U.S. Department of Homeland Security Annual Financial Report

Fiscal Year 2012

Homeland Security

Our Vision

A homeland that is safe, secure, and resilient against terrorism and other hazards.

About this Report

The *U.S. Department of Homeland Security Annual Financial Report for Fiscal Year (FY) 2012* presents the Department's detailed financial information relative to our mission and the stewardship of those resources entrusted to us. It also highlights the Department's priorities, strengths, and challenges in implementing programs to enhance the safety and security of our Nation.

For FY 2012, the Department is using the alternative approach—as identified in the Office of Management and Budget's Circular A-136—to produce its Performance and Accountability Reports, which consists of the following three reports:

- ***DHS Annual Financial Report***: Delivery date – November 15, 2012.
- ***DHS Annual Performance Report***: Delivery date – February 4, 2013. The *DHS Annual Performance Report* is submitted with the Department's Congressional Budget Justification.
- ***DHS Summary of Performance and Financial Information:*** Delivery date – February 15, 2013.

When published, all three reports will be located on our public website at: http://www.dhs.gov/xabout/budget/editorial_0430.shtm.

For more information, contact:

Department of Homeland Security
Office of the Chief Financial Officer
Office of Financial Management
245 Murray Lane, SW
Mailstop 200
Washington, DC 20528

Information may also be requested by sending an email to par@hq.dhs.gov.

Homeland Security

Table of Contents

Message from the Secretary

November 14, 2012

I am pleased to submit the Department of Homeland Security's (DHS) Annual Financial Report for Fiscal Year (FY) 2012. This report provides an assessment of the Department's detailed financial information and our stewardship of taxpayer resources in support of our mission of securing the United States. This report also outlines our major goals and priorities within the framework of the Quadrennial Homeland Security Review (QHSR), Bottom-Up Review (BUR), and DHS Strategic Plan for Fiscal Years 2012-2016.

In each mission area, we have continued to grow and mature as a department by strengthening and building upon our existing capabilities, enhancing partnerships across all levels of government and with the private sector, and streamlining our operations and increasing efficiencies.

This November marks the tenth anniversary of the creation of DHS, the largest reorganization of the Federal Government since the formation of the Department of Defense. After ten years of effort, we have helped build a more effective and integrated Department, a strengthened homeland security enterprise, and a more secure America that is better equipped to confront the range of threats we face.

Priority Areas

We continue to build on the significant progress made by focusing on the Department's five key mission areas: preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. Additionally, DHS provides essential support to national and economic security and strives to maximize the effectiveness and efficiency of its operations by maturing and strengthening our management functions.

Preventing Terrorism and Enhancing Security

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

Securing and Managing Our Borders

DHS secures the Nation's air, land and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and

streamlining lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations.

Enforcing and Administering Our Immigration Laws

DHS is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. The Department has fundamentally reformed immigration enforcement, focusing on identifying and removing criminal aliens who pose a threat to public safety and targeting employers who knowingly and repeatedly break the law.

Safeguarding and Securing Cyberspace

DHS has the lead for the Federal Government to secure civilian government computer systems and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems. DHS analyzes and reduces cyber threats and vulnerabilities; distributes threat warnings; and coordinates the response to cyber incidents to ensure our computers, networks, and cyber systems remain safe.

Ensuring Resilience to Disasters

DHS provides the coordinated, comprehensive Federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with Federal, state, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include bolstering information sharing; providing grants, plans and training to our homeland security and law enforcement partners; and facilitating rebuilding and recovery where disasters strike.

Providing Essential Support to National and Economic 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; protecting the financial services sector; 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 other five homeland security missions.

Maturing and Strengthening the Department

Over the past four years, we have led the development and implementation of a comprehensive, strategic management approach to enhance Department-wide maturation and integration. We have made key investments to strengthen the homeland security enterprise, increase unification and integration, address challenges raised by the U.S. Government Accountability Office (GAO), and build upon the management reforms that have been implemented under this Administration.

Along with efforts to strengthen financial management, DHS has also made an unprecedented commitment to efficiency to better support frontline operations by building a culture of fiscal

discipline and accountability throughout the Department. Through the DHS-wide Efficiency Review and other cost saving initiatives, we have implemented a variety of initiatives to cut costs, share resources across our Components, and consolidate and streamline operations wherever possible. To date, these efforts have identified over $4 billion in cost avoidances and cuts.

At the same time, we have challenged our workforce to fundamentally rethink how to do business—from the largest to the smallest investments. In both 2011 and 2012, DHS has conducted formal base budget reviews looking at all aspects of the Department's budget to find savings and better align with operational needs.

This report highlights the Department's activities and accomplishments in each of these mission areas in FY 2012 and discusses upcoming initiatives that will build on these efforts to achieve a safer and more secure nation.

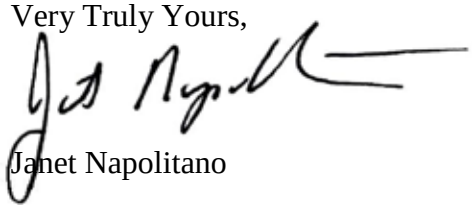
Management Assurances and Performance Measurement

Last year, DHS achieved a milestone that is a pivotal step towards increasing transparency and accountability for the Department's resources. For the first time since FY 2003, DHS earned a qualified audit opinion on its Consolidated Balance Sheet and Statement of Custodial Activity—highlighting the significant progress the Department has made in improving our financial management. Through these and other efforts across the Department, we will continue to ensure taxpayer dollars are managed with integrity, diligence, and accuracy and that the systems and processes used for all aspects of financial management demonstrate the highest level of accountability and transparency. This year, the Department expanded the scope of the FY 2012 financial statement audit to include three additional statements. Building on last year's success, the Department obtained a full-scope qualified audit opinion.

DHS is committed to improving performance measurement and accountability and I am able to provide reasonable assurance, based on our internal controls evaluations, that the performance measures reported for the Department in our performance and accountability reports are complete and reliable. DHS's performance and accountability reports for this and previous years are available on our public website: http://www.dhs.gov/xabout/budget/editorial_0430.shtm.

DHS has significantly improved the processes and structures in place to help ensure consistent operations for each of our financial accounting centers and financial management offices within our Components. The men and women of the Department of Homeland Security remain focused on achieving our objectives in the coming year while continuing to be responsible stewards of taxpayer resources.

Very Truly Yours,



Janet Napolitano

Management's Discussion and Analysis

The ***Management's Discussion and Analysis*** **(MD&A)** section explains the Department's organization, its mission and goals, and summarizes program and financial performance.

Mission and Organization

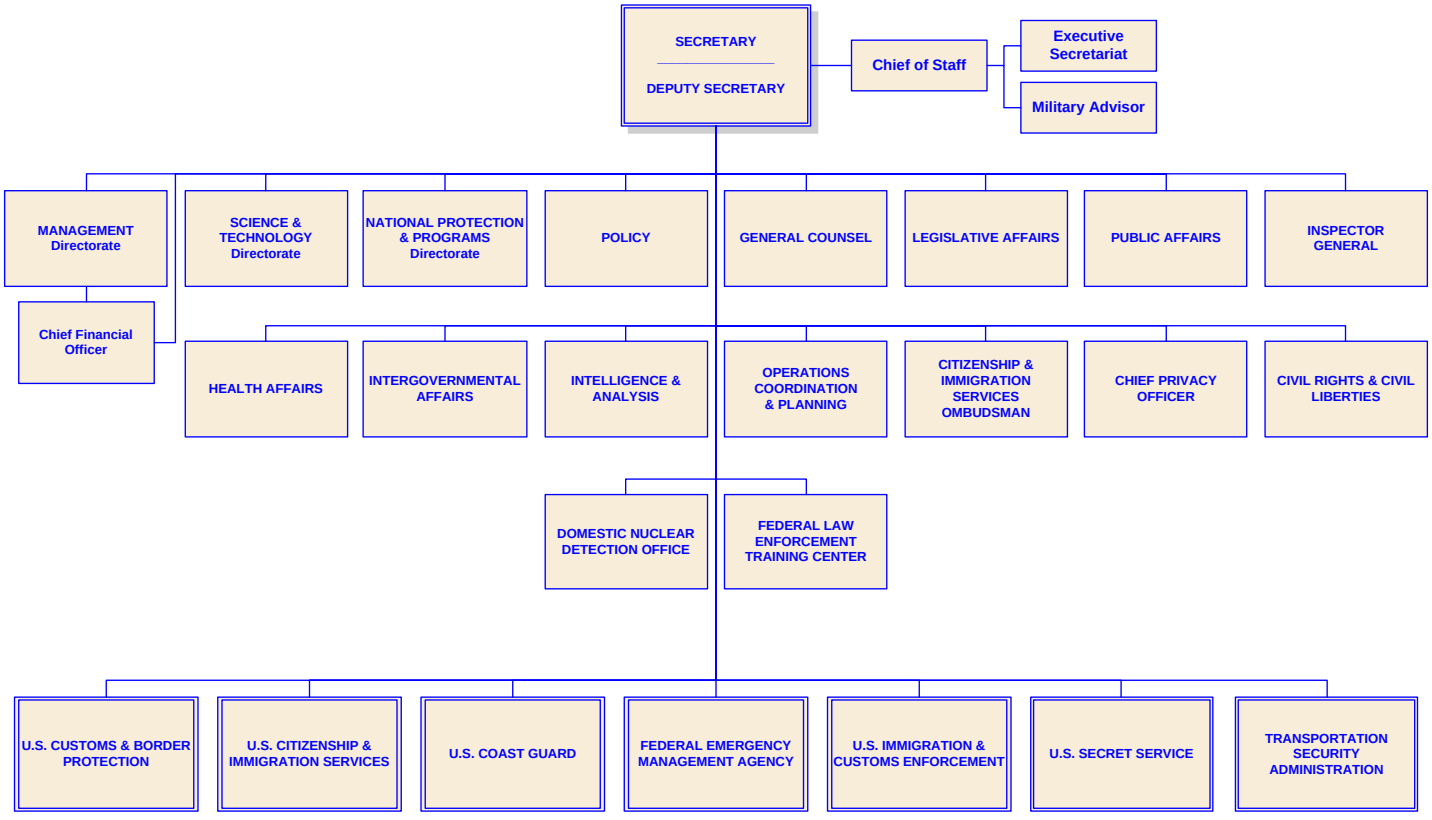
Mission

We will lead efforts to achieve a safe, secure, and resilient homeland. We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure resilience from disasters. We will accomplish these missions while providing essential support to national and economic security and maturing and strengthening both the Department of Homeland Security and the homeland security enterprise.

Our Organization

DHS's seven operational Components, listed along the bottom of the chart below, lead the Department's front-line activities to protect our Nation. The remaining DHS Components of the provide resources, analysis, equipment, research, policy development, and support to ensure the front-line organizations have the tools and resources to accomplish the DHS mission. For more information about the Department's structure, visit our website at http://www.dhs.gov/organization.

DHS Organizational Chart



Strategic Plan Summary

The *U.S. Department of Homeland Security Strategic Plan for Fiscal Years (FY) 2012-2016* presents the Department's missions, goals, and objectives. The plan was published on February 13, 2012 and can be accessed at http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf. The Strategic Plan continues the Department's efforts to prioritize front-line operations while maximizing the effectiveness and efficiency of every taxpayer dollar the Department receives. The Plan was developed from the deliberations and conclusions of the Quadrennial Homeland Security Review (QHSR) and describes the homeland security missions and the Department's efforts to provide essential support to national and economic security and to mature and strengthen DHS. The missions and goals of the Department are provided below.

Mission 1: Preventing Terrorism and Enhancing Security

Protecting the United States from terrorism is the cornerstone of homeland security. DHS's 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.

Goal 1.1: Preventing Terrorist Attacks – Prevent malicious actors from conducting terrorist attacks within or against the United States.

Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear (CBRN) Materials and Capabilities – Prevent malicious actors from acquiring or moving dangerous chemical, biological, radiological, and nuclear materials or capabilities within the United States.

Goal 1.3: Manage Risks to Critical Infrastructure, Key Leaders, and Events – Reduce the vulnerability of key sectors to attack or disruption.

Mission 2: 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.

Goal 2.1: Secure U.S. Air, Land, and Sea Borders – Prevent the illegal flow of people and goods across U.S. air, land, and sea borders.

Goal 2.2: Safeguard Lawful Trade and Travel – Facilitate and secure lawful trade and travel.

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations – Disrupt and dismantle transnational organizations that engage in smuggling and trafficking across the U.S. border.

Mission 3: Enforcing and Administering Our Immigration Laws

DHS is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. The Department has fundamentally reformed immigration enforcement, focusing on identifying and removing criminal aliens who pose a threat to public safety and targeting employers who knowingly and repeatedly break the law.

Goal 3.1: Strengthen and Effectively Administer the Immigration System – Promote lawful immigration, facilitate administration of immigration services, and promote the integration of lawful immigrants into American society while guarding against fraud and abuse of the immigration system.

Goal 3.2: Prevent Unlawful Immigration – Reduce conditions that encourage foreign nationals to illegally enter and remain in the United States, while identifying and removing those who violate our laws.

Mission 4: Safeguarding and Securing Cyberspace

DHS is responsible for protecting the federal Executive Branch civilian agencies and while working collaboratively with the private sector to protect 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.

Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment – Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure.

Goal 4.2: Promote Cybersecurity Knowledge and Innovation – Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.

Mission 5: Ensuring Resilience to Disasters

DHS coordinates the 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, federal, state local, tribal, and territorial partners to ensure a swift and effective recovery. 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 among the emergency management team; building plans and providing training to our homeland security partners; and promoting preparedness within the private sector.

Goal 5.1: Mitigate Hazards – Strengthen capacity at all levels of society to withstand threats and hazards.

Goal 5.2: Enhance National Preparedness through a Whole Community Approach to Emergency Management – Engage all levels and segments of society in improving preparedness.

Goal 5.3: Ensure Effective Emergency Response – Strengthen nationwide response capacity to stabilize and recover from a catastrophic event.

Goal 5.4: Rapidly Recover from a Catastrophic Event – Improve the Nation's ability to adapt and rapidly recover.

In addition to the core missions of the Department described above, DHS provides focus in two areas: 1) providing essential support to national and economic security; and, 2) maturing and strengthening DHS.

Providing Essential Support to National and Economic 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.

Goal: Collect Customs Revenue and Enforce Import/Export Controls – Maximize the collection of customs revenue and protect U.S. intellectual property rights and workplace standards.

Goal: Ensure Maritime Safety and Environmental Stewardship – Prevent loss of life in the maritime environment, maintain the marine transportation system, and protect and preserve the maritime environment.

Goal: Conduct and Support Other Law Enforcement Activities – Prevent the exploitation of individuals and provide law enforcement training for the execution of other non-DHS federal laws and missions.

Goal: Provide Specialized National Defense Capabilities – Support national defense missions and post-conflict reconstruction and stabilization.

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, territorial, non-governmental, 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 improve Department management and accountability.

Goal: Improve Cross-departmental Management, Policy, and Functional Integration – Transform and increase the integration of departmental management.

Goal: Enhance DHS Workforce – Continue to build human resource programs that support departmental mission goals and objectives, create high technical proficiency, and address the needs of the Department's employees in executing DHS missions.

Goal: Enhance Intelligence, Information Sharing, and Integrated Operations – Institute optimal mechanisms to integrate the Department's intelligence elements, increase operational capability, and harmonize operations.

Performance Overview

The performance overview provides a summary of each homeland security mission and focus area, selected accomplishments, key performance measures, and future initiatives to strengthen the Department's efforts in achieving a safer and more secure Nation. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS FY 2012-2014 Annual Performance Report in February 2013.

Preventing Terrorism and Enhancing Security

Preventing a terrorist attack in the United States remains the cornerstone of homeland security. Our vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve our freedom and prosperity. Achieving this vision requires us to focus on the core goal of preventing terrorist attacks, highlighting the challenges of preventing attacks using chemical, biological, radiological, and nuclear (CBRN) weapons and managing risks to critical infrastructure.

We will achieve this mission through meeting the following goals:

- **Preventing Terrorist Attacks –** Prevent malicious actors from conducting terrorist attacks within or against the United States.
- **Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities –** Prevent malicious actors from acquiring or moving dangerous chemical, biological, radiological, and nuclear materials or capabilities within the United States.
- **Manage Risks to Critical Infrastructure, Key Leaders, and Events –** Reduce the vulnerability of key sectors to attack or disruption.

TSA Pre✓™

The Transportation Security Administration (TSA) employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. TSA Pre✓™ is a pre-screening initiative that allows eligible passengers to volunteer information about themselves to possibly expedite their screening experience. Eligible passengers enter a separate security lane, and may pass through metal detectors without needing to remove shoes, light outerwear, belts, or remove laptops and 3-1-1 compliant liquids/gels from their carry-on.

Currently, eligible passengers include U.S. citizens flying on participating airlines as well as those who are members of U.S. Customs and Border Protection (CBP) Trusted Traveler programs, including Global Entry, SENTRI, and NEXUS. Beginning November 15, 2012, Canadian citizens traveling domestically in the United States who are members of NEXUS are also qualified to participate in TSA Pre✓™. TSA will always incorporate random and unpredictable security measures throughout the airport and no individual will be guaranteed expedited screening.

More than three million passengers have received expedited screening through TSA Pre✓™ security lanes since the initiative began in October 2011. TSA Pre✓™ will be available at 35 of the Nation's busiest airports by the end of 2012.

Below are highlighted performance measures related to *Preventing Terrorism and Enhancing Security*.

- **Percent of international air enplanements vetted against the terrorist watch list through Secure Flight:** TSA vets international air travelers against the terrorist watch list through the Secure Flight Program, continuing to achieve 100 percent screening in FY 2012. Secure Flight increases the security of air travel by screening every passenger against the latest intelligence before a boarding pass is issued.
- **Percent of overall compliance of domestic airports with established aviation security indicators:** Through the use of rigorous compliance inspections, TSA identifies air carrier compliance for U.S. flagged aircraft operating domestically with established security indicators. In FY 2012, TSA identified that 94.5 percent of domestic airports comply with established security indicators. Compliance rates will fluctuate as new aviation security requirements are implemented. In addition, corrective actions were issued to noncompliant airports to remedy any deficiencies.
- **Percent of air cargo screened on commercial passenger flights originating from the United States and territories:** TSA ensures the security of air cargo while facilitating the flow of legitimate commerce. In FY 2012—for the second year in a row—TSA screened 100 percent of cargo on commercial passenger flights originating from the United States and territories, up from 50 percent in FY 2009.
- **Percent of total U.S. Secret Service protection activities that are incident-free for protection of national leaders, foreign dignitaries, designated protectees and others during travel or at protected facilities:** The U.S. Secret Service (USSS) continues to meet its goal of 100 percent incident-free protection for our Nation's leaders, foreign dignitaries, and others during travel or while at protected facilities.

2012 NATO Summit Protection

The 2012 North Atlantic Treaty Organization (NATO) Summit—held in Chicago, Illinois in May 2012—was the largest gathering of world leaders on U.S. soil, outside of the United Nations General Assembly in New York City and was designated as a National Security Special Event (NSSE). When an NSSE is declared, the U.S. Secret Service becomes the lead agency for developing and executing a comprehensive operational security plan in coordination with Federal and local law enforcement partners, state and local governments, and the military.

In addition to securing nine different venues for 60 visiting delegations, the U.S. Secret Service provided protective details for 42 visiting heads of state or government in addition to the President. In total, more than 50 federal, state, local, and military agencies participated in the planning and execution of the security plan.

Future Initiatives

Protecting the United States from terrorism is the cornerstone of homeland security. DHS's counterterrorism responsibilities focus on three goals: preventing terrorist attacks; preventing the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and

nuclear materials and capabilities within the United States; and reducing the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards.

Below are a few initiatives that advance our efforts to achieve the Department's counterterrorism goals:

- Continue TSA's risk-based security initiative through a layered security approach that includes state-of-the-art technologies, better passenger identification techniques, trusted traveler programs like TSA Pre✓™ and other measures both seen and unseen.
- Continue efforts to secure the global supply chain through a layered detection system that interdicts dangerous goods and dangerous people at the earliest point possible. DHS's intelligence and targeting programs support a flexible enforcement capability that detects potential threats to our security, economy, and public safety, and shares intelligence with law enforcement agencies. Recent advances in technology and modeling, coupled with the expansion of the National Targeting Center, will increase operational efficiencies and enhance our ability to interdict potential terrorists, high-risk cargo, and other threats before they reach the United States.
- Continue efforts with respect to threats of nuclear and high-consequence biological attack, consistent with the *National Security Strategy*, while maintaining robust programs for prevention, interdiction, detection, and disruption of chemical and radiological attacks. Continue efforts to prevent and protect against radiological and nuclear terrorism through execution of the *National Strategic Five-Year Plan for Improving the Nuclear Forensics and Attribution Capabilities of the United States, Global Nuclear Detection Architecture Strategic Plan 2010,* and associated implementation plans.
- Continue to implement a multi-hazard approach to critical infrastructure protection and resilience through the deployment of Infrastructure Protective Security Advisors to state and local fusion centers, conducting inspections of high-risk chemical facilities, and outreach to critical infrastructure stakeholders.

Securing and Managing Our Borders

A safe and secure homeland requires that we secure our air, land, and sea borders and disrupt and dismantle transnational criminal and terrorist organizations while facilitating lawful travel and trade.

We will achieve this mission through meeting the following goals:

- **Secure U.S. Air, Land, and Sea Borders –** Prevent the illegal flow of people and goods across U.S. air, land, and sea borders.
- **Safeguard Lawful Trade and Travel –** Facilitate and secure lawful trade and travel.
- **Disrupt and Dismantle Transnational Criminal Organizations –** Disrupt and dismantle transnational organizations that engage in smuggling and trafficking across the U.S. border.

Southwest Border Security

Under this Administration, DHS has dedicated historic levels of personnel, technology, and resources to the Southwest Border. Today, the Border Patrol is staffed at higher levels on the Southwest Border than at any time in its 88-year history, having more than doubled the number of agents from approximately 9,100 in 2001 to more than 18,500 today. Under the Southwest Border Initiative, DHS has doubled the number of personnel assigned to Border Enforcement Security Task Forces; increased the number of intelligence analysts focused on cartel violence; tripled deployments of Border Liaison Officers to work with their Mexican counterparts; increased screening of southbound shipments for illegal weapons, drugs, and cash; and expanded unmanned aircraft system coverage to the entire Southwest Border.

Along the Southwest Border, DHS has deployed thousands of technology assets, including mobile surveillance units, thermal-imaging systems, large- and small-scale non-intrusive inspection equipment, and three Unmanned Aircraft Systems. For the first time, DHS unmanned aerial capabilities now cover the Southwest Border from California to Texas—providing critical aerial surveillance assistance to personnel on the ground. Attempts to cross the Southwest Border illegally, as measured by Border Patrol apprehensions, have decreased 49 percent in the past four years and are 78 percent less than what they were at their peak.

Below are highlighted performance measures related to *Securing and Managing Our Borders*.

1. **Percent of people apprehended multiple times along the Southwest Border:** The number of individuals attempting illegal entry across the Southwest Border multiple times has decreased. In FY2012, the percent of individuals who were apprehended multiple times for illegal entry has decreased to 17 percent, meeting our target of less than 19 percent.
2. **Percent of detected conventional aircraft incursions resolved along all borders of the United States:** CBP's Air and Marine Operations Center uses its capabilities, as well as those of the Department of Defense and civilian radar, to identify and track suspect aircraft incursions along our borders. In FY 2012, CBP successfully resolved 96 percent of confirmed border incursions, up from 95 percent in FY 2011.
3. **Percent of imports compliant with U.S. trade laws:** Annually, CBP conducts an extensive and thorough analysis of import compliance with U.S. trade laws. Due to CBP's risk-based targeting approach, CBP continues to experience high compliance rates achieving 96.5 percent import compliance in FY 2012.
4. **Security compliance rate for high-risk maritime facilities:** As part of its border security mission, the U.S. Coast Guard conducts routine and unannounced examinations of Maritime Transportation Security Act regulated facilities. In FY 2012, 98.7 percent of these examinations were found to be in compliance. Corrective actions were issued to noncompliant facilities to remedy the deficiencies.

Facilitating Legal Trade and Travel

Active Lane Management: CBP is leveraging its Trusted Traveler Programs and the growing prevalence of radio frequency identification travel documents to initiate the "active lane management" concept at our land border ports of entry (POEs). Active Lane Management involves monitoring and making adjustments to a POE's lane designations as traffic conditions and infrastructure limitations warrant expediting traffic and enhancing security. Ready Lanes, Dedicated Commuter Lanes, and Light Emitting Diode signage are established best practices being deployed so Port Directors can re-designate lanes and communicate to the public in order to expedite both trusted and "ready" traffic.

Business Transformation at Ports of Entry: In order to strengthen security and expedite legal travel and trade at POEs, CBP is engaged in a series of business transformation initiatives. These initiatives involve reassessing core processes, incorporating technology enhancements, assessing utilization of law enforcement staffing, and developing automation efforts. Efficiencies and new technologies that have already been implemented, such as the Western Hemisphere Travel Initiative, Radio Frequency Identification enabled documents, License Plate Readers, Trusted Traveler Programs, and Non-Intrusive Inspection equipment are saving CBP hundreds of millions of dollars and creating a workforce multiple of several thousand positions.

Future Initiatives

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

Below are a few initiatives that advance our efforts to achieve the Department's border security goals:

- Continue the Administration's robust border security efforts, while facilitating legitimate travel and trade through the sustainment of historic deployments of personnel along U.S. borders.
- Continue interdiction efforts at U.S. POEs through outbound vehicle and passenger processing, counter-surveillance, and perimeter enforcement to respond to evolving threats.
- Continue modifications, improvements, and maintenance to land, sea, and air POEs. This infrastructure facilitates nearly $150 billion in economic activity and expedites travel for more than 340 million international visitors per year.
- Enhance the Automated Commercial Environment system to eliminate unnecessary paperwork and enable electronic processing of manifests, entry forms, and other documentation to expedite trade and travel. Over time, this system will provide a single window for CBP to interact, manage, and oversee import and export data, custodial revenue management, and enforcement systems to provide end-to-end visibility of the entire trade cycle.

Enforcing and Administering Our Immigration Laws

A fair and effective immigration system enriches American society, unifies families, and promotes our security. Our Nation's immigration policy plays a critical role in advancing homeland security.

We will achieve this mission through meeting the following goals:

- **Strengthen and Effectively Administer the Immigration System –** Promote lawful immigration, facilitate administration of immigration services, and promote the integration of lawful immigrants into American society while guarding against fraud and abuse of the immigration system.
- **Prevent Unlawful Immigration –** Reduce conditions that encourage foreign nationals to illegally enter and remain in the United States, while identifying and removing those who violate our laws.

USCIS's Electronic Immigration Application System

In 2012, U.S. Citizenship and Immigration Services (USCIS) launched the first two phases of its electronic immigration application system, known as USCIS ELIS. The system has been created to modernize the process for filing and adjudicating immigration benefits.

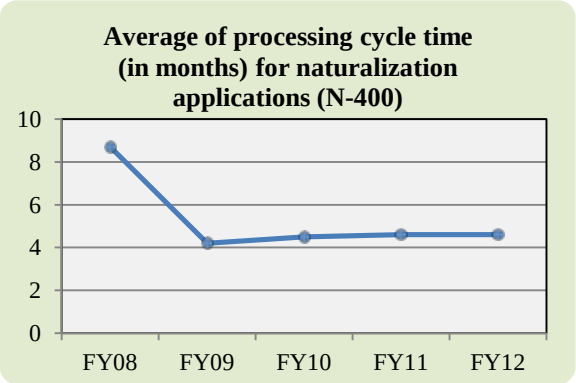
Historically, USCIS customers have had to apply for most benefits by mail and USCIS employees then review paper files and ship documents between offices to complete their adjudication. Under ELIS, eligible individuals can establish an account and apply online to extend or change their nonimmigrant status for certain visa types. ELIS also enables USCIS officers to review and adjudicate online filings from multiple agency locations across the country.

Benefits of using ELIS include filing applications and paying fees online, faster average processing times, and the ability to update user profiles, receive notices, and respond to requests electronically. The system also includes enhanced tools to combat fraud and identify national security concerns. As of September 30, 2012, 4,679 primary applications have been initiated online through ELIS.

Since the launch of ELIS in May 2012, the ELIS Customer Satisfaction Surveys show overwhelmingly positive results with 90.3 percent of respondents reporting a positive overall experience with ELIS and 94 percent of respondents would recommend ELIS to another USCIS applicant.

Below are highlighted performance measures related to *Enforcing and Administering Our Immigration Laws*.

- **Average of processing cycle time (in months) for naturalization applications (N-400):** An N-400, Application for Naturalization, is filed by an individual applying to become a United States citizen. USCIS has implemented several improvement programs to quickly and effectively adjudicate naturalization requests and have consistently achieved their target of processing naturalization applications in less than five



months on average. In FY 2012, USCIS met their target of less than five months for the fourth year in a row achieving an average processing time of 4.6 months.

- **Overall customer service rating of the immigration process:** This measure gauges the overall satisfaction of the immigration process and is based on the results from the following areas: accuracy of information; responsiveness to customer inquiries; accessibility to information; and customer satisfaction. In FY 2012, USCIS achieved an overall customer service rating of 93 percent, up from 80 percent in FY 2011.
- **Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days):** This measure assesses the length of time convicted criminal aliens are detained in one of U.S. Immigration and Customs Enforcement's (ICE) detention facilities while awaiting a final order of removal. In FY 2012 the average length of stay in detention of all convicted criminal aliens prior to removal was 31.9 days, meeting the target of less than 35 days and down 13.8 percent from 37 days in FY 2010.

Future Initiatives

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.

Below are a few initiatives that advance our efforts to achieve the Department's immigration enforcement and administration goals:

- Deploy additional near-term functionality for use in USCIS ELIS to include improved user account access and electronic signature of benefit request forms. In addition, new functionality will provide USCIS adjudicators improved decision notification options, risk data, and reporting capabilities.
- Continue our focus on monitoring and compliance, promoting adherence to worksite-related laws, Form I-9 inspections, and expansion of the E-Verify program.
- Bolster USCIS's effort to support immigrant integration efforts, including programs supporting English language acquisition and citizenship education.
- Support initiatives that focus finite resources on criminal aliens and other high priority cases.
- Implement Secure Communities nationwide in FY 2013, and in collaboration with the U.S. Department of Justice (DOJ), focus resources on the detained docket to increase the identification and removal of criminal aliens and other priority individuals. ICE is working with DHS's Office for Civil Rights and Civil Liberties and the DOJ on an oversight and evaluation process for Secure Communities, which includes additional training to state and local law enforcement.

Safeguarding and Securing Cyberspace

Our economic vitality and national security depend on a vast array of interdependent and critical cyber networks, systems, services, and resources. By statute and Presidential Directive, DHS is the lead for the Federal Government to secure civilian government computer systems; working with industry to defend privately owned and operated critical infrastructure; and, working with state, local, tribal, and territorial governments to secure their information systems.
We will achieve this mission through the following goals:

- **Create a Safe, Secure, and Resilient Cyber Environment –** Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure.
- **Promote Cybersecurity Knowledge and Innovation –** Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.

Cyber Workforce Initiative

DHS is focused on building the next generation of cyber security professionals to support the Department's work today and in the future. In June 2012, Secretary Napolitano announced a new initiative through the Homeland Security Advisory Council, in conjunction with public and private sector partners, to develop an agile cyber workforce across the Federal Government. Since its creation, the Department has increased its cybersecurity workforce by more than 600 percent while working with universities to develop and attract talent through competitive scholarships, fellowships, and internship programs.

Below are highlighted performance measures related to *Safeguarding and Securing Cyberspace*.

- **Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies:** This measure assesses DHS's increased vigilance in identifying malicious activity across Federal Executive Branch civilian agency networks. DHS operators monitor these networks using EINSTEIN intrusion detection system sensors, which are deployed to Trusted Internet Connection locations that minimize agencies' external gateways to the network. In FY 2012, 73 percent of Federal Executive Branch civilian network traffic was monitored for cyber intrusion using advanced technology, exceeding the target of 55 percent. DHS plans to have full operating capability by FY 2015.
- **Average amount of time required for initial response to a request for assistance from public and private sector partners to prevent or respond to major cyber incidents (in minutes):** Through the implementation of targeted process improvements and the adoption of agile incident response standard operating procedures, DHS responded on average within 14.1 minutes to major cyber incidents. This was a more than two hour improvement over the FY 2011 results of 138 minutes, meeting the target of less than 90 minutes.
- **Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace:** This measure gauges the extent to

which the DHS Intelligence Enterprise is satisfying their customers' needs related to understanding the threats as they relate to cybersecurity. The DHS Intelligence Enterprise actively seeks out and identifies cyber threats, and once found, communicates this information to those who can take action to assess, manage, and resolve the threat. In FY 2012 the DHS Intelligence Enterprise obtained an 88 percent rating of satisfactory or higher, exceeding their target of 80 percent.

Industrial Control Systems Cyber Emergency Response Team

DHS provides key analysis and assistance through its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to protect the industrial control systems that help operate the U.S. power grid, manufacturing systems and other essential critical infrastructure from dangerous malware and viruses that may cause damage or destroy key resources.

In early December 2011, ICS-CERT responded to a cybersecurity incident affecting a rail company. The initial report indicated that the rail company was experiencing a cyber attack to its secondary communications equipment. ICS-CERT, working in coordination with asset owners, analyzed various data and determined that the incident was not the result of a targeted attack. In this case, the rail company quickly implemented effective measures to maintain the safety of its operation and worked closely with ICS-CERT to understand the incident and take appropriate mitigation measures.

In addition, DHS's ICS-CERT has been working since March 2012 with critical infrastructure owners and operators in the oil and natural gas sector to address a series of cyber intrusions targeting natural gas pipeline companies. In conjunction with the FBI and other federal agencies, ICS-CERT is working with affected organizations to prepare mitigation plans customized to their current network and security configurations to detect, mitigate, and prevent such threats.

Future Initiatives

Below are a few initiatives that advance our efforts to achieve the Department's cybersecurity goals:

- Support the acceleration of the National Cybersecurity Protection System's prevention capability (E^3A) on civilian government computer systems to prevent and detect intrusions.
- Continue to provide high-quality, cost-effective virtual cybersecurity education and training to develop and grow a robust cybersecurity workforce that is able to protect against and respond to national cybersecurity threats and hazards.
- Increase outreach to Critical Infrastructure and Key Resource owners and improve control systems cybersecurity awareness, incident response, coordination, and information sharing.
- Enhance information sharing processes with critical infrastructure owners and operators to create shared situational awareness of cyber threats across sectors and facilitate collaborative incident response though the National Cybersecurity and Communications Integration Center.

- Build on the National Cyber Incident Response Plan, which enables DHS to coordinate the response of multiple federal agencies, state and local governments, international partners, and private industry to incidents at all levels.

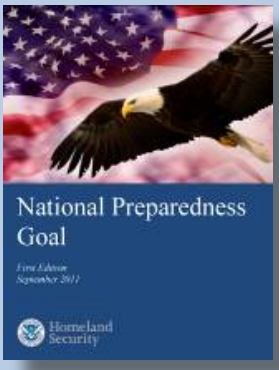
Ensuring Resilience to Disasters

Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as attacks, may occur. The challenge is to build the capacity of American communities to be resilient in the face of disasters and other threats. Our vision of a resilient Nation is one with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

We will achieve this mission through meeting the following goals:

- **Mitigate Hazards –** Strengthen capacity at all levels of society to withstand threats and hazards.
- **Enhance National Preparedness through a Whole Community Approach to Emergency Management –** Engage all levels and segments of society in improving preparedness.
- **Ensure Effective Emergency Response –** Strengthen nationwide response capacity to stabilize and recover from a catastrophic event.
- **Rapidly Recover from a Catastrophic Event –** Improve the Nation's ability to adapt and rapidly recover.

National Preparedness Goal



In October 2011, DHS announced the release of the country's first-ever National Preparedness Goal. The goal is the first deliverable required under Presidential Policy Directive (PPD) 8: National Preparedness. The goal sets the vision for nationwide preparedness and identifies the core capabilities and targets necessary to achieve preparedness across five mission areas laid out under PPD 8—prevention, protection, mitigation, response, and recovery.

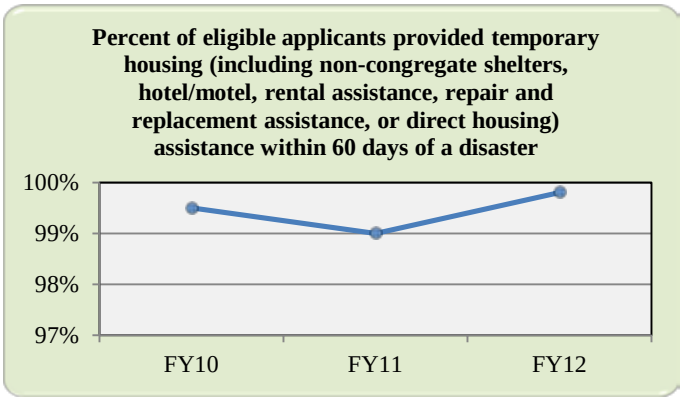
In March 2012, the National Preparedness Report (NPR) was released which focuses on the five mission areas outlined in the National Preparedness Goal. Within these mission areas are 31 core capabilities central to preparedness. The NPR assesses each core capability and identifies areas where the Nation has made significant progress, opportunities for improvement and reinforces the core principles of national preparedness. Areas of national strength identified in the NPR include planning, operational coordination, intelligence and information sharing, and other response-related capabilities.

The NPR is part of a series of deliverables required under PPD 8 aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters.

Below are highlighted performance measures related to *Ensuring Resilience to Disasters*.

- **Percent of time that critical communications for response operations are established within 12 hours:** This measure reflects the percent of time that critical communications are established for the Federal Emergency Management Agency's (FEMA) on-site emergency responders within 12 hours of the deployment of Mobile Emergency Response Support. FEMA met its target of 100 percent in establishing critical communications for response operations within 12 hours in FY 2012.

- **Percent of eligible applicants provided temporary housing (including non-congregate shelters, hotel/motel, rental assistance, repair and replacement assistance, or direct housing) assistance within 60 days of a disaster**: State and local governments and FEMA's Emergency Support Function-6 partners provide emergency sheltering for those in need during the initial stages of a declared emergency. Once the emergency is contained and FEMA supports the community in beginning full recovery efforts, individuals may receive temporary housing assistance which includes transitional sheltering assistance (hotel/motel), rental assistance, repair and replacement assistance, or direct housing (temporary housing units). In FY 2012, FEMA placed eligible applicants in temporary housing within 60 days 99.8 percent of the time, exceeding their target of 97 percent.



- **Reduction in the potential cost of natural disasters to communities and their citizens:** FEMA uses a risk-based strategic approach to deploy mitigation grants, conduct outreach, and provide technical assistance to support state and local initiatives that result in safer communities by reducing the loss of life and property. Through the deployment of mitigation initiatives, long-term costs are avoided. In FY 2012, it is estimated that a reduction of $3.12 billion dollars in the potential cost of natural disasters to communities and their citizens was avoided, exceeding the target of $2.4 billion.

- **Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected:** The ability of our National Security and Emergency Preparedness personnel to communicate effectively during emergency situations is vital. The call completion rate is the percent of calls that a national security/emergency preparedness user successfully completes via public telephone network to communicate with the intended user, location, or system, during an emergency situation. In FY 2012, the call completion rate was 99.4 percent, meeting our annual target and up from the FY 2011 result of 97.8 percent.

Hurricane Isaac Response and Recovery Efforts

On the evening of August 28, 2012, Hurricane Isaac made landfall along the coast of Louisiana and continued to impact Gulf Coast communities for days thereafter. Within hours, both Louisiana and Mississippi received Presidential disaster declarations allowing federal assistance to flow into those states. FEMA and other federal agencies deployed prior to the storm and located in states all along the Gulf Coast to prepare for and be ready to respond to the damages of Isaac. Supply centers in the anticipated impact areas were stocked with supplies including large and small generators in expectation of widespread power outages.

Hurricane Isaac demonstrated the value of mitigation projects put in place following Hurricane Katrina allowing communities along the Gulf Coast to successfully respond to and recover from Isaac's impact.

Future Initiatives

DHS provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster, or other large-scale emergency while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include bolstering information sharing and providing grants, plans, and training to our homeland security and law enforcement partners. To be successful, DHS must foster a national approach to disaster management built upon a foundation of proactive engagement at the community level that builds community resilience and supports local emergency management needs.

Below are a few initiatives that advance our efforts to achieve our resilience goals:

- Continue to build the core capabilities of state and local law enforcement and emergency management communities, providing the tools needed to respond to evolving threats through grants, training, fusion centers, and intelligence analysis and information sharing.
- Support the proposed National Preparedness Grants Program to create a robust national preparedness capability. DHS will leverage a comprehensive process to assess regional and national capability gaps, identify and prioritize cross jurisdictional and readily deployable capabilities, and require grantees to regularly report progress in the acquisition and development of these capabilities.
- Using the results from the National Preparedness Report, FEMA will work with Whole Community partners to leverage grants, training, and technical assistance to bolster the 31 core capabilities central to preparedness.

Providing Essential Support to National and Economic 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:

- **Collect Customs Revenue and Enforce Import/Export Controls –** Maximize the collection of customs revenue and protect U.S. intellectual property rights and workplace standards.
- **Ensure Maritime Safety and Environmental Stewardship –** Prevent loss of life in the maritime environment, maintain the marine transportation system, and protect and preserve the maritime environment.
- **Conduct and Support Other Law Enforcement Activities –** Prevent the exploitation of individuals and provide law enforcement training for the execution of other non-DHS federal laws and missions.
- **Provide Specialized National Defense Capabilities –** Support national defense mission and post-conflict reconstruction and stabilization.

Below are highlighted performance measures related to *Providing Essential Support to National and Economic Security*.

- **Percent of revenue successfully collected:** This measure estimates the collected duties expressed as a percent of the all collectable revenue due from commercial imports to the United States directed by trade laws, regulations, and agreements. In FY 2012, 98.9 percent (estimated) of collectable revenue was collected.
- **Five-year average number of commercial and recreational boating deaths and injuries:** This measure reports the sum of the five-year average numbers of reportable commercial mariner, commercial passenger, and recreational boating deaths and injuries and is a long-term trend indicator of the U.S. Coast Guard Maritime Prevention Program's impact on marine safety. In FY 2012, there were 4,473 commercial and recreational boating deaths and injuries, a decrease from FY 2011 and meeting the five-year average target of fewer than 4,642.
- **Availability of maritime navigation aids:** This measure indicates the hours that short-range federal aids-to-navigation are available. There are about 50,000 short range aids-to-navigation throughout the United States to support improved safety and navigability on our open waters. The U.S. Coast Guard has a long history of maintaining these navigational aids and consistently achieves its target of 97.5 percent availability. In FY 2012 the availability of maritime navigations aids was 98.3 percent, exceeding the target.
- **Number of Federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation**

process: This performance measure reflects the cumulative number of federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation (FLETA) process. Accreditation ensures that training and services provided meet professional training standards for law enforcement and re-accreditation is conducted every three years to remain current. The cumulative results through FY 2012 of 83 accreditations or re-accreditations exceeded FLETA's target of 74.

Future Initiatives

Below are a few initiatives that advance our efforts to achieve our national and economic security goals:

- Continue the U.S. Coast Guard's recapitalization of cutters; boats; aircraft; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems; and infrastructure to improve the security of the maritime environment, and to improve mission readiness and response capability. Through a balanced approach, limited resources will be effectively deployed to support operations and mission execution.
- Leverage a new operational partnership between ICE and USSS through the Electronic Crimes and Financial Crimes Task Forces to enhance national security, target large-scale producers of child pornography, and prevent attacks against critical U.S. infrastructure.
- Continue to target the gap in lost revenue from commercial imports through the use of various enforcement methods such as audits, targeting, and statistical random sampling to bridge revenue gap and identify non-compliance with U.S. trade laws, regulations and agreements.

Maturing and Strengthening DHS

The strategic aims and objectives for maturing and strengthening DHS are drawn from the common themes that emerge from each of the mission areas. Ensuring a shared awareness and understanding of risks and threats, building capable communities, creating unity of effort, and enhancing the use of science and technology underpin our national efforts to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters.

We will continue to make progress in maturing and strengthening DHS by focusing on the following goals:

- **Improve Cross-Departmental Management, Policy, and Functional Integration –** Transform and increase the integration of departmental management.
- **Enhance DHS Workforce –** Continue to build human resource programs that support departmental mission goals and objectives, create high technical proficiency, and address the needs of the Department's employees in executing DHS missions.

- **Enhance Intelligence, Information Sharing, and Integrated Operations –** Institute optimal mechanisms to integrate the Department's intelligence elements, increase operational capability, and harmonize operations.

Future Initiatives

Below are a few initiatives that advance our efforts to achieve our maturing and strengthening goals:

- Improve the Department's comprehensive and strategic approach to strengthen the homeland security enterprise by increasing unification and integration, addressing challenges raised by GAO, and building upon the management reforms that have been implemented under this Administration.
- Using a phased approach, modernize the financial systems within DHS to provide integrated financial management services.
- Execute the Balanced Workforce Strategy, which is designed to ensure the Department has the appropriate mix of federal employees and contractors to fulfill our mission in a manner that is cost-effective and ensures appropriate federal oversight.
- Improve the Department's acquisition workforce capacity—including additional systems engineers, program managers, logisticians, and business cost estimators, to ensure operational requirements are properly developed and included in DHS contracts to provide greater oversight and accountability.
- Continue expansion of the Secretary's Department-wide Efficiency Review to maximize the effectiveness and efficiency of limited resources.

Financial Overview

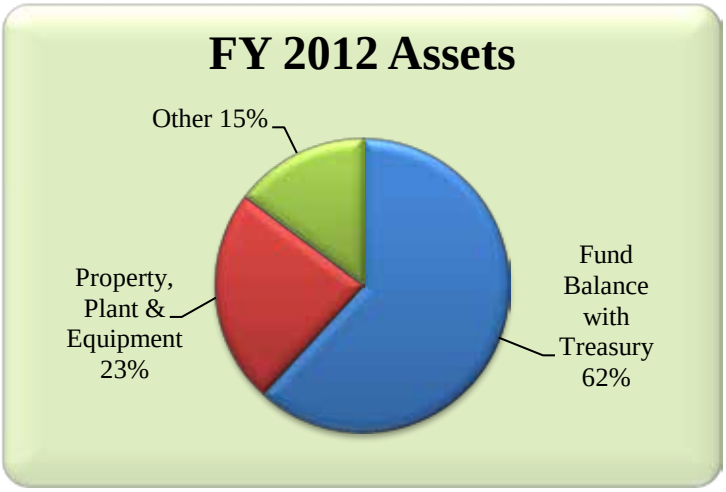
DHS's budgetary resources were approximately $79.5 billion for FY 2012, approximately $1 billion more than in FY 2011. The budget represents our plan for efficiently and effectively achieving the strategic objectives set forth by the Secretary to carry out our mission and to ensure that DHS manages its operations within the appropriated amounts using budgetary controls. DHS prepares its annual financial statements on an accrual basis, in accordance with generally accepted accounting principles, meaning that economic events are recorded as they occur, regardless of when cash is received or disbursed. These financial statements provide the results of our operations and financial position, including long-term commitments and obligations. DHS primarily uses the cash basis for its budgetary accounting. The cash basis is an accounting method in which income is recorded when cash is received and expenses are recorded when cash is paid out. The audit of the Department's principal financial statements was performed by KPMG LLP.

Balance Sheet

The Balance Sheet presents the resources owned or managed by DHS that have future economic benefits (assets) and the amounts owed by DHS that will require future payments (liabilities). The difference between DHS's assets and liabilities is the residual amount retained by DHS (net position) that is available for future programs and capital investments.

Total Assets

As of September 30 (in Millions)	FY 2012	FY 2011
Fund Balance with Treasury	$ 53,875	$ 55,960
General Property, Plant, and Equipment, Net	20,491	20,037
Other	12,790	10,892
Total Assets	$ 87,156	$ 86,889



Assets – What We Own and Manage
Assets represent amounts owned or managed by DHS that can be used to accomplish its mission. At September 30, 2012, DHS had $87 billion in assets, representing a $267 million increase from FY 2011.

Fund Balance with Treasury (FBwT), the Department's largest asset, comprises 62 percent ($54 billion) of the total assets. Included in FBwT is the remaining balance of DHS's unspent prior-year budgets plus miscellaneous receipts. FBwT decreased by approximately $2 billion from FY 2011 primarily due to FEMA disbursements related to Hurricane Irene and CBP disbursements related to border station construction and lawsuit


U.S. Coast Guard assets account for approximately half of the property, plant, and equipment assets of DHS.

settlements. In addition, funds were available for disbursement for a longer period than in FY 2011 due to the timing of the passage of the FY 2012 appropriations bill

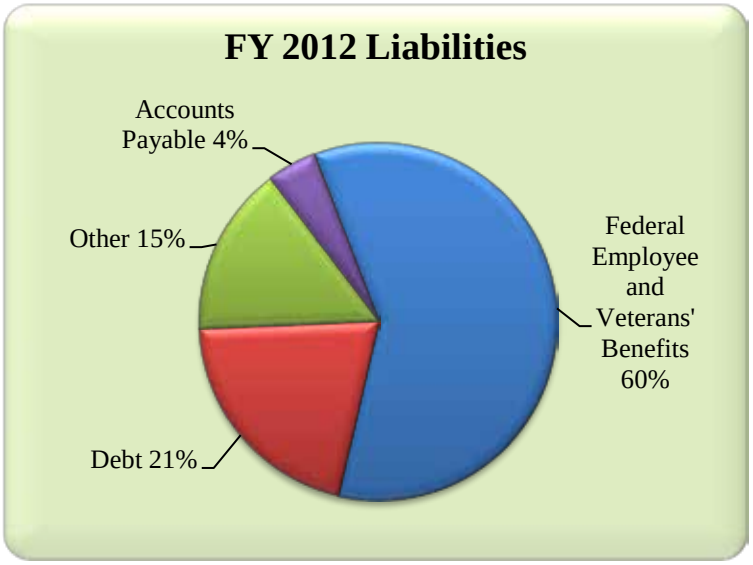
Property, Plant, and Equipment (PP&E) is the second largest asset, comprising 23 percent of total assets. The major items in this category include construction in progress, buildings and facilities, vessels, aircraft, and other equipment. In acquiring these assets, DHS either spent cash or incurred a liability to make payment at a future date; however, because these assets should provide future benefits to help accomplish the DHS mission, DHS reports these items as assets rather than expenses. PP&E is recorded net of accumulated depreciation. Recording the net value of the PP&E items is intended to approximate its remaining useful life. During FY 2012, PP&E increased by approximately $454 million dollars. The increase in FY 2012 is due to CBP's construction of new border stations and land ports of entry, as well as MGMT's purchase of additional equipment for DHS consolidated data centers. Other sources of the increase include the St. Elizabeths construction project; routine upgrades of TSA Explosive Detection X-ray systems; and USCIS' deployment of new software systems over the course of the fiscal year in support of the transition towards an electronic-based adjudication process.

Liabilities – What We Owe

At September 30, 2012, DHS reported approximately $87 billion in total liabilities. Liabilities are the amounts owed to the public or other federal agencies for goods and services provided but not yet paid for; to DHS employees for wages and future benefits; and for other liabilities.

Total Liabilities

As of September 30 (in Millions)	FY 2012	FY 2011
Federal Employee and Veterans' Benefits	$ 51,953	$ 49,664
Debt	18,072	17,754
Other	13,456	15,453
Accounts Payable	3,890	4,598
Total Liabilities	$ 87,371	$ 87,469



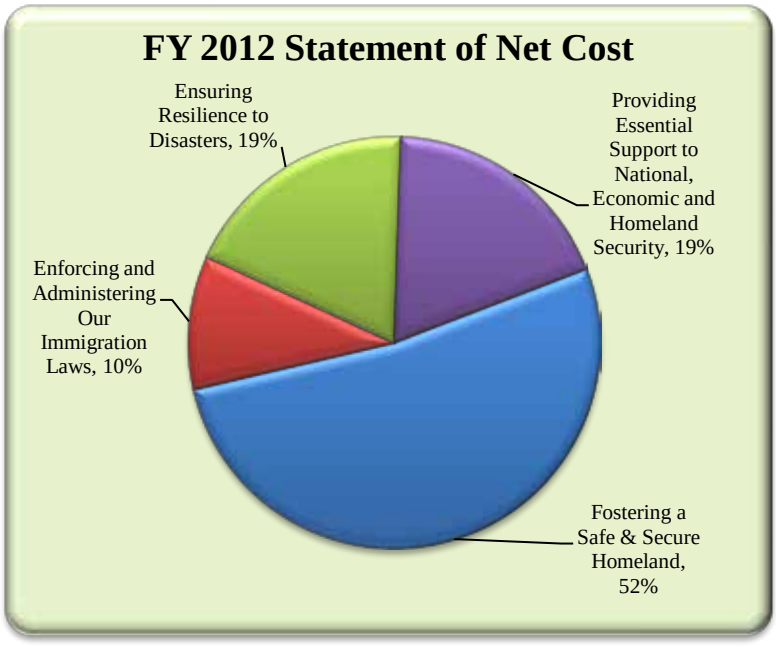
DHS's largest liability is for Federal Employee and Veterans' Benefits, representing 60 percent of total liabilities. This liability increased approximately $2.3 billion from FY 2011. The increase in FY 2012 primarily relates to U.S. Coast Guard changing its discount rate and assumptions used to calculate the Military Retirement and Health System actuarial liabilities. For more information, see Note 16 in the Financial Information Section. DHS owes these amounts to current and past civilian and military personnel for pension and other post-employment benefits. The liability also includes medical costs for approved workers' compensation cases and an estimate for incurred but not yet reported workers' compensation costs. This liability is not covered by current budgetary resources, and DHS will use future appropriations to cover these liabilities (see Note 14 in the Financial Information section).


The National Flood Insurance Program and the Disaster Assistance Direct Loan Program operations of FEMA account for 100 percent of the overall debt of DHS.

Debt is DHS's second-largest liability, representing 21 percent of total liabilities. This debt results from Department of Treasury loans and related interest payable to fund the National Flood Insurance Program (NFIP) and Disaster Assistance Direct Loan Program operations of FEMA. Total debt increased approximately $318 million from FY 2011. Direct Loans increased in FY2012 per OMB's direction to FEMA to reinstate loans that were written off in prior years based on the *Disaster Assistance Recoupment Fairness Act of 2011*. Given the current premium rate structure, FEMA will be unable to pay its debt when due, and legislation will need to be enacted to provide funding to repay the Bureau of Public Debt. This is discussed further in Note 15 in the Financial Information section.

Other liabilities, comprising 15 percent of the Department's liabilities, includes unpaid wages and benefits for current DHS employees, deferred revenue, insurance liabilities, environmental liabilities, and other. Other liabilities decreased approximately $2 billion from FY 2011. The decrease occurred primarily due to FEMA basing its FY 2011 insurance liability actuarial estimates on historical averages in accordance with industry practices. However, the events related to this accrual estimate did not conform to historical averages. Four percent of total liabilities results from accounts payable, which are actual or estimated amounts DHS owes to vendors for goods and services provided for which we have not yet paid. These liabilities are covered by current budgetary resources.

Statement of Net Cost



Net Cost of Operations represents the difference between the costs incurred by DHS programs less revenue. The Department's FY 2012 Statement of Net Cost displays DHS costs and revenue and groups the five strategic goals and two focus areas into four major missions. The first, *Fostering a Safe and Secure Homeland*, includes Missions 1, *Preventing Terrorism and Enhancing Security*, 2, *Securing and Managing Our Borders*, and 4, *Safeguarding and Securing Cyberspace*. This major mission, which involves the security and prevention aspects of the DHS Strategic Plan, represents 52 percent of the

Department's net cost. *Providing Essential Support to the National, Economic and Homeland Security* consists of the two focus areas of the DHS Strategic Plan: Providing Essential Support to National and Economic Security and Maturing and Strengthening DHS and represents 19 percent of the Department's net cost. *Ensuring Resilience to Disasters* is Mission 5 of the strategic plan and represents 19 percent of total net costs. *Enforcing and Administering Our Immigration Laws* is Mission 3 of the strategic plan and represents 10 percent of the Department total. The consolidation of the seven strategic goals into four major missions allows the average reader of the Statement of Net Cost to clearly see how resources are spent towards the common goal of a safe, secure, and resilient America. Note 23 in the Financial Information section shows costs by responsibility segment aligned to the major missions.

As a result of the Department's new strategic plan, combined with the change in the Statement of Net Cost presentation and cost-tracing methods implemented in FY 2012, DHS is not presenting the FY 2011 Statement of Net Cost comparative to FY 2012. The Department presents its FY 2011 Statement of Net Cost and related note disclosures by responsibility segment, as it appeared in the FY 2011 Annual Financial Report (AFR).

During FY 2012, the Department earned approximately $11.6 billion in revenue; this is an increase of about $619 million from $11 billion as of September 30, 2011. The increase is primarily due to an increase in FEMA's flood insurance premium revenue; acceleration of USCIS' H-1B applications, work authorizations, and adjustment status applications; and an increase in Federal Protective Service fees. The Department classifies revenue as either exchange ("earned") or non-exchange revenue. Exchange revenue arises from transactions in which DHS and the other party receive value and that are directly related to departmental operations. DHS also collects non-exchange duties, taxes, and fee revenue on behalf of the Federal Government. This non-exchange revenue is presented in the Statement of Custodial Activity, rather than the Statement of Net Cost.

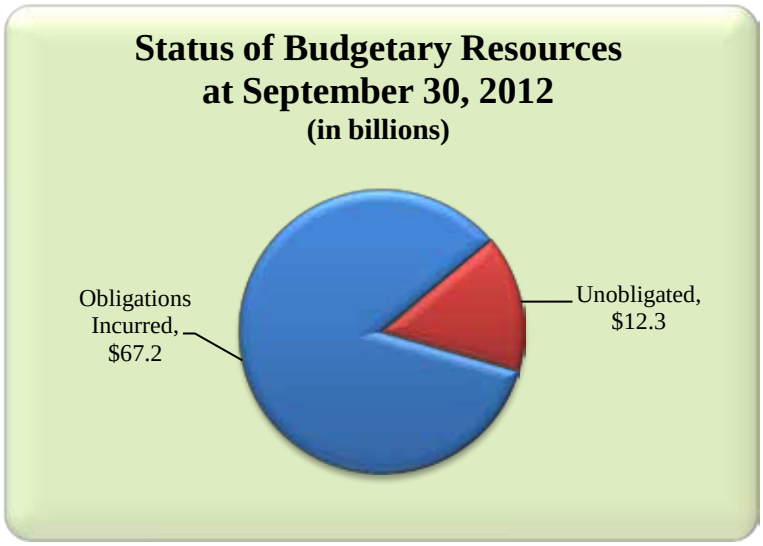
Statement of Changes in Net Position

Net position represents the accumulation of revenue, expenses, budgetary and other financing sources since inception, as represented by an agency's balances in unexpended appropriations and cumulative results of operations on the Statement of Changes in Net Position. Financing sources increase net position and include, but are not limited to, appropriations, user fees, and excise taxes. The net costs discussed above and transfers to other agencies decrease net position. Net position increased in FY 2012. This increase is primarily due to an overall decrease in net costs from FY 2011 and an adjustment due to a change in accounting principle for repairable spares at U.S. Coast Guard in FY 2012. For more information, see Note 32 in the Financial Information Section.

Statement of Budgetary Resources

This statement provides information on the status of the approximately $79.5 billion in budgetary resources available to DHS during FY 2012. The authority was derived from appropriations of $55.4 billion, $11.2 billion in authority carried forward from FY 2011, $10 billion in collections, and $2.9 billion of miscellaneous authority.

The total amount of resources available increased by approximately $1 billion from FY 2011. The change is primarily due to an increase in FEMA's disaster funding in FY 2012.



Of the total budget authority available, DHS incurred a total of $67.2 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions. These obligations will require payments during the same or future period. As of September 30, 2012, $12.3 billion of the $79.5 billion was not yet obligated. The $12.3 billion represents $8.5 billion in apportioned funds available for future use, and $3.8 billion in unapportioned funds.

Statement of Custodial Activities

This statement presents the disposition of revenue collected and disbursed by DHS on behalf of other recipient entities. An example of non-exchange revenue is user fees that CBP collects on behalf of the Federal Government as a result of its sovereign powers rather than as a result of providing goods or services for a fee. CBP collects revenue from a variety of duties, excise taxes, and various other fees. Non-exchange revenue is either retained by the Department to further its mission or returned to Treasury's General Fund. Total cash collections increased by more than $1 billion in FY 2012. This is due to increased importing, which resulted in additional cash collections for customs duties at CBP.

Stewardship Assets and Investments

DHS's stewardship assets primarily consist of U.S. Coast Guard heritage assets, which include ship equipment, lighthouses and other aids to navigation, communication items, military uniforms, ordnance, artwork, and display models. A heritage asset is any personal property that is retained by DHS because of its historic, cultural, educational, or artistic value as opposed to its current usefulness to carrying out the mission of the Department. When a heritage asset is predominantly used for general government operations, the heritage asset is considered a multi-use heritage asset. The U.S. Coast Guard has over 700 memorials, recreational areas, and other historical areas designated as multi-use heritage assets. CBP has four historical buildings and structures located in Puerto Rico, and FEMA has one training facility that is used by the United States Fire Administration for training in Emmitsburg, Maryland. In addition, CBP, USCIS, TSA, and S&T have collection-type assets that consist of documents, artifacts, immigration and naturalization files, architectural and building artifacts used for education, and a historical lighthouse at Plum Island Animal Disease Center.

Stewardship investments are substantial investments made by the Federal Government for the benefit of the Nation. When incurred, stewardship investments are treated as expenses in

calculating net cost, but they are separately reported as Required Supplementary Stewardship Information (RSSI) to highlight the extent of investments that are made for long-term benefits. Included are investments in research and development, human capital, and non-federal physical property.

Limitations of Financial Statements

The principal financial statements have been prepared to report the financial position and results of operations of the Department, pursuant to the requirements of Title 31, United States Code, Section 3515(b) relating to financial statements of federal agencies. While the statements have been prepared from the books and records of the entity in accordance with generally accepted accounting principles (GAAP) for federal agencies and the formats prescribed by OMB, the statements are in addition to the financial reports used to monitor and control budgetary resources, which are prepared from the same books and records. The statements should be read with the realization that they are for a component of the Federal Government, a sovereign entity.

Other Key Regulatory Requirements

See the Other Accompanying Information section for *Prompt Payment Act*, *Debt Collection Improvement Act*, and *Biennial User Charges Review* information.

Management Assurances

The Federal Managers' Financial Integrity Act, Federal Financial Management Improvement Act, and Department of Homeland Security Financial Accountability Act

DHS management is responsible for establishing, maintaining, and assessing internal control to provide reasonable assurance that the objectives of the *Federal Managers' Financial Integrity Act* (31 U.S. Code 3512, Sections 2 and 4) and the *Federal Financial Management Improvement Act* (Pub. L. 104-208) are met. In addition, the *Department of Homeland Security Financial Accountability Act* (Pub. L. 108-330) requires a separate management assertion and an audit opinion on the Department's internal controls over financial reporting.

In FY 2006, the Office of Management & Budget revised its Circular A-123 to address internal control reporting changes to align with private industry regulatory requirements. At that time, DHS management prepared a multi-year plan to implement its evaluation of controls over financial reporting as required under the revised guidance. Since FY 2006, DHS management has made significant improvements in management controls across DHS operations and financial management and reporting. Staff and management at Headquarters and in the Components have worked steadily and extensively to remediate operating and financial reporting controls such that DHS will be able to sustain its financial statement opinion and be able to achieve an opinion over internal control in the near future.

In FY 2011, DHS controls and financial management were improved such that DHS achieved its first opinion on the Balance Sheet and Statement of Custodial Activity. This was a major milestone for the Department. This year DHS achieved an opinion on all its financial statements, and is able to provide a qualified assurance over financial reporting controls. Much work remains to improve financial management processes and procedures in order to meet and sustain these critical milestones over time and become more efficient.

In assessing the Department's operational and financial management controls, management executes annual assessments to evaluate the status of internal controls to support the Secretary's annual assurance statement. These annual assessments are part of a multi-year implementation plan and management is required to assess controls to determine the extent and materiality of the deficiencies.

A material weakness within internal control over financial reporting is defined as a reportable condition or combination of reportable conditions that results in more than a remote likelihood that a material misstatement of the financial statements or other significant financial reports will not be prevented or detected. To identify material weaknesses and nonconformance conditions, management used the following criteria:

- Merits the attention of the Executive Office of the President and the relevant Congressional oversight committees;
- Impairs fulfillment of essential operations or mission;
- Deprives the public of needed services;

- Significantly weakens established safeguards against waste, loss, unauthorized use or misappropriation of funds, property, other assets, or conflicts of interest;
- Substantial noncompliance with laws and regulations; and
- Financial management systems conformance to government-wide systems requirements.

DHS instituted an Accountability Structure, which includes a Senior Management Council (SMC), an Internal Control Coordination Board (ICCB), and a Senior Assessment Team (SAT). The SMC approves the level of assurances for the Secretary's consideration and is comprised of the Department's Under Secretary for Management, Chief Financial Officer, Chief Readiness Support Officer, Chief Human Capital Officer, Chief Information Officer, Chief Information Security Officer, Chief Security Officer, and Chief Procurement Officer.

The ICCB seeks to integrate and coordinate internal control assessments with other internal control related activities and includes representatives from all DHS lines of business to address crosscutting internal control issues. Finally, the SAT, led by the Chief Financial Officer, is comprised of senior-level financial managers assigned to carry out and direct Component-level internal control over financial reporting assessments.

Component Senior Leadership provided assurance statements to the SAT that serve as the primary basis for the Secretary's assurance statements. These assurance statements are also based on information gathered from various sources including management-initiated internal control assessments, program reviews, and evaluations. In addition, these statements consider the results of reviews, audits, inspections, and investigations performed by the DHS Office of Inspector General (OIG) and the Government Accountability Office (GAO).

Secretary's Assurance Statement

November 14, 2012

The Department of Homeland Security is committed to a culture of integrity, accountability, fiscal responsibility, and transparency. The Department's management team is responsible for establishing and maintaining effective internal control over the three internal control objectives: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations.

In accordance with the *Federal Managers' Financial Integrity Act* (FMFIA) and the *Department of Homeland Security Financial Accountability Act* (DHS FAA), I have directed an evaluation of internal control at the Department of Homeland Security in effect during the fiscal year (FY) ending September 30, 2012. This evaluation was conducted in accordance with Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*. The Department provides reasonable assurance that the objectives of FMFIA, Section 2 over non-financial operations have been achieved, with the exception of three material weaknesses related to Financial Assistance Awards Policy and Oversight, Acquisition Management, and Funds Control.

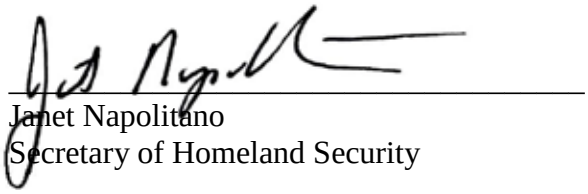
The Department has completed its FY 2012 limited-scope evaluation of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with our OMB approved plan; OMB Circular A-123, Appendix A; and departmental requirements. The Department provides reasonable assurance that our internal controls over financial reporting were operating effectively as of September 30, 2012, with the exception of three business processes – Financial Reporting; Property, Plant, and Equipment; and Budgetary Accounting – and IT systems and functionality, where material weaknesses have been identified and remediation is in process, as further described in the Other Accompanying Information. In addition, DHS does not currently have consolidated financial management systems that conform to the objectives of FMFIA, Section 4, and the *Federal Financial Management Improvement Act* (FFMIA). The Department will continue efforts to ensure that management control systems are in place to achieve the mission of the Department.

The Department follows a risk-based approach in determining which business processes will be assessed during the current year. Based on the results of the work performed, no additional material weaknesses were identified in the business processes listed in the Other Accompanying Information Section of this report.

We have made significant financial management improvements over the last several years enabling these historic milestones. The Department has identified, mitigated and reduced our material weaknesses related to internal controls over financial reporting to an unprecedented level and we are now able to provide reasonable assurance as required by law and regulation. We are committed to fully mitigating and eliminating the remaining material weaknesses such that we can provide full assurance and subsequently achieve an unqualified opinion on internal control. The outcome of the FY 2012 full scope audit and its resulting opinion on the Department's financial statements

represents a major milestone for DHS management. In addition, we are providing reasonable assurance over financial reporting in pursuit of our opinion on internal control.

We will continue to ensure taxpayer dollars are managed with integrity, diligence, and accuracy, and that the systems and processes used for all aspects of financial management demonstrate the highest level of accountability and transparency.



Janet Napolitano
Secretary of Homeland Security

Federal Financial Management Improvement Act

The Federal Financial Management Improvement Act of 1996 (FFMIA) requires Federal agencies to implement and maintain financial management systems that comply substantially with:

- Federal financial management system requirements;
- Applicable federal accounting standards; and
- The U.S. Standard General Ledger at the transaction level.

In assessing compliance with FFMIA, DHS uses OMB guidance and considers the results of the OIG's annual financial statement audits and *Federal Information Security Management Act* (FISMA) compliance reviews. As reported in the Secretary's Management Assurance Statements, significant system improvement efforts are in progress to modernize, certify, and accredit all financial management systems to conform to Government-wide requirements.

Financial Management Systems

Pursuant to the CFO Act, the DHS CFO is responsible for developing and maintaining agency accounting and financial management systems to ensure systems comply with applicable accounting principles, standards, and requirements and with internal control standards. As such, the DHS OCFO will oversee and coordinate all financial system modernization efforts.

DHS has adopted a hybrid approach to modernizing financial management systems across the Department. Our approach includes:

- Expanding business intelligence and standardizing data across Components to quickly provide enterprise-level reporting.
- Targeting investments in financial systems modernization in a cost-effective manner and minimizing duplication in infrastructure in accordance with emerging technologies and guidance, prioritizing essential system modernizations for the Components with the most critical need.

In accordance with OMB guidance, DHS will plan and implement incremental Component-level financial system modernization projects in order to deliver functionality faster and reduce risks often associated with large, complex IT projects. By splitting the projects into smaller, simpler segments with clear deliverables, DHS can ensure delivery of timely, well-managed solutions. DHS will also leverage existing infrastructure and evolving technologies, such as shared service providers and cloud-based solutions.

DHS has made great strides during the past year in our Financial Systems Modernization initiative. The Financial Systems Modernization Playbook (Playbook) articulates the vision and actions DHS is undertaking to strengthen access to and the quality of financial information to support decision making. It communicates our plan for expanding business intelligence capability to provide enterprise-level information and for strengthening financial systems in a cost-effective manner. These standards will also strengthen internal controls throughout the Department to provide more efficient operations.

DHS plans to continue forward by executing the financial system modernization activities as described in the Playbook. Specific goals for FY 2013 include the FEMA Technical refresh, a decision on the U.S. Coast Guard path forward, and a decision on the ICE path forward for financial systems modernization.

Federal Information Security Management Act

The *E-Government Act of 2002* (Pub. L. 107-347) Title III FISMA provides a framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. FISMA provides a statutory definition for information security.

The U.S. Department of Homeland Security 2012 Federal Information Security Management Act Report and Privacy Management Report consolidates reports from three DHS offices:

- Chief Information Officer (CIO) / Chief Information Security Officer (CISO);
- Inspector General (OIG); and
- Privacy Office.

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, the OIG reported that DHS continued to improve its information security program during FY 2012. For example, the CISO:

- Developed the *Fiscal Year 2012 DHS Information Security Performance Plan t*o enhance DHS's information security program and continue to improve existing processes, such as continuous monitoring, Plan of Action and Milestones (POA&M), and security authorization.
- Updated the Department's baseline IT security policies and procedures in DHS Sensitive Systems Policy Directive 4300A and its companion, *DHS 4300A Sensitive Systems Handbook*, to reflect the changes made in DHS security policies and various NIST guidance.
- In April 2012, the DHS CISO issued its second *State of Cybersecurity at The Department of Homeland Security* report. The report outlines how DHS anticipates and addresses emerging security risks from new technology products and advanced threat actor techniques, including its new initiatives and programs that ensure a secure computing environment within the Department. The report presents relevant information to employees for protecting their information and increasing the Department's cybersecurity awareness.
- The overall quality of security authorization documentation continues to improve in FY 2012. Compared with FY 2011, DHS identified fewer deficiencies in the security authorization documentation for the systems that were selected for review.

The OIG report, *Evaluation of DHS' Information Security Program for Fiscal Year 2012*, identified six recommendations for information security improvements. The CISO concurred with the recommendations and corrective actions are already underway to address each.