandatory

Under 21 U.S.C. §1704(d) and ONDCP Circular *Drug Control Accounting*, DHS OIG is required to review assertions made by management related to FY 2013 obligations for the National Drug Control Program. We will contract with IPA firms to review CBP, USCG, and ICE ONDCP assertions. This review will address, 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 2013 ONDCP Management Assertions
- CBP Audit Report – Review of FY 2013 ONDCP Performance Summary Report
- ICE Audit Report – Review of FY 2013 ONDCP Management Assertions
- ICE Audit Report – Review of FY 2013 ONDCP Performance Summary Report

- USCG Audit Report – Review of FY 2013 ONDCP Management Assertions
- USCG Audit Report – Review of FY 2013 ONDCP Performance Summary Report
- FLETC Audit Report – Review of FY 2013 ONDCP Management Assertions
- FLETC Audit Report – Review of FY 2013 ONDCP Performance Summary Report
- FEMA Audit Report – Review of FY 2013 ONDCP Management Assertions
- FEMA Audit Report – Review of FY 2013 ONDCP Performance Summary Report

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

DHS' Acquisition of Unmanned Aircraft Systems, Discretionary

CBP and the 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 Intelligence Enterprise and Activities, Discretionary

Since its inception, DHS has maintained an intelligence capability. In 2005, the DHS Secretary commissioned an evaluation of the programs and policies in DHS called the Second Stage Review. In the Second Stage Review, it was reported that DHS intelligence operations were not integrated or coordinated enough to be effective and were not meeting the needs of the stakeholders. In 2007, DHS OIG conducted a survey of the DHS Intelligence Enterprise, and the survey revealed problems were still occurring but improving in the Second Stage Review.

During the past 5 years, the DHS Intelligence Enterprise has improved its intelligence collection, information sharing activities, and processes. DHS has implemented plans for integration, coordination, and information sharing between the intelligence components and offices. New intelligence programs, activities, and intelligence collection technologies have made DHS intelligence better able to respond to its Federal, State and local government, and private sector customers.

Objectives: Determine the adequacy of (1) the activities within DHS that generate or disseminate intelligence-related information and each activity's mission, function, and capabilities; (2) the sources of information collected or obtained by the DHS intelligence enterprise activities, and how the information is collected or obtained; and (3) how intelligence products are disseminated. *Office of Inspections*

TSA's Oversight of the TSA Pre✓™ **Screening Initiative, Discretionary**

TSA's mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. To enhance its mission, TSA has partnered with CBP on the TSA Pre✓™ initiative. TSA Pre✓™ is a key component of the administration's intelligence-driven, risk-based approach to security and is designed to help TSA focus resources on higher-risk and unknown passengers, while expediting the process for lower-risk and known passengers whenever possible. TSA Pre✓™ is a voluntary program.

Once TSA vets a passenger and determines that the passenger is eligible for expedited screening in the TSA Pre✓™ program, information is embedded in the barcode of the passenger's boarding pass. TSA reads the barcode at designated airport locations and may direct eligible passengers to a lane where they will receive expedited screening. Eligible passengers are not guaranteed expedited screening, as TSA will continue to incorporate random and unpredictable security measures throughout airports.

In October 2011, TSA began the TSA Pre✓™ pilot program at four airports: Atlanta Hartsfield Jackson International Airport, Detroit Wayne County International Airport, Dallas Fort Worth International Airport, and Miami International Airport. Initially, participation was available only to Delta Airlines and American Airlines passengers. TSA continued to expand the program in 2012 to include additional airlines and airports. In May 2012, TSA's Administrator announced that the program had screened more than 1 million travelers. TSA Pre✓™ continued growth and passenger participation affirms TSA's commitment to the evolution of the intelligence-driven, risk-based security approach.

***Objectives*:** Determine (1) what processes and procedures exist to ensure proper vetting of participants, (2) how continued eligibility is ensured, and (3) how TSA processes are tested for effectiveness and timeliness. *Office of Inspections*

Research and Development Efforts to Secure Rail Transit Systems, Discretionary

We are initiating a review of the TSA and S&T research and development efforts to secure passenger rail transit systems against improvised explosives threats.

Millions of Americans use passenger rail systems, including subways, commuter rail, and light rail systems, daily. Passenger rail systems worldwide have been targets of terrorist attacks, primarily using improvised explosive devices. These attacks plus alleged terrorist plots against passenger rail systems in the United States show that these systems continue to be attractive targets for terrorists. In addition to being attractive targets, the openness and accessibility of passenger rail systems, high ridership volume, expensive infrastructure, and locations in or near large metropolitan areas make passenger rail systems a challenge to secure. TSA is responsible for securing the nation's transportation systems. TSA, along with S&T, share responsibilities for researching, developing, and deploying technologies to secure passenger rail transit systems. This includes technologies to detect the threat of improvised explosive devices against passenger rail systems.

Objectives: Determine (1) how critical gaps in detecting improvised explosives threats against passenger rail systems are identified and prioritized; and (2) how TSA and S&T coordinate research and development efforts to secure passenger rail systems. Office of Inspections

Information Sharing on Foreign Nationals: Interior Immigration Enforcement and Activities, Discretionary

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. A unified information sharing structure among these components would enhance decisions on claims and applications, impede the entry of ineligible persons, and augment investigations. This phase of the report focuses on in-country adjudications and investigations.

Objectives: Determine (1) the timeliness and thoroughness of information sharing 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*

DHS' Efforts To Address Weapons Smuggling to Mexico, Discretionary

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*

Projects In-progress

DHS' Involvement in the Investigative Operation "Fast and Furious," Congressionally Requested

Representative Michael T. McCaul requested that DHS OIG conduct a review of DHS' involvement in Operation "Fast and Furious," an Organized Crime Drug Enforcement Task Force effort to combat weapons smuggling to Mexico. Operation Fast and Furious began in January or February 2010, and included members of the DOJ Bureau of Alcohol, Tobacco, Firearms and Explosives, the United States Attorney's Office, and DHS ICE. The DHS Customs and Border Enforcement component may also have been involved.

Objectives: Determine DHS' (1) involvement in planning and implementing Operation "Fast and Furious" and (2) compliance with DHS policies, processes, and procedures for weapons smuggling investigations. *Office of Inspections*

Reducing Overclassification of DHS' Classified National Security Information, Mandatory

DHS OIG is conducting the first of two congressionally mandated evaluations of DHS' classified national security information program. P.L. 111-258, *Reducing Over-Classification Act*, October 2010, requires the Secretary of Homeland Security to develop a strategy to prevent the overclassification of homeland security and other information. We will evaluate the scope and nature of the DHS' classified national security information program with respect to its ability to properly classify homeland security information.

Objectives: Determine (1) the classification program's activities and challenges, (2) the effectiveness of the classification program, and (3) DHS' response to misclassification. *Office of Inspections*

AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

Project In-progress

Costs Claimed by Recipients of Recovery Act Funds Granted by FEMA for Fire Station Construction, and Maritime Port and Transit Security (17 audits), Mandatory

FEMA awarded 350 Fire Station Construction and Maritime Port and Transit Security grants valued at 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**

DHS OIG will select grantees for audit on the basis of grant expenditures and location of the project, and will issue separate reports on each grantee reviewed. This effort completes Phase III of DHS OIG's 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*

Chapter 6 – Other OIG Activities Planned for FY 2013

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

Council of the Inspectors General on Integrity and Efficiency, Homeland Security Roundtable

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was 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 Inspectors 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 DHS OIG Inspector General is the roundtable chair.

CIGIE – Investigations Committee Hotline Review

DHS OIG 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 OIG 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 (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 1 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 Information Technology Audits*

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. DHS OIG is 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 Legislative Affairs*

AUDIT AND INSPECTION OFFICES

Listed below are nontraditional projects and nonaudit services that our audit and inspection offices will undertake in FY 2013. The projects may or may not result in our issuing a report. 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 2013, Mandatory

The *Homeland Security Act of 2002* brought together 22 agencies to create a new Cabinet-level department focused on reducing U.S. vulnerability to terrorist attacks and natural disasters and minimizing damages and assisting in recovery from attacks and disasters 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 OIG 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 2013 as required by the *Reports Consolidation Act of 2000*. *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 Intelligence Community (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

To protect the Nation from dangerous people and dangerous goods, INV will—

- Open 100 percent of allegations of corruption or compromise of DHS employees or systems related to securing the Nation's borders, including the smuggling of drugs, weapons, and people (CBP – ICE);
- Open 100 percent of allegations of corruption or compromise of DHS employees or systems related to securing the Nation's federally regulated transportation systems (TSA); and
- Open 100 percent of allegations of corruption or compromise of DHS employees or systems related to immigration processes or documentation (USCIS – CBP).

To protect the civil rights and civil liberties of individuals and DHS employees, INV will—

- Investigate all ICE detainee deaths that involve suspicious circumstances;
- Investigate credible referrals of 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 DHS employee authority, including those that result in deprivation of rights.

To protect the integrity of DHS programs, as well as its assets, information, and infrastructure, INV will—

- Investigate significant grant and contract fraud allegations;
- Investigate gross misuse of classified information, privacy information, or law enforcement information;
- Investigate fraud involving FEMA contractors, claimants, or employees;
- Investigate allegations of corruption or criminal misconduct by DHS employees in the processing of immigration documentation (USCIS – CBP); and
- Exercise oversight of DHS component 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 by continuing to develop our hotline and referral process, and administering a robust training program and innovative training initiatives;
- Enhance our relationship and communication with DHS law enforcement component internal affairs offices to advance intelligence and information sharing; and
- Participate in CIGIE functions and other professional law enforcement organizations.

OFFICE OF MANAGEMENT

Efficiency Review Initiative

OM leads participation 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.

OM will continue to manage the Efficiency Review Initiative program within OIG, participate in bimonthly Component Efficiency Representative meetings, and participate in DHS working groups to develop new efficiency initiatives. In addition, OM will submit efficiency performance metrics quarterly to DHS Efficiency. The metrics provide the Department with a consistent framework for reviewing components' operational performance, and monitor the progress of efficiency initiatives using quantifiable and qualitative standards of measure.

In line with the spirit of both the Efficiency Review Initiative and the administration's Campaign to Cut Waste, OM will continue to increase the efficiency and effectiveness of OIG operations, and reduce administrative costs so that funds can be redirected toward the most significant mission-related priorities and challenges facing OIG.

Efficiency Task Forces

OM leads the coordination of our office's participation in several of the Secretary's efficiency task forces, including Civil Rights and Civil Liberties, Executive Secretariat, 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 with 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 information on homeland security and weapons of mass destruction. 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 DHS OIG's 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 professional standards and our OIG internal audit/inspection policies. During FY 2013, OM will conduct internal quality control reviews using its Planning and Compliance Division staff. OM will also determine whether our quality assurance program is suitably designed and 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 2013, 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, OM 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 OM's 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 matters that affect 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 and networking opportunities for new employees, especially for those from underrepresented groups.

Alternative Workplace Arrangements

OM will continue to oversee 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 was launched as an approach to design and implement new work environments for our field office locations. The objectives are to maintain or reduce lease costs, minimize renovation costs (if necessary), and improve 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 can provide an excellent return on investment. This innovative approach is in line with the administration's requirements to increase occupancy rates in current facilities through a phased approach to space management, and to offset reductions in inventory when new space is required.

Information Technology Division

During FY 2013, OM will support and enable the mission with technology through the Information Technology Division. For FY 2013, OM will focus on—

- Enhancing the enterprise data system case management system and enterprise applications that support mission needs, technology efficiencies, and systems effectiveness;
- Modernizing IT infrastructure to meet current DHS and OMB mandates;
- Strengthening cybersecurity to include HSPD-12 compliance for logical system access and continuous monitoring; and
- Executing and coordinating the OIG IT budget and spending plan.

Training and Workforce Development

During FY 2013, OM will support organizational-wide training and workforce development initiatives through the Training and Workforce Development Division. For FY 2013, OM will focus on enhancing programs that support employees' professional goals to provide comprehensive, systematic, and cost-effective career development, education, and training systems to improve organizational efficiency and effectiveness. OM will collaborate with program offices and a cadre of 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 curriculums. OM will continue the Mentor-Protégé program, which provides invaluable insight and a continuity of pass-along knowledge beyond the employee's own education and experiences. Incorporating human performance technology methodologies, processes, and policies, OM will strengthen the OIG workforce to further refine and document individual workforce competencies that directly influence a well-trained, certified, and highly qualified workforce. Partnering with

internal and external stakeholders, OM will work collaboratively with CIGIE, DHS's Enterprise Learning Division, and other systems owners to standardize and consolidate learning/knowledge management and Web-based instructional systems.

Budget Initiatives

During FY 2013, 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 the FY 2013 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[3] requests;
- Manage travel service, including Government travel card transactions and travel voucher processing;
- Collaborate with stakeholders such as DHS, OMB, and congressional officials regarding the FY 2014 budget; and
- Formulate the 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 recommendations, congressional requests, and other correspondence that requires an OIG response. The system

[3] PRISM is a commercial-off-the-shelf software product that provides full procurement life-cycle support including all phases from advanced acquisition planning through contract closeout.

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 its tracking and workflow functions, 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

The OIG Performance Management Program's mission is to support the OIG organizational goals by promoting and sustaining a high-performance culture. Its purpose is to establish and maintain an employee performance appraisal program designed to improve individual and organizational performance through effective communication of performance. It is designed to foster two-way communication, establish accountability, and provide joint ownership of performance goals and outcomes.

OFFICE OF LEGISLATIVE AFFAIRS

OLA 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 support 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:

External Communications

The Media

OPA is the principal point of contact with the media and 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 timely.

DHS OIG.Gov

OPA, which is responsible for the content of OIG's public website, 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 by showcasing OIG reports and other activities. Additionally, we will use our website as a tool for educating and promoting transparency and openness among our internal and external customers.

Internal Communications

OIG Newslink

OPA publishes *OIG Newslink,* the digital monthly employee newsletter of the Office of Inspector General. The *Newslink* is a primary source of communication within OIG, with a target audience of more than 600 employees. It gives information on OIG current events and recognizes employee accomplishments.

OIG Media Review

OPA compiles and produces daily and weekly OIG Media Reviews, which provide OIG officials with comprehensive rundowns of current OIG press coverage and public perceptions of OIG's activities.

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.

OFFICE OF COUNSEL

OC enhances and supports the Inspector General's independence and provides 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, they 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 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 postemployment counseling, provides annual ethics training, and reviews annual financial disclosure reports for our employees.

Personnel

OC works closely with our office's HR 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 DOJ 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 DOJ 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 DOJ 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, DOJ, 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, FOIA and the *Privacy Act*, and suspension and debarment; served on working groups to provide responses to legal questions posed by FLETC; 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 – Tables by DHS Components

Mandatory Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
CBP	IT Matters Related to the FY 2012 Financial Statement Audit of CBP	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
CBP	CBP's Use of Radiation Portal Monitors at Seaports	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Trade Operations and Security	In-progress	OA
FEMA	IT Matters Related to the FEMA Component of the FY 2012 DHS Financial Statement Audit	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
FEMA	State Homeland Security and Urban Area Grant Audits	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Grants Management	Planned	OA
FEMA	State Homeland Security and Urban Area Grant Audits (North Carolina, Kentucky, Rhode Island, Massachusetts, American Samoa, Northern Mariana Islands, Guam, Indiana, Virginia, Mississippi, Connecticut, Nebraska)	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Grants Management	In-progress	OA
FLETC	IT Matters Related to the FLETC Component of the FY 2012 DHS Financial Statement Audit	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
I&A	Annual Evaluation of DHS' Information Security Program (Intelligence Systems-IC IG) for FY 2013	M4 – Safeguarding and Security Cyberspace	Planned	ITA
I&A	Annual Evaluation of DHS' Information Security Program (Intelligence Systems) for FY 2013	M4 – Safeguarding and Security Cyberspace	Planned	ITA
Mgmt	IT Matters Related to the FY 2012 Financial Statement Audit – DHS Consolidated	M4 – Safeguarding and Security Cyberspace	Planned	ITA
Mgmt	Annual Evaluation of DHS' Information Security Program for FY 2013	M4 – Safeguarding and Security Cyberspace	Planned	ITA
Mgmt	FY 2013 *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	Maturing and Strengthening DHS ; Major Management Challenge-Financial Management	Planned	OA

Mandatory Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
Mgmt	DHS' FY 2013 Compliance With the *Improper Payments Elimination and Recovery Act of 2010*	Maturing and Strengthening DHS; Major Management Challenges-Financial Management and Acquisitions	Planned	OA
Mgmt	Other than Full and Open Competition Contracting During Fiscal Year 2012	Maturing and Strengthening DHS; Major Management Challenge-Acquisitions	Planned	OA
Mgmt	Other than Full and Open Competition Contracting During Fiscal Year 2013	Maturing and Strengthening DHS; Major Management Challenge-Acquisitions	Planned	OA
Mgmt	*Single Audit Act* Reviews	Maturing and Strengthening DHS; Major Management Challenges-Grants Management	Planned	OA
Mgmt	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	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	In-progress	OA
Mgmt	DHS Compliance with Federal Acquisition Regulation Revisions for the Proper Use and Management of Cost Reimbursement Contracts	Maturing and Strengthening DHS; Major Management Challenge-Acquisitions	In-progress	OA
TSA	IT Matters Related to the TSA Component of the FY 2012 DHS Financial Statement Audit	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
TSA	Covert Testing of TSA's Law Enforcement Officer Screening Procedures	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	OA
USCG	IT Matters Related to the USCG Component of the FY 2012 DHS Financial Statement Audit	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
USCG	USCG's Annual Mission Performance (FY 2012)	Maturing and Strengthening DHS	Planned	OA
USCG	USCG's Annual Mission Performance (FY 2011)	Maturing and Strengthening DHS	In-progress	OA
USCIS	Information Technology Matters Related to the USCIS Component of the FY 2012 DHS Financial Statement Audit	M4 – Safeguarding and Securing Cyberspace	Planned	ITA

Mandatory Projects

DHS Component	Project Title	DHS Strategic Mission Area/ Management Challenge	Project Status	OIG Office
USICE	The Performance of 287(g) Agreements Report - FY 2013 Update, Mandatory ICE's 287(g) Agreements Report Update (Mandatory)	M3 – Enforcing and Administering Our Immigration laws	Planned	ISP
USICE	IT Matters Related to the ICE Component of the FY 2012 DHS Financial Statement Audit	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
Multiple Components	FY 2012 Office of National Drug Control PolicyReviews at CBP, ICE, and USCG	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	Planned	OA
Multiple Components	FY 2013 Office of National Drug Control Policy Reviews at CBP, ICE, and USCG	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	Planned	OA
Multiple Components	Reducing Over-classification of DHS' Classified National Security Information	Maturing and Strengthening DHS	In-progress	ISP

Congressionally Requested Projects

DHS Component	Project Title	DHS Strategic Mission Area/ Management Challenge	Project Status	OIG Office
CBP	Efficacy of CBP's Penalties Process	M2 – Securing and Managing Our Borders; Major Management Challenge-Trade Operations and Security	In-progress	OA
CBP	U.S. Customs and Border Protection's Use of Force	M3 – Enforcing and Administering Our Immigration Laws; Major Management Challenge-Border Security	In-progress	ISP
FEMA	FEMA's Efforts To Recoup Improper Payments in Accordance with the *Disaster Assistance Recoupment Fairness Act of 2011*	M5 – Ensuring Resilience to Disasters; Major Management Challenges-Emergency Management and Financial Management	Planned and in-progress quarterly reports	EMO
Mgmt	DHS' Internal Controls Over Travel, Conferences, and Employee Awards Programs	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	In-progress	OA
NPPD	Effectiveness of the Infrastructure Security Compliance Division's Management Practices To Implement the Chemical Facilities Anti-Terrorism Standards Program	M1 – Preventing Terrorism and Enhancing Security	In-progress	ISP
TSA	Management and Oversight of Transportation Security at Honolulu International Airport	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	In-progress	OA
TSA	TSA Procurement of Security Badge Vetting Services	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenges-Transportation Security and Acquisitions	In-progress	OA
TSA	Transportation Security Administration's Screening Partnership Program	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	In-progress	OA
TSA	TSA Deployment and Use of Advanced Imaging Technology	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	In-progress	OA
TSA	TSA's Screening of Passengers by Observation Techniques (SPOT) Program	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	In-progress	OA

Congressionally Requested Projects

DHS Component	Project Title	DHS Strategic Mission Area/ Management Challenge	Project Status	OIG Office
TSA	Personnel Security and Internal Control at TSA's Legacy Threat Assessment and Credentialing Office	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	ISP
USCIS	Followup Review of the L Intracompany Transferee Visa Program	M3 – Enforcing and Administering Our Immigration Laws	In-progress	ISP
USCIS	Iraqi Refugees Wrongfully Admitted to the United States	M1 – Preventing Terrorism and Enhancing Security, M2 – Securing and Managing Our Borders, M3 – Enforcing and Administering Our Immigration Laws; Major Management Challenge-Border Security	In-progress	ISP
USICE	Representative King - OIG Response – Foreign Terrorist Organizations (FTOs) (placeholder)	M3 – Enforcing and Administering Our Immigration Laws	Planned	ISP
Multiple Components	DHS's Involvement in the Investigative Operation "Fast and Furious"	M1 – Preventing Terrorism and Enhancing Security, M2 – Securing and Managing Our Borders	In-progress	ISP

Recovery Act Projects

DHS Component	Project Title	DHS Strategic Mission Area/ Management Challenge	Project Status	OIG Office
FEMA	Costs Claimed by Recipients of *American Recovery and Reinvestment Act* Funds Granted by FEMA for Fire Station Construction, Maritime Port Security, and Transit Security, 17 audits	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Grants Management	In-progress	OA

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
CBP	CBP Controls To Ensure Fingerprinting of All International Travelers Seeking Admission Into the United States	M4 – Safeguarding and Security Cyberspace	Planned	ITA
CBP	Extent of Fraud in the Uncollectible Amounts Related to Anti-Dumping/Countervailing Duties	M4 – Safeguarding and Security Cyberspace	Planned	ITA
CBP	Automated Targeting System	M4 – Safeguarding and Security Cyberspace	Planned	ITA
CBP	CBP's Use of Unattended Ground Sensors To Secure U.S. Land Borders	M2 – Securing and Managing Our Borders; Major Management Challenge-Border Security	Planned	OA
CBP	CBP's Ability To Respond to Incursion on the Southwest Border	M2 – Securing and Managing Our Borders; Major Management Challenge-Border Security	Planned	OA
CBP	Ensuring the Integrity of CBP's Secure Electronic Network for Travelers Rapid Inspection Program	M2 – Securing and Managing Our Borders, M3 – Enforcing and Administrating Our Immigration Laws; Major Management Challenge-Transportation Security	Planned	ISP
CBP	Developing Efficiencies for the Acquisition, Conversion, and Maintenance of CBP and USCG H-60 Helicopters, Discretionary	M2 – Securing and Managing Our Borders	In-Progress	OA
CBP	The IT Insider Threat at CBP	M4 – Safeguarding and Security Cyberspace	In-Progress	ITA
FEMA	FEMA Privacy Stewardship	Maturing and Strengthening DHS	In-Progress	ITA
FEMA	Capping Report: FY 2012 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits	M5 – Ensuring Resilience to Disasters; Major Management Challenges-Grants Management, Emergency Management, and Financial Management	Planned	EMO
FEMA	Disaster Assistance Grants – Regional Offices	M5 – Ensuring Resilience to Disasters; Major Management Challenges-Grants Management, Emergency Management, and Financial Management	Planned	EMO
FEMA	Management Cost of FEMA's Area Field and Long-Term Recovery Offices	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	Duplication of FEMA Benefits From Hurricane Irene and Tropical Storm Lee	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
FEMA	FEMA's Decisions To Repair or Replace Damaged Facilities	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	Mission Assignment Eligibility and Closeout Activities	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	FEMA's Oversight of the Mission Assignment Process	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	Grantee Policies and Procedures for Evaluating Procurement Associated with Public Assistance Grant Funds	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	FEMA Public Assistance Grant Funds (Single Settlement Request) Awarded to Recovery School District (Master Plan), New Orleans, Louisiana, Discretionary	M5 – Ensuring Resilience to Disasters; Major Management Challenges-Emergency Management and Financial Management	Planned	EMO
FEMA	Hurricane Wilma Insurance Settlements to FEMA Subgrantees by the Florida League of Cities-Florida Municipal Insurance Trust	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	FEMA's Logistics Supply Chain Management System	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	OA
FEMA	Assistance to Firefighter Grants	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	OA
FEMA	FEMA's Management of the Temporary Housing Unit Program	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	Planned	EMO
FEMA	FEMA's Temporary Housing in 2011	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	In-Progress	EMO
FEMA	FEMA's Policy for Land Acquisition Costs of Permanently Relocated Damaged Facilities	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	In-progress	EMO
FEMA	FEMA's Deployment of Disaster Assistance Employees in Response to Hurricane Irene and Tropical Storm Lee	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	In-progress	EMO

Discretionary Projects

DHS Component	Project Title	DHS Strategic Mission Area/ Management Challenge	Project Status	OIG Office
FEMA	Personal Property at FEMA Joint Field Offices	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Emergency Management	In-progress	EMO
FEMA	FEMA's Oversight of Grantees Using a Risk-based Approach	M5 – Ensuring Resilience to Disasters; Major Management Challenge-Grants Management	In-progress	OA
I&A	Insider Threat at the DHS Office of Intelligence and Analysis	M4 – Safeguarding and Securing Cyberspace ;Maturing and Strengthening DHS	Planned	ITA
I&A	DHS' Watchlisting Cell Efforts To Coordinate Departmental Nominations	M1 – Preventing Terrorism and Enhancing Security	In-progress	ISP
Mgmt	Telework Security	Maturing and Strengthening DHS	Planned	ITA
Mgmt	DHS' Implementation of HSPD-12 Compliant Cards for Logical Access	Maturing and Strengthening DHS	Planned	ITA
Mgmt	Cloud Computing	Maturing and Strengthening DHS	Planned	ITA
Mgmt	Homeland Security Presidential Directive 20 (HSPD-20) Compliance	Maturing and Strengthening DHS	Planned	ITA
Mgmt	Technical Security Evaluation of Dallas-Forth Worth International Airport	Maturing and Strengthening DHS	Planned	ITA
Mgmt	Human Resource IT Consolidation/Modernization	Maturing and Strengthening DHS	Planned	ITA
Mgmt	DHS Financial Systems	Maturing and Strengthening DHS	Planned	ITA
Mgmt	Survey of Acquisition, Operation, and Maintenance of DHS' Aviation Assets	Maturing and Strengthening DHS; Major Management Challenges-Acquisition and Border Security	Planned	OA
Mgmt	DHS' Oversight of Fleet Management and Fuel Expenses	Maturing and Strengthening DHS; Major Management Challenge-Acquisition	Planned	OA
Mgmt	DHS' Use and Oversight of Other Transaction Agreements	Maturing and Strengthening DHS	Planned	OA
Mgmt	DHS' Competition in Contracts With One Bid Received, Discretionary	Maturing and Strengthening DHS	Planned	OA
Mgmt	Government 2.0/Web 2.0 – Social Media Use in DHS	Maturing and Strengthening DHS	In-progress	ITA
Mgmt	Technical Security Evaluation of Hartsfield-Jackson International Airport	M1 – Preventing Terrorism and Enhancing Security	In-Progress	ITA

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
Mgmt	Radio Communication Inventory	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenges-Emergency Management and Information Technology Management	In-Progress	OA
Mgmt	Homeland Security Information Network Review	M4 – Safeguarding and Security Cyberspace	In-Progress	ITA
Mgmt	Control Systems Cybersecurity	M4 – Safeguarding and Security Cyberspace	In-Progress	ITA
NPPD	Controls Over the Fraudulent Use of Documents To Obtain Entrance Into the United States	M3 – Enforcing and Administering Our Immigration Laws; M4 – Safeguarding and Security Cyberspace	Planned	ITA
NPPD	DHS' Implementation of Its Additional Cybersecurity Responsibilities	M4 – Safeguarding and Security Cyberspace	Planned	ITA
NPPD	National Cybersecurity Center's (NCSC) Effort To Coordinate Cyber Operations Centers Across the Government	M4 – Safeguarding and Security Cyberspace	Planned	ITA
NPPD	NPPD Privacy Stewardship	Maturing and Strengthening DHS	Planned	ITA
NPPD	National Cyber Security Review Status	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
NPPD	Effectiveness of the Federal Protective Service in Providing Security at Federal Facilities	M1 – Preventing Terrorism and Enhancing Security	Planned	OA
NPPD	Review of DHS's Disaster Recovery Program	Maturing and Strengthening DHS	In-Progress	ITA
OHA	National Bio-surveillance Integration System Audit	M4 – Safeguarding and Securing Cyberspace; Providing Essential Support to National and Economic Security	Planned	ITA
S&T	The Science and Technology Directorate's Research and Development Efforts to Detect Cyber Attacks Against the DHS' Network Systems	M4 – Safeguarding and Securing Cyberspace	Planned	ISP
S&T	Effects of Recent Portfolio Balancing Reviews and Budgetary Constraints on S&T's Workforce and Ability To Carry Out Its Mission	M1 – Preventing Terrorism and Enhancing Security; M4 – Safeguarding and Securing Cyberspace; M5 – Ensuring Resilience to Disasters; Major Management Challenges-Emergency Management, Infrastructure Protection, Transportation Security	Planned	ISP

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
S&T	Goals and Metrics for Science and Technology's Research Projects	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Infrastructure Protection	Planned	ISP
TSA	Controls Over the Transportation Security Administration's Vetting of Secure Identification Display Area (SIDA) Badges	M4 – Safeguarding and Securing Cyberspace; Maturing and Strengthening DHS	Planned	ITA
TSA	TSA IT Management	M4 – Safeguarding and Securing Cyberspace; Maturing and Strengthening DHS	Planned	ITA
TSA	Access to Secured Airport Perimeter Areas	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	OA
TSA	TSA's Airport Screening Equipment Maintenance Program	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	OA
TSA	Effectiveness of Automated Target Recognition in Passenger Screening	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	OA
TSA	TSA's Preclearance Aviation Security Operations Program	M1 – Preventing Terrorism and Enhancing Security, M2 – Securing and Managing Our Borders; Major Management Challenge-Transportation Security	Planned	ISP
TSA	Workforce Strength and Deployment in TSA's Federal Air Marshal Service	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	ISP
TSA	TSA's Office of Inspections Efforts	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	In-progress	OA
USCG	USCG Privacy Stewardship	M4 – Safeguarding and Security Cyberspace	Planned	ITA
USCG	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Modernization	M4 – Safeguarding and Security Cyberspace	Planned	ITA

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
USCG	Laptop Security	M4 – Safeguarding and Security Cyberspace	Planned	ITA
USCG	USCG IT Insider Threat	M4 – Safeguarding and Security Cyberspace	Planned	ITA
USCG	USCG Operations on the Rio Grande	M2 – Securing and Managing Our Borders; Major Management Challenge-Border Security	Planned	OA
USCG	USCG's Implementation of Recommendations in Deepwater Horizon After-Action Reports	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	Planned	OA
USCG	Marine Accident Reporting to the USCG	Maturing and Strengthening DHS	In-progress	OA
USCG	USCG Reutilization and Disposal Program	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	In-progress	OA
USCIS	USCIS Controls To Ensure That Employers with 50 Percent or More H1B Employees Properly Declare Their Status	M4 – Safeguarding and Security Cyberspace; Maturing and Strengthening DHS	Planned	ITA
USCIS	Adjudication of I-130 Marriage-based Petitions	M3 – Enforcing and Administering Our Immigration Laws	In-progress	OA
USCIS	Security and Monitoring of U.S. Citizenship and Immigration Services' EB-5 Immigrant Investor Pilot Program	M3 – Enforcing and Administering Our Immigration Laws	In-progress	OA
USCIS	DHS Administration of the T and U Visa Process, Discretionary	M3 – Enforcing and Administering Our Immigration Laws	In-progress	ISP
USCIS	USCIS Transformation	M4 – Safeguarding and Securing Cyberspace	Planned	ITA
USICE	ICE's Management of Its *Federal Employees' Compensation Act* Program	Maturing and Strengthening DHS; Major Management Challenge-Financial Management	Planned	OA
USICE	ICE's Management of Medical Care for Detained Aliens	M3 – Enforcing and Administering Our Immigration laws	Planned	OA

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
USICE	Detention and Deportation of U.S. Citizens	M3 – Enforcing and Administering Our Immigration Laws	Planned	ISP
USICE	Effectiveness of Alternatives to Detention	M3 – Enforcing and Administering Our Immigration Laws; Major Management Challenge-Border Security	Planned	ISP
USICE	DHS' Efforts To Address Weapons Smuggling to Mexico, Discretionary	M3 – Enforcing and Administering Our Immigration Laws	Planned	ISP
USICE	ICE Worksite Enforcement Strategy	M3 – Enforcing and Administering Our Immigration Laws	In-progress	OA
USICE	ICE Enforcement and Removal Operations Contract Funding and Payment Processes	M3 – Enforcing and Administering Our Immigration Laws; Major Management Challenge-Acquisition Management	In-progress	OA
USSS	U.S. Secret Service IT Modernization	M4 – Safeguarding and Security Cyberspace	Planned	ITA
USSS	United States Secret Service's Network Security	M4 – Safeguarding and Security Cyberspace	Planned	ITA
USSS	United States Secret Service Administration of Workplace Programs	M1 – Preventing Terrorism and Enhancing Security	In-progress	ISP
USSS	USSS After-Action Review of the Advance Team Incident in Cartagena, Colombia	M1 – Preventing Terrorism and Enhancing Security	In-progress	ISP
Multiple Components	The Use of Radio Frequency Identification (RFID) Technology at DHS	M4 – Safeguarding and Security Cyberspace	Planned	ITA
Multiple Components	DHS Controls Over Foreign Military Sales and International Agreements	M1– Preventing Terrorism and Enhancing Security; M2 – Securing and Managing Our Borders; Major Management Challenge-Acquisitions Management	Planned	OA
Multiple Components	DHS Intelligence Enterprise and Activities	M1 – Preventing Terrorism and Enhancing Security, M3 – Enforcing and Administering Our Immigration Laws	Planned	ISP

Discretionary Projects				
DHS Component	**Project Title**	**DHS Strategic Mission Area/ Management Challenge**	**Project Status**	**OIG Office**
Multiple Components	TSA's Oversight of the TSA Pre✓™ Screening Initiative	M1 –Preventing Terrorism and Enhancing Security, M2 – Securing and Managing Our Borders; Major Management Challenges-Transportation Security; Border Security	Planned	ISP
Multiple Components	Research and Development Efforts To Secure Rail Transit Systems	M1 – Preventing Terrorism and Enhancing Security; Major Management Challenge-Transportation Security	Planned	ISP
Multiple Components	Information Sharing on Foreign Nationals: Interior Immigration Enforcement and Activities	M3 – Enforcing and Administering Our Immigration Laws	Planned	ISP
Multiple Components	DHS' Acquisition of Unmanned Aircraft Systems	M2 – Securing and Managing Our Borders	Planned	OA

Appendix B – FY 2012 Annual Performance Report on Goals, Measures, and Accomplishments

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 at strengthening the Department and achieving our strategic goals. The following chart represents our Annual Performance Report, or our accomplishments for FY 2012.

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.	Yes
1.2	Achieve at least 85 percent concurrence with recommendations contained in OIG audit and inspection reports.[4]	94%
1.3	Complete draft reports for at least 75 percent of inspections and audits within 6 months of the project start date (i.e., entrance conference).	43%
1.4	Achieve at least a 50 percent implementation rate for OIG recommendations that are more than 1 year old.[4]	77%
Goal 2. Ensure integrity of DHS programs and operations.		
2.1	At least 75 percent of substantiated investigations are accepted for criminal, civil, or administrative action.[4]	68%
2.2	At least 75 percent of investigations referred resulted in indictments, convictions, civil findings, or administrative actions.[4]	68%
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 percent concurrence from DHS management with OIG recommendations on grant audits.[4]	85%
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 percent of peer review recommendations.	Yes
3.2	Ensure that 100 percent of DHS OIG employees have an annual Individual Development Plan.	Yes
3.3	Ensure that 100 percent of all eligible DHS OIG employees have a performance plan and receive an annual Rating of Record.	Yes

[4] Data results as of September 26, 2012.

Appendix C – FY 2013 Annual Performance Plan
Goals and Measures

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. In FY 2012, we coordinated a Focus Group to reassess our strategic goals, and our strategic planning team focused its efforts on refining performance measures. As a result of our strategic planning process, we adopted a new Strategic Plan covering FYs 2012 through 2016, with the following performance goals and measures for FY 2013.

Goal 1. Deliver relevant, accurate, and timely quality products and services, which identify the best use of taxpayer dollars.
1.1 Issue at least 95 audit and inspection reports during a fiscal year.
1.2 Issue at least 45 grant reports during a fiscal year.
1.3 Publicly issue nonclassified audit and inspection reports within 6 days of transmitting them to DHS.
1.4 Provide audit and inspection coverage of 80 percent of DHS' strategic objectives and major management challenges.
1.5 Achieve 90 percent concurrence on management report recommendations from DHS management.
1.6 Ensure that OIG Counsel confirms legal sufficiency of 100 percent of all OIG reports before issuance.
1.7 Achieve a 50 percent implementation rate for OIG recommendations that are more than 1 year old, based on the number of recommendations mutually closed by OIG and DHS.
1.8 Issue draft reports to DHS for audits and inspections within timeframes outlined in OIG guidance.
1.9 Implement 100 percent of peer review recommendations with which we agreed.

Appendix C – FY 2013 Annual Performance Plan
Goals and Measures (continued)

Goal 2. Protect the integrity of DHS programs and operations.
2.1 Achieve at least 75 percent of substantiated investigations that are accepted for criminal, civil, or administrative action.
2.2 Achieve at least 75 percent of investigations referred for indictments, convictions, civil findings, or administrative actions.
2.3 Identify and report cost savings, or funds put to better use.
2.4 Identify recoveries
2.5 Achieve at least 85 percent concurrence from DHS management on grant audit report recommendations.
2.6 Achieve disposition of 100 percent of OIG Hotline calls.
2.7 Identify and report monetary disallowances resulting from questioned, unsupported, and ineligible costs.

Appendix C – FY 2013 Annual Performance Plan
Goals and Measures (continued)

Goal 3. Attract, invest in, and retain a highly motivated, skilled, and agile workforce empowered through a robust infrastructure, modernized technology, and flexible worker-friendly policies.
3.1 Timely deliverables are provided to our customers, using our agency guidelines as benchmarks.
3.2 All employees receive midyear and annual performance evaluations.
3.3 All employees have an approved Individual Development Plan.
3.4 Increases in positive percentages are reflected on employee Human Capital satisfaction surveys sponsored by OPM.
3.5 All employees attend annual ethics training.
3.6 All employees meet required 40 hours of professional education training each year.
3.7 Increasing percentages of our employees have advanced degrees and professional certifications
3.8 Employee retention percentages increase.
3.9 Cost savings are realized in administrative areas other than IT.

Appendix D – OIG Headquarters and Field Office Contacts

Headquarters Address:

Department of Homeland Security
Attn: Office of Inspector General
245 Murray Drive, SW, Bldg 410
Washington, D.C. 20528
(202) 254-4100 / Fax: (202) 254-4285

Visit us at http://www.oig.dhs.gov/ for our Field Office Address Information.

Email:

dhs-oig.officepublicaffairs@dhs.gov

Telephone:

(202) 254-4100

Click here to: Subscribe to OIG Email Alerts

OIG Headquarters Senior Management Team:

Charles K. Edwards	……	Acting Inspector General
Carlton I. Mann	……	Acting Deputy Inspector General
Yvonne Manino	……	Acting Chief of Staff
Dorothy Balaban	……	Special Assistant to the Inspector General
Richard N. Reback	……	Counsel to the Inspector General
D. Michael Beard	……	Assistant Inspector General/Emergency Management Oversight
Anne L. Richards	……	Assistant Inspector General/Audits
John Dupuy	……	Acting Assistant Inspector General/Investigations
Deborah Outten-Mills	……	Acting Assistant Inspector General/Inspections
Frank Deffer	……	Assistant Inspector General/Information Technology Audits
Russell Barbee	……	Assistant Inspector General for Management
Philip D. McDonald	.....	Acting Director, Office of Legislative Affairs
William Hillburg	…….	Acting Director, Office of Public Affairs

Appendix E – Acronyms and Abbreviations

Acronyms and Abbreviations	Description
AD	anti-dumping
ADIS	Arrival and Departure Information System
AFR	Agency Financial Report
AIT	advanced imaging technology
ARRA	*American Reinvestment and Recovery Act of 2009*
ATS	Automated Targeting System
ATSA	*Aviation Transportation Security Act*
AWA	alternative workplace arrangement
BEST	Border Enforcement Security Task
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CBP	United States Customs and Border Protection
CFATS	Chemical Facilities Anti-Terrorism Standards
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CV	countervailing
DFW	Dallas Fort Worth
DARFA	*Disaster Assistance Recoupment Fairness Act of 2011*
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOJ	Department of Justice
EMO	Office of Emergency Management Oversight, Office of Inspector General
ERO	Enforcement and Removal Operations
FAMS	Federal Air Marshal Service
FAR	Federal Acquisition Regulation
FAST	Future Attribute Screening Technology
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*
FPS	Federal Protective Service
FTO	foreign terrorist organization
FY	fiscal year
GAO	Government Accountability Office
HMGP	Hazard Mitigation Grant Program
HSIN	Homeland Security Information Network
HRIT	Human Resources Information Technology
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis
IC	Intelligence Community

Acronyms and Abbreviations	Description
ICE	United States Immigration and Customs Enforcement
INV	Office of Investigations, Office of Inspector General
IPA	independent public accounting
ISAP	Intensive Supervision Appearance Program
ISCD	Infrastructure Security Compliance Division
ISP	Office of Inspections, Office of Inspector General
IT	Information technology
ITA	Office of Information Technology Audits, Office of Inspector General
NBIS	National Bio-surveillance Integration System
NCSD	National Cyber Security Division
NCTC	National Counterterrorism Center
NFIP	National Flood Insurance Program
NPPD	National Protection and Programs Directorate
NS/EP	National Secure/Emergency Preparedness
OA	Office of Audits, Office of Inspector General
OC	Office of Counsel
OFM	Office of Financial Management
OIG	Office of Inspector General
OLA	Office of Legislative Affairs, Office of Inspector General
OM	Office of Management, Office of Inspector General
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OPA	Office of Public Affairs, Office of Inspector General
OTA	Other Transaction Agreement
PA	Public Assistance
PAR	Performance and Accountability Report
RFID	radio frequency identification
PTS	Project Tracking System
S&T	Directorate for Science and Technology
SENTRI	Secure Electronic Network for Travels Rapid Inspection
SIDA	Secure Identification Display Area
SPOT	Screening of Passengers by Observation Techniques
SPP	Screening Partnership Program
TSA	Transportation Security Administration
TTAC	Transportation Threat Assessing and Credentialing
USCG	United States Coast Guard
USCIS	United States Customs and Immigration Service
USSS	United States Secret Service
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
VTVPA	*Victims of Trafficking and Violence Protection Act of 2000*
WLC	Watchlisting Cell

ADDITIONAL INFORMATION AND COPIES

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

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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