U.S. Department of Homeland Security Agency Financial Report

Fiscal Year 2013

Homeland Security

About this Report

The *U.S. Department of Homeland Security Agency Financial Report for Fiscal Year (FY) 2013* 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 2013, 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 Agency Financial Report*: Delivery date – December 11, 2013, revised December 19, 2013.

- *DHS Annual Performance Report*: Delivery date – February 3, 2014. The *DHS Annual Performance Report* is submitted with the Department's Congressional Budget Justification.

- *DHS Summary of Performance and Financial Information:* Delivery date – February 17, 2014.

When published, all three reports will be located on our public website at: http://www.dhs.gov/performance-accountability.

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

Visit Our Website
www.dhs.gov

Table of Contents

Message from the Acting Secretary

December 11, 2013

I am pleased to submit the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2013. 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, Bottom-Up Review, and DHS Strategic Plan.

Events of the past year demonstrate the significant challenges our Nation continues to face from terrorist attacks and natural disasters. Hurricane Sandy, the devastating wildfires across the western United States, and the tornadoes in Moore, Oklahoma, resulted in lives lost and billions of dollars in property damage. The Boston Marathon bombings and the arrest in Boise, Idaho, of an Uzbekistan national allegedly planning to use a weapon of mass destruction provide stark reminders that it only takes a few individuals to cause great harm. The global cyber heist and seizure of the Liberty Reserve digital currency system in May 2013 and sophisticated intrusions of public and private sector networks illustrate the growing threat of cyber crime and the importance of cybersecurity.

Now in its second decade as a Cabinet department, DHS continues its preparations to respond to all of these challenges and more. Since its creation, DHS has provided the Nation with significant new capabilities in the areas of cybersecurity and critical infrastructure protection, disaster preparedness, information sharing, and border security. 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.

Our work is never done, however, and we continue to face new and emerging threats in a constrained fiscal environment. We must strengthen our Nation's resiliency and provide protections from home-grown terrorists, radicalized individuals, and a range of potential threats from abroad. We must ensure our front lines are fully trained, equipped, and well supported while continuing to streamline operations and maximize efficiencies wherever feasible. We must also be prepared to address new operational and funding requirements that may be imposed on the Department, ranging from response to new terrorist tactics to the enactment of comprehensive immigration reform.

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. 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 to

increase efficiencies. In addition, 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 unclassified federal civilian government networks, work with critical infrastructure owners and operators to protect information systems, combat cyber crime, build a national capacity to promote responsible cyber behavior and cultivate the next generation of frontline cybersecurity professionals—while keeping a steady focus on safeguarding the public's civil rights and civil liberties.

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

DHS has made key investments to strengthen the homeland security enterprise, increase unification and integration, address challenges raised by the U.S. Government Accountability Office, 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. At the same time, we have challenged our workforce to fundamentally rethink how to do business—from the largest to the smallest investments. For the past four years, 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 2013 and discusses upcoming initiatives that will build on these efforts to achieve a safer and more secure Nation.

Management Assurances and Performance Measurement
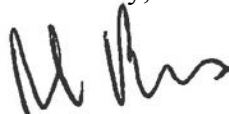
In FY 2012, DHS achieved a considerable milestone by earning a full-scope qualified audit opinion on all five financial statements. This was a first in the history of the Department and demonstrated the tremendous progress that has been made to improve the quality of financial management across DHS. Through continued commitment and dedication the Department has surpassed our previous achievements to bring even stronger transparency and accountability to financial management and reporting. I am proud to say that this year DHS has earned a clean full-scope audit opinion on all financial statements. This is a landmark accomplishment for the agency and was made possible because of the tremendous efforts of the men and women of the Department.

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, except those noted in our Annual Performance Report. DHS's performance and accountability reports for this and previous years are available on our public website: http://www.dhs.gov/performance-accountability.

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 scope of our mission is broad, challenging, and vital to the security of the Nation. We will continue to meet these and other challenges head-on, with a sense of urgency and purpose that the American people expect and that our mission requires. Thank you for your partnership and collaboration.

Sincerely,

Rand Beers
Acting Secretary

Management's Discussion and Analysis

The ***Management's Discussion and Analysis*** is required supplementary information to the financial statements and provides a high-level overview of the Department of Homeland Security.

The ***Overview*** section describes the Department's organization, its missions and goals, and provides an overview of our front-line Components.

The ***Performance Overview*** section 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.

The ***Financial Overview*** section provides a summary of DHS's financial data explaining the major sources and uses of funds and provides a quick look at our Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, Statement of Custodial Activities, Stewardship Assets and Investments, and Limitations of Financial Statements.

The ***Management Assurances*** section provides the Secretary's Assurance Statement related to the *Federal Managers' Financial Integrity Act*, the *Federal Financial Management Improvement Act*, and the *Department of Homeland Security Financial Accountability Act*. This section also describes the Department's efforts to address our financial management systems to ensure systems comply with applicable accounting principles, standards, requirements, and with internal control standards.

Overview

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 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
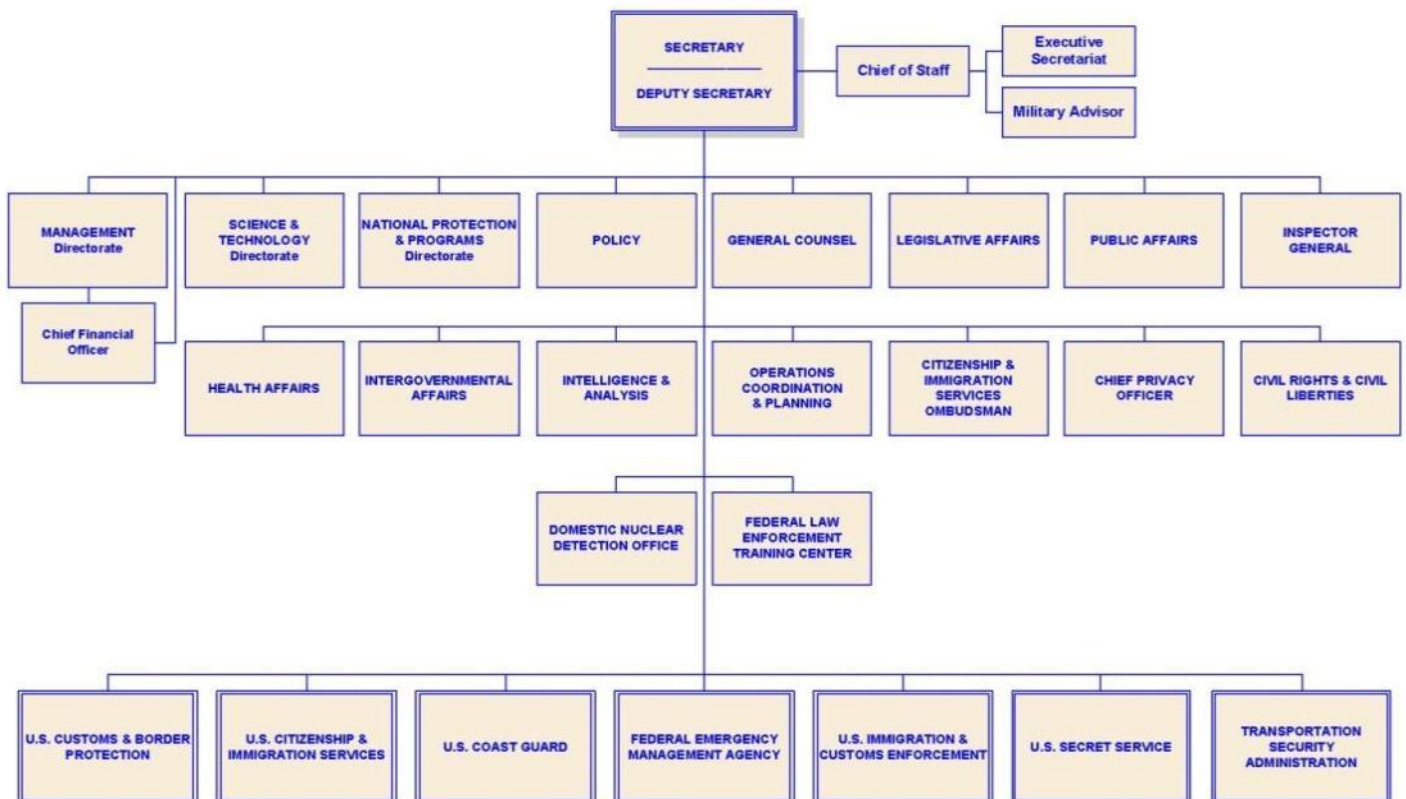
DHS Components

The following is a description of the major Components that make up the Department of Homeland Security. See our FY 2013 Federal Program Inventory at http://www.dhs.gov/publication/federal-program-inventory for more detail regarding the major programs within the DHS Components. Components listed below are those for which Congress appropriates funds through the budgeting process, whereas the Components in the financial reporting section are those tracked in the Treasury Information Executive Repository system presented in Note 1.A in the Financial Section. Click on the Component name for more information on their website.

Analysis and Operations manages the intelligence, information sharing, and operations coordination functions for DHS. Analysis and Operations includes the Office of Intelligence and Analysis (I&A) and the Office of Operations Coordination and Planning (OPS).

Departmental Management and Operations (DMO) provides support to the Secretary and Deputy Secretary in the overall leadership, direction, and management to the Department and all of its Components, ensuring the delivery of effective and efficient business and management services. DMO is responsible for Department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements.

Domestic Nuclear Detection Office (DNDO) works to enhance the nuclear and radiological detection efforts of federal, state, territorial, tribal, and local governments, and the private sector to ensure a coordinated response to such threats. DNDO is also responsible for advancing and integrating U.S. Government technical nuclear forensics efforts.

Federal Emergency Management Agency (FEMA) supports our citizens and first responders to ensure that as a Nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

Federal Law Enforcement Training Centers (FLETC) provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

National Protection and Programs Directorate (NPPD) leads the Department's mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability and through regulation of security of high-risk facilities.

Office of Health Affairs (OHA) serves as DHS's principal authority for all medical and health issues. OHA provides medical, public health, and scientific expertise to the Department in support of the DHS mission to prepare for, respond to, and recover from all threats.

Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Pub. L. 107-296) by an amendment to the *Inspector General Act of 1978*. OIG has a dual reporting responsibility to the Secretary of DHS and to Congress. OIG serves as an independent and objective audit, inspection, and investigative body to promote economy, effectiveness, and efficiency in DHS programs and operations, and to prevent and detect fraud, waste, and abuse.

Science and Technology (S&T) Directorate's mission is to strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise.

Transportation Security Administration (TSA) protects the Nation's transportation systems to ensure freedom of movement for people and commerce.

U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States and is responsible for granting immigration and citizenship benefits, promoting awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

U.S. Coast Guard (USCG) is one of the five armed forces of the United States and safeguards our Nation's maritime interests and natural resources, defends our maritime borders, and saves those in peril. Additionally, the USCG is a law enforcement and regulatory agency with broad domestic legal authorities.

U.S. Customs and Border Protection (CBP) is responsible for securing America's borders to protect the United States against threats and prevent the illegal entry of inadmissible persons and contraband, while facilitating lawful travel and trade.

U.S. Immigration and Customs Enforcement (ICE) is the largest investigative arm of DHS and the second largest investigative agency in the Federal Government. ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

U.S. Secret Service (USSS) carries out a unique dual mission of protection and investigations. The Service protects the President, Vice President, designated national leaders, other visiting heads of State and Government, and National Special Security Events; safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy; and investigates cyber and electronic crimes.

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 2010 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 focus areas of the Department are provided below. The plan will be updated in February 2014 in conjunction with the second QHSR.

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.

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.

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.

Mission 4: Safeguarding and Securing Cyberspace

DHS is responsible for protecting the federal Executive Branch civilian agencies 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.

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, and 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.

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.

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.

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 results will be published in the DHS FY 2013-2015 Annual Performance Report with the FY 2015 Budget Submission and can be accessed at http://www.dhs.gov/performance-accountability.

Performance Management in DHS

DHS is committed to strengthening our ability to report on performance results in achieving our goals and delivering value to the American public. The figure below shows our performance management progression. Department-wide measurement occurs each quarter and results are made available to DHS internal stakeholders. Detailed end-of-year results are made available to our external stakeholders through our Performance and Accountability Reports.

| Missions | Goals | Objectives | Mission Programs | Program Performance Goals | Performance Measures | Performance Targets | Performance Results |

Missions:	Describes at the highest level what the Department aims to achieve.
Goals:	A goal is a statement of aim or purpose included in the Department's Strategic Plan. In the DHS Annual Performance Plan, goals are the overarching structure used to group multiple Department objectives and their associated program performance goals. In their aggregate, program performance goals and Department objectives influence achievement of the Department goals.
Objectives:	An objective is an outcome-oriented statement in the Department's Strategic Plan that describes a targeted area of action to support achievement of the Department goals.
Mission Programs:	A mission program is an organized set of activities acting together to accomplish high-level outcomes external to DHS. Mission Programs are the operational processes, skills, technology, human capital, and other resources leveraged to achieve Department missions, goals, and objectives.
Program Performance Goals:	This is an outcome-oriented statement for each major DHS program that describes the value the program intends to deliver to its beneficiaries and the American public. Program performance goals are understood in terms of their associated performance measures and performance targets, which express the tangible, measurable objective against which actual achievement can be compared.
Performance Measures:	This is an indicator, statistic, or metric used to gauge program performance and assess progress in meeting the program performance goal, and in turn the missions, goals, and objectives of the Department.
Performance Targets:	A target is the projected level of performance for each performance measure during a fiscal year. A target is a quantifiable or measureable characteristic that communicates how well, or at what level, a program aspires to perform.
Performance Results:	A result is the actual level of performance for each performance measure achieved during a fiscal year. Results are compared to targets to determine how well actual performance measures up to that which was planned.

Mission 1: 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.

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 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

TSA Pre✓™

At participating airports with dedicated TSA Pre✓™ screening lanes, passengers assessed as low risk are afforded expedited physical screening and allowed to keep on their shoes, light outer wear/jackets, and belts, and are permitted to keep compliant 3-1-1 liquids and laptop computers inside their carry-on baggage. These procedures allow TSA to focus more attention to passengers assessed as unknown or higher risk. TSA Pre✓™ is now offered at more than 100 airports and more than 25 million travelers have undergone TSA Pre✓™ expedited screening. In November, TSA exceeded the 2013 year-end goal to achieve 25 percent of the 1.8 million travelers being eligible for expedited physical screening.

Other efforts to leverage the TSA Pre✓™ capability include: 1) allowing active duty military personnel who have Department of Defense issued Common Access Cards access to TSA Pre✓™; 2) conducting real-time threat assessments to identify low-risk passengers not formally designated for TSA Pre✓™ screening permission to receive TSA Pre✓™ expedited screening for that trip; and, 3) an enrollment program where travelers can apply directly for acceptance into the TSA Pre✓™ program eligibility.

Percent of international air enplanements vetted against the terrorist watch list through Secure Flight (TSA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	100%	100%	100%	100%

Airlines submit passenger information to Secure Flight, which uses it to perform watch list matching. This serves to prevent individuals on the No Fly List from boarding an aircraft and to identify individuals on the Selectee List for enhanced screening. After matching passenger information against government watch lists, Secure Flight transmits the matching results back to airlines before they can issue passenger boarding passes. TSA has maintained a 100 percent vetting of international travelers against the terrorist watch list for the past three years.

Percent of inbound air cargo screened on international passenger flights originating from outside the United States and Territories (TSA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	93%	100%	99.5%

TSA reached the legislatively mandated target of 100 percent of inbound cargo screened beginning in January 2013. The end-of-year percentage reflects the entire fiscal year to include a portion of the first quarter of FY 2013 that was not covered by the 100 percent screening mandate. This is a significant milestone, as it is the culmination of numerous policies and procedures, agreements with foreign countries, equipment installations, training, and logistical strategies to implement an effective and efficient process to ensure the security of air cargo while facilitating the flow of legitimate commerce.

Percent of overall compliance of domestic airports with established aviation security indicators (TSA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
95%	96%	95.9%	95%	100%	94.4%

This measure reflects key security indicators that are a predictor of the overall security posture of an airport. Identifying compliance with the key indicators assesses airport vulnerabilities and is part of TSA's overall risk reduction process. In FY 2013, TSA identified that 94.4 percent of domestic airports comply with established security indicators, slightly down from FY 2012 results and consistent with the long-term trend in compliance. 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 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 (USSS)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
100%	100%	100%	100%	100%	100%

The USSS continues to meet its goal of 100 percent incident-free protection for our Nation's leaders, foreign dignitaries, designated protectees, and others during travel or while at protected facilities. USSS's protection planning process requires close coordination with federal, state, or local law enforcement and other officials. Only through intense planning, communication, and training can the USSS successfully provide incident-free protection.

National Special Security Event – 2013 Presidential Inauguration

The 2013 Presidential Inauguration was designated as a National Special Security Event (NSSE). The Department of Homeland Security designates an event as an NSSE when there is an inherent risk of terrorism, or other security issues requiring additional federal assets and resources. When an event is declared an NSSE, USSS 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.

USSS's security planning process recognizes that no one federal, state, or local government agency alone can carry out the measures necessary to secure the event. Only through intense planning, communication, and training can an NSSE be secured successfully.

The 57th Presidential Inauguration was held in Washington, D.C. on January 20, 2013. It was the 43rd NSSE in which the Secret Service designed and implemented the security plan. Over the three-day period covering the Inauguration, the USSS covered more than 1,000 post standing assignments. There were 17 federal, state, local, and military agencies who served as members of the Executive Steering Committee and 25 subcommittees.

Looking Forward

The United States has made significant progress in securing the Nation from terrorism. Nevertheless, work remains as the terrorist threats facing the country have evolved and will continue to change. Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners, internationally, across the federal, state, and local governments, tribal and territorial, public and private sectors, and communities across the country have strengthened the homeland security enterprise to better mitigate and defend against dynamic threats. Below are a few areas that advance our efforts to achieve the Department's mission of preventing terrorism and enhancing security.

Information Sharing

One of the principal recommendations of the 9/11 Commission was to address information sharing shortfalls. Protecting the country from evolving transnational threats requires a strengthened homeland security enterprise that shares information across organizational boundaries while ensuring that information is available to frontline operators. DHS has implemented a national network of fusion centers that serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and state, local, tribal, territorial, and private sector partners. DHS is conducting annual assessments through the collection of outcome-based performance data and targeted exercises to identify capability gaps in order to develop future improvements to our information sharing capabilities. In addition, DHS will be expanding its strategic partnerships with international allies to enhance targeting and information sharing efforts to interdict threats and dangerous people and cargo at the earliest point possible.

Risk-Based Security

DHS continues to improve and strengthen the security of the Nation's transportation systems while ensuring the freedom of movement for people and commerce. To enable our agents to focus on the highest risk passengers, TSA and CBP are expanding the use of trusted traveler programs, such as TSA Pre✓™ and CBP Global Entry. These are pre-screening initiatives for travelers to expedite screening at domestic checkpoints. TSA anticipates 25 percent of the traveling public will be eligible for expedited domestic screening through TSA Pre✓™ by the end of 2013. Global Entry membership nearly doubled in FY 2013, with wait times for Global Entry members approximately 85 percent lower than the average wait times of non-members. CBP is continuing to expand Global Entry by creating new enrollment centers and conducting on-site enrollment events to better serve the public.

Global Nuclear Detection Architecture

DHS seeks to evolve the Global Nuclear Detection Architecture in coordination with other DHS Components, the U.S. Attorney General, the intelligence community, and the Departments of State, Defense, and Energy. This comprehensive framework incorporates detector systems, telecommunication, and personnel, with the supporting information exchanges, programs, and protocols that serve to detect, analyze, and report on radiological and nuclear materials that are not in regulatory control. DNDO is working to ensure that capabilities to scan for radiological and nuclear threats at ports of entry can be maintained and sustained. In FY 2013, DNDO conducted numerous trade studies and initiated an analysis of alternatives to determine the best path forward for replacing and/or refurbishing radiation portal monitor (RPM) systems. In FY 2014, an analysis of alternatives will be completed and acquisition activities will start—to include initiating operational requirements/capabilities documentation, concept of operations, logistical support, life-cycle cost documents, and test planning—in support of the RPM acquisition strategy.

Mission 2: 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.

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

Consequence Delivery System – Improving Border Control

In January 2011, the U.S. Border Patrol began implementing the Consequence Delivery System (CDS) on the Southwest border as a means to employ an analytical process that standardizes decision making about the application of consequences, and gives the Border Patrol the ability to examine the efficiency and effectiveness of individual consequences on various types of deportable aliens. In FY 2013, CDS began expanding and is currently at various stages of implementation in Northern and coastal border sectors, and in Southwest border field offices at land ports of entry.

Recidivism and the average number of apprehensions per recidivist are the strongest indicators of CDS's effectiveness. Since CDS implementation in FY 2011, the annually reported recidivism rate has decreased each year from an average of 27 percent to 16 percent in FY 2013. Likewise, the number of apprehensions associated with each recidivist has also decreased significantly from an average of 2.71 to 2.41 in FY 2013.

The results and details of the CDS methodologies are continuously shared with CBP's strategic partners, informing a risk-based decision-making process and determining the most effective and efficient use of post-apprehension resources. CDS provides sound, evidence-based guidance that informs decision-making at the tactical, operational, and strategic levels. CBP will continue to expand and automate CDS processes to rapidly respond to changing operational conditions.

Percent of people apprehended multiple times along the Southwest border (CBP)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	---	≤ 18%	16%

This measure examines the percent of deportable individuals who have been apprehended multiple times by the U.S. Border Patrol. Effective and efficient application of consequences for illegal border crossers will, over time, reduce overall recidivism. In FY 2013, CBP exceeded their target and will continue to expand their consequence delivery system approach to all sectors.

Percent of imports compliant with U.S. trade laws (CBP)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	98.89%	97.67%	96.46%	97.5%	97.66%

This measure reports the percent of imports that are compliant with U.S. trade laws including customs revenue laws. Ensuring that all imports are compliant and free of major discrepancies allows for lawful trade into the United States. Based on improved oversight and strong trade partnership programs, the FY 2013 results improved from FY 2012.

Security compliance rate for high-risk maritime facilities (UCSG)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	99.9%	98.7%	100%	99.3%

This measure is a leading indicator of maritime facility security and resiliency in our Nation's ports. Compliance of high-risk facilities is determined based on whether a major problem is found during an inspection, requiring a notice of violation or civil penalty. High-risk maritime facilities are a

subset of the entire national waterfront facility population which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked based on the nature of their activities and/or the products they handle. The FY 2013 results are consistent with prior year results and with a slight increase over FY 2012 results.

Trade Partnership Programs

Initiated shortly after the tragic events of 9-11, the Customs Trade Partnership Against Terrorism (C-TPAT) program is one of the most successful trade partnership programs ever, and C-TPAT is one of the cornerstones in CBP's fight against terrorism.

C-TPAT served as the model for all international supply chain security/industry partnership programs and one of its primary goals was to internationalize its core principles into a shared global strategy. To achieve its goal, C-TPAT pioneered the concept of the bilateral Mutual Recognition Arrangement (MRA), a process where C-TPAT and a foreign customs administration's industry partnership program have established a standard set of security requirements which allows one industry partnership program to recognize the validation findings of the other program. This leads to a series of benefits to both customs administrations and to the private sector participants. To date, C-TPAT has signed seven MRAs.

C-TPAT expanded the MRA concept beyond a bilateral agreement by signing an MRA with the European Union (EU), a confederation of 28 countries. The leadership of CBP and the European Union Taxation and Customs Union Directorate signed the MRA on May 4, 2012. The US-EU MRA covers one third of the world's trade, and expedites cargo through the import/export process, which has a positive effect on approximately 10,000 business entities within supply chains on both sides of the Atlantic. It is the first MRA that has a fully automated data exchange process; data to and from each of the programs flows automatically and securely 24 hours a day. The protocols establishing the automated data exchange were adopted by the World Customs Organization and are now the template for new MRAs worldwide.

Looking Forward

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 global economy is increasingly a seamless economic environment connected by systems and networks that transcend national boundaries. The United States is deeply linked to other countries through the flow of goods and services, capital and labor, and information and technology across our borders. As much as these global systems and networks are critical to the United States and our prosperity, their effectiveness and efficiency also make them targets for exploitation by our adversaries, terrorists, and criminals. Thus, border security cannot begin simply at our borders. Below are a few areas that advance our efforts to achieve the Department's border security goals.

Border Control by Consequence Delivery
CDS, implemented in FY 2011, applies targeted enforcement in response to cross-border illegal activity along the Southwest, Northern, and coastal U.S. borders. Through CDS, consequences are applied through advanced analysis of consequence programs and alien classification to yield the greatest impact. CDS standardizes the decision-making process, guiding management and agents

through a process designed to uniquely evaluate the circumstances of each apprehension of a subject and apply the best consequence for that individual to influence the subject against future illegal entry attempts. The results and details of the CDS methodologies are continuously shared with CBP's strategic partners, informing a whole-of-government risk-based decision-making process and determining the most effective and efficient use of post-apprehension resources. CDS provides sound, evidence-based guidance that informs decision-making at the tactical, operational, and strategic levels. CBP will continue the expansion and automation of CDS processes to rapidly respond to changing operational conditions.

Global Supply Chain
DHS is working with the thousands of companies who are members of the C-TPAT to strengthen security in the supply chain, as described on the previous page. The purpose of C-TPAT is to partner with the trade community to secure the U.S. and international supply chains from possible intrusion by terrorist organizations. In addition, the DHS Container Security Initiative (CSI) is the only multi-national program in the world protecting the primary system of global trade—maritime containerized shipping—from being exploited or disrupted by international terrorists. Operational in 58 ports, CSI facilitates screening of approximately 80 percent of the volume of maritime cargo destined for the U.S. by using automated tools to identify containers that pose a potential risk and using technology to scan these containers for radiological or nuclear material without impeding the flow of trade. Although C-TPAT and CSI programs are in a steady-state of operations, DHS has ongoing collaborative activities with the Departments of Agriculture and Commerce, and the Food and Drug Administration to further streamline trusted trader programs. In addition, DHS is analyzing the feasibility of a joint program with the TSA's Known Shipper Program through a pilot initiated this past year.

Border Detection Capability
DHS technology programs deliver detection and surveillance systems to both the Southwest and Northern borders. These technology systems enhance DHS's ability to know what is happening along our borders—referred to as situational awareness—to respond to and resolve illegal activity. In addition, investments in surveillance technology, in particular, have a workforce multiplier effect. Prior to recent investments in technology, many Border Patrol agents provided situational awareness through individual detection related duties. With the deployment of fixed and mobile surveillance capabilities, these new technologies now perform those duties, freeing agents to focus on other vital tasks such as identification, tracking, interdiction, and resolution of events. As part of the Arizona Technology Plan, CBP plans to acquire and deliver integrated fixed tower systems. An integrated fixed tower system is a network of towers that consist of surveillance equipment mounted on fixed towers and integrated with command and control equipment capable of displaying information on a common operating platform. This technology is selected for remote, difficult terrain areas to maintain security and situational awareness with persistent, wide-area surveillance.

Intellectual Property
CBP has implemented its five-year strategy to enforce intellectual property rights (IPR) based on the pillars of facilitation, enforcement, and deterrence. This strategy improves DHS's ability to facilitate lawful trade, seize counterfeit and pirated goods, and deter violations. CBP's IPR strategy assesses the risk of imports for IPR violations, targets suspect shipments, conducts seizures of infringing goods, and completes the process with post-entry audits and coordination with ICE for prosecution of violators. The ICE-led National Intellectual Property Rights Coordination Center's mission is to ensure national security by protecting the public's health and safety and the

U.S. economy. The IPR Center brings together 17 key federal investigative agencies, Interpol, Europol, and the governments of Canada and Mexico in a task force setting to efficiently and effectively leverage the resources, skills, and authorities, and provide a comprehensive response to IP theft. The IPR Center will continue to focus its efforts on strengthening its commercial fraud enforcement program, addressing developing threats related to online intellectual property theft, and investigating those who seek to introduce counterfeit and substandard products that pose a health and safety risk. DHS has also continued refining the maritime environment IPR predictive risk model. The IPR strategy is correlated with a 64 percent increase in seizures from 2009. Moving forward, CBP will coordinate several IPR enforcement operations such as the new post-entry IPR Strike Unit, being piloted in coordination with ICE Homeland Security Investigations (HSI), which has re-engineered the IPR compliance review process by focusing on real-time techniques and informed compliance to build better cases against IPR violators.

Mission 3: 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.

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

Deferred Action for Childhood Arrivals

On June 15, 2012, the former Secretary of Homeland Security, Janet Napolitano announced that certain people who came to the United States as children and meet several key guidelines may request consideration of deferred action for a period of two years, subject to renewal, and would then be eligible for work authorization. Deferred action does not provide an individual with lawful status. Deferred action is a discretionary determination to defer removal action of an individual as an act of prosecutorial discretion to ensure that enforcement resources are not expended on low priority cases. DHS instead focuses enforcement resources on the removal of individuals who pose a danger to national security or a risk to public safety, including individuals convicted of crimes with particular emphasis on violent criminals, felons, and repeat offenders.

Since August 15, 2012, USCIS has received more than 599,000 requests for consideration of deferred action under the Deferred Action for Childhood Arrivals (DACA) process. During FY 2013, USCIS immigration services officers reviewed and approved more than 436,000 requests, and issued Employment Authorization Documents to those found eligible under the program. DACA illustrates USCIS's ability to develop a new filing process quickly and successfully, through hard work and a committed workforce.

Average of processing cycle time (in months) for naturalization applications (N-400) (USCIS)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
4.2	4.5	4.6	4.6	≤ 5	4.7

An N-400, Application for Naturalization, is filed by an individual applying to become a U.S. citizen. This measure assesses the program's ability to meet its published processing time goals by center or field office. Although the N-400 cycle times achieved the annual target, the slight upward trend over the past few years can be attributed to an increase in receipts and shifting immigration services officer adjudication hours across application types with the greatest pending volumes.

Overall customer service rating of the immigration process (USCIS)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	80%	93%	85%	87%

This measure gauges the overall rating of the immigration process and is based on the results from the following areas: 1) accuracy of information; 2) responsiveness to customer inquiries; 3) accessibility to information; and 4) customer satisfaction. Although there was a decrease in the overall customer satisfaction rating from FY 2012, USCIS met its target and exceeded industry customer satisfaction averages.

Percent of initial mismatches for authorized workers that are later determined to be "Employment Authorized" (USCIS)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	0.28%	0.24%	≤ 1.0%	0.22%

This measure gauges the accuracy of the E-Verify process by assessing the percent of employment verification requests that result in a confirmation that are not positively resolved during initial review. E-Verify continues to be very successful in matching employees to their government records during the initial electronic matching phase. In those cases where the electronic check does not find a match, it is very rare that the applicant will be found to be employment authorized after contesting the initial determination. USCIS continues to improve its processes through E-Verify enhancements such as mismatch notices to employees and Self Check, a free online service that allows an individual to check his or her employment eligibility. FY 2013 results are consistent with the past two years and remain significantly below target and trending downward.

Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days) (ICE)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	37.0	34.7	31.9	≤ 35	33.5

This measure provides an indicator of efficiencies achieved in working to drive down the average length of stay for convicted criminal aliens in ICE's detention facilities. Decreases in the average length of stay can significantly reduce the overall costs associated with maintaining an alien population prior to removal. In FY 2013, ICE saw a moderate increase in the average length of stay for criminal aliens due to reduced participation in the Alien Transfer Exit Program on June 1, 2013 and guidance that detainers not be placed upon some aliens who, although illegally present in the United States, have only committed minor offenses, or none at all.

Looking Forward
The success of our Nation's immigration policy plays a critical role in advancing homeland security. DHS is focused on smart and effective enforcement of U.S. immigration laws while

streamlining and facilitating the legal immigration process. Effective administration of the immigration system depends on ensuring that immigration decisions are impartial, lawful, and sound; that the immigration system is interactive and user friendly; that policy and procedural gaps are systematically identified and corrected; and that those vulnerabilities that would allow persons to exploit the system are eliminated. Enforcement efforts must prioritize the identification and removal of dangerous foreign nationals who threaten our national security or the safety of our communities and must include safe and humane detention conditions and respect for due process and civil rights as accorded by law. Below are a few initiatives that advance our efforts to achieve the Department's immigration enforcement and administration goals.

Immigration Business Processing Transformation

USCIS continues to make major strides by modernizing the process for filing and adjudicating immigration benefits. Using USCIS's Electronic Immigration System (ELIS), the Agency will transition from a paper-based environment for adjudicating benefit applications to an electronic one. Iterative releases will add form types and functions to the system, gradually expanding to cover filing and adjudication for all USCIS immigration benefits. USCIS's long-term goal is to add functionality and benefit types until all applications are processed through ELIS.

Criminal Alien Removals

ICE Enforcement and Removal Operations (ERO) is responsible for ensuring that every alien ordered to leave the United States does so. In order to enhance the efficiency and effectiveness of the program, ERO is focusing its detention programs primarily towards aliens who pose a risk to public safety, with an emphasis on violent criminals, felons, and repeat offenders. This strategy allows ICE to place low-risk, non-mandatory detainees in lower cost alternatives to detention programs, such as electronic monitoring and intensive supervision. ICE has developed an Agency Priority Goal to focus on the removal of criminal aliens over the next two years and plans to implement actions to identify and apprehend criminal aliens through joint operations and through targeted and surge operations both regionally and nationwide. ICE will also be focusing on opportunities to reduce the average length of stay of those criminal aliens in detention by focusing on efficiencies in the legal process. ICE is also pursuing improvements in the handling of cases involving alternate removal methods such as stipulated and reinstated orders of removal.

Homeland Security Investigations

HSI has the broadest legal authority of any U.S. federal criminal investigative agency—empowered to enforce over 400 federal statutes—and uses this authority to investigate all types of smuggling and transnational criminal activity to deter, disrupt, and dismantle terrorist organizations and other malicious actors. HSI leadership implemented the strategic risk assessment (SRA) to identify HSI's highest priority enforcement areas. The SRA enables HSI to make risk-informed resource allocation decisions and serves as a conduit through which HSI improves the operational effectiveness of criminal investigations that protect the United States against terrorists and criminal organizations. Over the next two years, HSI will work to optimize the SRA process and integrate into ICE's 2016-2020 Strategic Planning.

Mission 4: 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.

> **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

EINSTEIN Expansion

In July 2013, the National Cybersecurity Protection System, operationally known as EINSTEIN, deployed EINSTEIN 3 Accelerated (E^3A) for intrusion prevention security services to its first federal civilian agency. DHS is transitioning the program from one in which the government builds and deploys intrusion prevention systems to one in which DHS contracts with major internet service providers (ISPs) to supply intrusion prevention security services. These services are then augmented through the sharing of sensitive government information with those service providers.

E^3A employs cyber threat indicators to inform threat-based decision-making on network traffic entering or leaving participating civilian Federal Executive Branch networks. E^3A leverages cutting edge ISP cyber capabilities to deploy rapidly scalable solutions, operating and evolving with agility to match dynamic threats. This public-private collaborative effort initially focuses on two critical intrusion prevention security services capabilities: domain name service sinkholing and e-mail filtering, which are threat pathways comprising 85 percent of known threats to the .gov domain. E^3A is currently scheduled to be fully deployed to all federal agencies by the end of FY 2015, three years earlier than an initial design concept based on a government-owned and operated solution.

Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies (NPPD)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	73%	70%	82.4%

This measure assesses DHS's scope of coverage for malicious cyber activity across participating civilian Federal Government Agencies.[1] Federal Executive Branch network monitoring uses EINSTEIN intrusion detection system sensors, which are deployed to trusted internet connection locations at agencies or ISPs. These sensors capture network flow information and provide alerts when signatures, indicative of malicious activity, are triggered by inbound or outbound traffic. In FY 2013, the target was significantly exceeded, achieving 82 percent of traffic monitored.

---

[1] Defined as Chief Financial Officers (CFO) Act agencies (other than the Department of Defense) as well as non-CFO Act agencies that are Trusted Internet Connection Access Provider agencies.

Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace (I&A)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	88%	90%	94%

This measure gauges the extent to which the DHS Intelligence Enterprise is satisfying their customers' needs related to understanding threats to cyberspace so they can manage risks and respond effectively to incidents. In FY 2013, results improved over FY 2012 and exceeded expectations.

Number of law enforcement individuals trained in cyber crime and cyber forensics both domestically and overseas (USSS)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	---	1,000	1,517

This measure represents the annual participation in USSS cyber crime and cyber forensics courses. This specialized technical training occurs both domestically and overseas in an effort to strengthen our ability to fight cyber crime. In FY 2013, USSS trained 1,517 individuals, far exceeding expectations.

Percent of planned cyber security products and services transitioned to commercial and open sources (S&T)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	---	60%	89%

This measure reflects the percent of the S&T Directorate projects that identify and complete planned transitions of a cybersecurity product and/or service to a commercial or open source. In FY 2013, S&T exceeded expectations, completing 89 percent of planned cybersecurity product and service transitions.

Stop.Think.Connect.™ Campaign Partnership Grows

The Stop.Think.Connect.™ Campaign significantly grew its partnership programs during FY 2013, with a kick-off during National Cyber Security Awareness Month in October with more than 20 events focused on Law Enforcement and Cybersecurity, Online Safety for Business/Industry, and Digital Literacy.

Using social media to raise national awareness, the campaign leveraged the DHS @cyber Twitter handle and its more than 11,800 followers to market new content development, blogs, and updates, and solicit participation in monthly "Twitter Chats" with partners and stakeholders—potentially creating more than 31 million interactions. As members of the Stop.Think.Connect.™ National Network, the Young Women's Christian Association (YWCA) and its leadership actively promoted the campaign by regularly issuing tweets from the @YWCAUSA and @YWCEO Twitter handles to more than 3,200 followers.

As an indicator of its successful outreach through various avenues during FY 2013, the Stop.Think.Connect.™ Campaign saw 34 government partners join the campaign's Cyber Awareness Coalition, representing a 36 percent increase since the end of the 2012 calendar year. During the same timeframe, 34 non-profit partners joined the campaign's national network, representing an increase of 54 percent since the end of the 2012 calendar year. In addition, as of the end of September 2013, more than 34,000 individuals have signed up to become friends of the campaign and to receive information regarding cybersecurity awareness, which is an increase of 35 percent since the end of FY 2012.

Looking Forward
Cyberspace is highly dynamic and the risks posed by malicious cyber activity transcend traditional borders and boundaries. Today's threats to cybersecurity require the engagement of the entire society—from government and law enforcement to the private sector and most importantly, members of the public—to mitigate malicious activities while bolstering defensive capabilities. Below are a few areas that advance our efforts to achieve the *Department's Safeguarding and Securing Cyberspace* mission.

Continuous Monitoring and Diagnostics
Continuous Monitoring and Diagnostics (CMD) provides hardware, software, and services designed to strengthen the operational security posture of all federal civilian networks. CMD involves the procurement, operations, and maintenance of monitoring equipment, diagnostic sensors and tools, and dashboards to provide situational awareness at federal enterprise and agency levels. With CMD, agencies will be able to identify which network security issues to address first, and empower technical managers to prioritize and mitigate risks. The Department will expand this capability across federal networks in support of mitigation activities designed to strengthen the operational security posture of federal civilian networks to better mitigate advanced, persistent cyber threats that are emerging in a dynamic threat environment.

National Cybersecurity Protection System
The National Cybersecurity Protection System (NCPS) serves as an integrated intrusion detection, analytics, information sharing, and intrusion prevention system that utilize hardware, software, and other components to support DHS responsibilities within the Comprehensive National Cybersecurity Initiative mission. NCPS will continue to expand traffic protocols covered by intrusion prevention services and acquire failover capabilities at internet services providers to ensure system redundancy and improve service to geographically distributed federal networks. In addition, NCPS will support the expansion of multi-directional information sharing capabilities in support of government and private sector cybersecurity operations.

Critical Infrastructure Cybersecurity
As physical and cyber infrastructure continue to become increasingly connected, critical infrastructure and emergency response functions are inseparable from the information technology systems that support them. The government's role in this effort is to share information and encourage enhanced security and resilience, while identifying and addressing gaps not filled by the private sector. The Department will work with critical infrastructure, on a voluntary basis, to implement or otherwise mature initiatives developed pursuant to Executive Order 13636 (Improving Critical Infrastructure Cybersecurity) while continuing to support private sector risk management at the nexus of cyber and physical infrastructure. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) will continue to reduce risks within and across all critical infrastructure sectors by collaborating with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. Over the next two years, ICS-CERT is planning to conduct more than 100 voluntary cybersecurity assessments across the Nation's critical infrastructure and key resources sectors. ICS-CERT will also revise and update the cybersecurity evaluation tool, a self-assessment tool provided freely to critical infrastructure partners that identifies potential cybersecurity vulnerabilities within a network. Through the DHS Loaned Executive Program, the Department will continue working with the private sector on innovative solutions to homeland security challenges, including cybersecurity.

Cyber Crime

Cyber crime is the fastest growing criminal activity world-wide. DHS efforts to mitigate this risk are focused on identity theft, financial crime, and national security-related crimes committed over the internet. ICE and USSS will continue their work to provide computer forensics support and training for investigations into domestic and international criminal activities, including computer fraud, network intrusions, financial crimes, access device fraud, bank fraud, identity crimes and telecommunications fraud, benefits fraud, arms and strategic technology, money laundering, counterfeit pharmaceuticals, child pornography, and human trafficking occurring on or through the Internet.

Mission 5: 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.

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
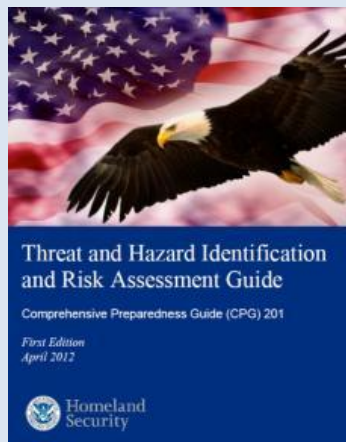
Threat Hazard Identification – Understanding Our Risk

DHS works hard to ensure that the Nation continually strengthens its resiliency and becomes as prepared as it can be against all hazards. Building upon progress made in the National Preparedness Goal and the description of the National Preparedness System, DHS continues to use Threat and Hazard Identification and Risk Assessments (THIRAs) to understand the risks communities face. All states and territories submitted a THIRA this past year, providing invaluable information to inform the overall level of national preparedness identified in the National Preparedness Report. In addition, 34 urban areas and tribal governments submitted THIRAs.

Providing a common way to more fully understand the risks communities face, the THIRA does not just look at natural hazards or terrorist threats, but takes into account the threats and hazards that pose the greatest risk to a community, regardless of cause. The THIRAs demonstrated collaboration among partners inside and outside of government and highlighted interesting similarities and differences in perspective. Moving forward, the THIRAs received in FY 2013 will serve as a foundation from which FEMA and its partners can understand collective risks and make informed decisions about how to best to allocate resources and manage risk.

Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes (FEMA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	48%	56%	53%	57%

This measure assesses the number of communities adopting building codes containing provisions that adequately address earthquake, flood, and wind hazards. FEMA works with code adoption and enforcement organizations to support community implementation of disaster resistant building codes. In FY 2013, results demonstrated a slight increase from FY 2012 and met expectations.

Percent of states with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance (FEMA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	---	100%	86%

Developing and maintaining an understanding of risks faced by communities and the Nation is an essential component of the National Preparedness System. THIRA guidance provides a common and consistent approach for identifying and assessing risks and their associated impacts. Completing a THIRA enables a community to maintain a baseline understanding of the risks that they face, facilitates efforts to identify capability and resource gaps, focuses capability improvements, and informs the community of actions they can take to manage their risks. Although all states and territories submitted their THIRAs, not all met the current DHS guidance. FEMA has provided updated guidance and will provide technical assistance that will allow us to meet our 100 percent target in FY 2014.

Percent of incident management and support actions necessary to stabilize a jurisdiction within 72 hours or by the agreed upon time (FEMA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	---	100%	100%

This measure reflects FEMA's role in effectively responding to any threat or hazard, with an emphasis on saving and sustaining lives within 72 hours, in support of state, local, tribal, and territorial governments. Actions necessary to stabilize an incident in order to ensure the best outcomes for survivors are defined as those functions that must be initiated immediately following an incident such as: interoperable communications between FEMA-supported incident sites; deploying urban search and rescue resources; rapidly activating response coordination centers; and issuing timely alerts, warnings, operations orders, and situation reports. In FY 2013, FEMA achieved its 100 percent target.

Percent of recovery services through Individual Assistance delivered to disaster survivors gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster (FEMA)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	---	---	91%	94.5%

Recovery assistance helps individuals affected by disasters and emergencies return to normal quickly and efficiently. This measure reflects FEMA's role in delivering quality services to disaster survivors using a random survey of registered disaster assistance applicants who received assistance within the previous fiscal quarter. In FY 2013, FEMA exceeded its target, achieving a 94.5 percent satisfaction rating.

Hurricane Sandy Recovery: Use of Social Media

On October 29, 2012, Hurricane Sandy made landfall along the East Coast with battering waves and wind gusts. Using forward deployed personnel and resources, FEMA effectively supported disaster preparedness and response operations, including search and rescue, situational awareness, communications and logistical support. FEMA continues to lead the Federal Government's efforts to support affected communities as they recover.

Despite the good work done by the whole community to come together to meet the needs of disaster survivors, some rumors circulated online about fraudulent services. FEMA was active in social media engagement by identifying and responding to misinformation through a rumor control page on fema.gov and m.fema.gov. To ensure correct information was provided to survivors, social media and websites were updated regularly with the online links or physical locations to apply for assistance. To further build on the social media engagement, FEMA held Twitter chats, using the @FEMASandy Twitter account, which served as great opportunities to engage directly with citizens and answer their questions about the recovery progress.

Looking Forward

DHS coordinates comprehensive federal efforts to prepare for, protect against, respond to, recover from, and mitigate a terrorist attack, natural disaster or other large-scale emergency, while working with individuals, communities, the private and nonprofit sectors, faith-based organizations, and local, state, tribal, territorial and federal partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include fostering a Whole Community approach to emergency management nationally; building the Nation's capacity to stabilize and recover from a catastrophic event; bolstering information sharing and building unity of effort and common strategic understanding among the emergency management team; building plans and providing training to our homeland security partners; and promoting preparedness within the private sector. Below are a few initiatives that advance our efforts to achieve our resilience goals.

National Preparedness Goal

The National Preparedness Goal envisions a secure and resilient Nation 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. The National Preparedness Report documented the areas of national strength in planning, operational coordination, intelligence and information sharing, and operational communications. The Nation achieved gains in cybersecurity, recovery, and the integration of individuals with disabilities and access and functional needs, but challenges remain. FEMA will publish the Federal Interagency Operational Plans in FY 2014, which define in depth the objectives, roles, and responsibilities of the federal agency stakeholders in the National Preparedness System: Prevention, Protection, Mitigation, Response, and Recovery.

Disaster Resilience Planning

Ensuring resilience to disasters by strengthening disaster preparedness and response capabilities is critical to the Nation's success. FEMA has worked to develop THIRA, which creates a common approach for states and territories to identify and assess risk, document their associated impacts, and set capability targets. The ability of states to complete a THIRA is a central tenet of DHS's FY 2012 -2013 Agency Priority Goal (APG) on resilience. FEMA will continue to mature the THIRA process and the APG to increase understanding of capability needs in the Nation and to assess and measure improvements in preparedness over the next two years.

Flood Insurance Reform

With the enactment of the *Biggert Waters Flood Insurance Reform Act* in 2012, DHS has taken steps to increase the financial stability of the National Flood Insurance Program. Changes to flood insurance and floodplain management will be phased in over time, beginning this past year. Reforms will eliminate some artificially low insurance rates and subsidies in order to reflect more accurately the risk and costs of flooding. In order to mitigate the costs of these reforms, DHS has, and will continue to help communities lower flood insurance premiums and potential recovery costs through remodeling and rebuilding homes and buildings to be more resilient to flood damage and taking community-wide mitigation steps to lower flood risk.

National Disaster Recovery Framework

The National Disaster Recovery Framework establishes an organization of Recovery Support Functions (RSFs) to promote more effective recovery efforts by federal agencies before and after disaster strikes. The objective of the RSFs is to facilitate the identification, coordination, and delivery of federal assistance needed to supplement recovery resources and efforts by local, state and tribal governments, as well as private and nonprofit sectors for: Community Planning and

Capacity Building (DHS/FEMA); Economic (Department of Commerce); Health and Social Services (Department of Health and Human Services); Housing (Department of Housing and Urban Development); Infrastructure Systems (Department of Defense, U.S. Army Corps of Engineers); and Natural and Cultural (Department of the Interior).

Sandy Recovery Improvement Act
In January 2013, President Obama signed the *Sandy Recovery Improvement Act of 2013* (SRIA) into law, the most significant piece of legislation impacting FEMA since the Post-Katrina *Emergency Management Reform Act of 2006*. Several of the key SRIA provisions provide alternatives to recovery efforts from which applicants may choose the best option for their particular recovery. SRIA mandates that these alternatives must reduce the costs to the Federal Government of providing disaster assistance, increase the flexibility in the administration of such assistance, expedite the provision of such assistance, and provide financial incentives for the timely and cost-effective completion of projects with such assistance.

Focus Area: 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.

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 mission and post-conflict reconstruction and stabilization

Ensuring Effective Emergency Response: The U.S. Coast Guard is *"Always Ready"*

In the wake of Hurricane Sandy, USCG's talented responders coordinated with state and local governments, and private industry stakeholders, to save lives, protect the environment and help restore normal operations. The core principles of contingency preparedness and emergency management helped the USCG effectively manage hundreds of incidents following the storm, some of which are highlighted below:

1) Search and Rescue – Offshore, southeast of Cape Hatteras, North Carolina, the crew of the Bounty hailed USCG for assistance and was forced to abandon their sinking ship. USCG arrived to the scene of the sinking ship with aircraft and cutters, saving 14 of the 16 crew members with two MH-60 helicopters. **2) Marine Environmental Response and Contingency Preparedness** – Closer inland, USCG partnered with the Environmental Protection Agency, and the New York Department of Environmental Conservation to improve situational awareness, command and control, and optimize environmental recovery efforts. USCG deployed specialized strike teams and helped direct a systematic canvassing of affected coastal and port areas for pollution, damage assessments, and tailored environmental response activities while supporting the pumping and power-restoration efforts in New York's tunnels and subways restoring daily transportation services for millions of commuters. **3) Aids to Navigation** – Both at sea and ashore, USCG conducted port assessments, responded to channel marker discrepancies and verified waterway safety to restore the flow of commerce and emergency services.

Percent of import revenue successfully collected (CBP)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	99.12%	98.88%	100%	98.73%

This measure estimates the collected duties, taxes, and fees expressed as a percent of all collectable revenue due from commercial imports to the United States directed by trade laws, regulations, and agreements. Consistent with previous years, CBP collected 98.73 percent of import revenue in FY 2013. Nearly half the revenue gap is attributable to our Far East trading partners and CBP will continue to apply 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.

Five-year average number of commercial and recreational boating deaths and injuries (USCG)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
---	---	4,567	4,469	≤ 4,546	4,241

This measure is an indicator of the long-term trend of USCG Maritime Prevention Program's impact on marine safety. USCG works diligently to ensure our waterways are safe for both commercial and recreational purposes. FY 2013 results are significantly lower than FY 2012 and show a steady downwards trend from FY 2011.

Availability of maritime navigation aids (USCG)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
98%	98.5%	98.5%	98.3%	97.5%	98.2%

This measure indicates the hours that short-range federal aids to navigation are available. The U.S. Aids to Navigation System is a system maintained by USCG, consisting of visual, audible, and electronic signals which are designed to assist the prudent mariner in the process of navigation. They establish a consistent way to navigate safely and avoid collisions when two boats are crossing paths, are on course to meet head-on, or when one boat wishes to overtake another. USCG continued its long-term success in mainlining aids to navigation achieving 98.2 percent availability in FY 2013.

Number of federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation process (FLETC)					
FY09 Result	FY10 Result	FY11 Result	FY12 Result	FY13 Target	FY13 Result
50	52	66	83	99	97

The Federal Law Enforcement Training Accreditation (FLETA) Board is the accrediting body for all federal law enforcement training and support programs. The accreditation ensures that training and services provided meet professional training standards for law enforcement. Through FY 2013, 97 federal law enforcement training programs and/or academies have been accredited or re-accredited narrowly missing the FY 2013 target. As a testament to the FLETA process and standards, two planned programs were not awarded accreditation because these programs did not meet all of the FLETA standards. Because FLETA accreditation is a voluntary government-wide process, the agency owning these programs will have to decide if the agency wishes to re-submit applications and begin the accreditation process again.

FLETC Saves Lives via a Research Based Approach: Lessons Learned/Lessons Anticipated

FLETC's mission is "We train those who protect our homeland." To carry out this mission, the Lessons Learned / Lessons Anticipated (LL/LA) working group has adopted a research based approach to target serious issues confronting law enforcement officers. Research efforts this past year have focused on the topic of distracted driving which is a contributing factor in taking officer lives, and the unique situation of mistaken identity shooting of plain clothes officers. Several factors have been identified in each area and FLETC has developed training to mitigate these factors and save officer lives.

One of the leading causes of officer fatalities is vehicle crashes and one of its contributing factors is distracted driving. FLETC's distracted driving initiative is intended to create a keen awareness of the dangers associated with law enforcement job related distractions. Currently, the Distracted Driving program has been presented to 537 members of federal, state, local, and rural law enforcement agencies, with higher numbers expected to be reached in the coming year. Another area that has needlessly taken officer lives is that of mistaken identity. Plain clothes officers responding to a call occasionally creates a situation termed "police-on-police" shooting. FLETC has been leading an effort to reduce the number of shootings through collaboration with state and local law enforcement agencies, review of existing research, surveying law enforcement organizations for policies and procedures, performing novel testing on police identification systems and conducting scenario based performance tests. The LL/LA group will continue to identify and research issues that contribute to the success and survival of the Nation's men and women in law enforcement.

__Looking Forward__

Homeland security is an integral element of broader U.S. national security and domestic policy. It is not, however, the only element. The *National Security Strategy* clearly identifies national defense and economic security as other elements—along with homeland security—of overall U.S. national security. DHS leads and supports many activities that provide essential support to national and economic security while fulfilling its homeland security missions. Below are a few initiatives that advance our efforts to achieve our support to national and economic security goals.

__USCG Recapitalization__
USCG's authorities, capabilities, and partnerships coupled with its fleet of cutters, aircraft, and boats executed in a layered operational approach, achieves effective safety, security, and stewardship throughout the entire maritime continuum from overseas to the critical ports within our homeland. USCG uses these authorities and assets to accomplish its statutory missions, providing the resiliency and capability to serve as the Nation's maritime first responder, as well as adapt quickly to meet ever changing threats in the maritime domain. USCG recapitalization is intended to provide a fleet of assets that will enable the Coast Guard to replace its fleet of aging cutters, boats, and aircraft, while also addressing mission requirements.

__CBP's Single Transaction Bond Policy__
A single transaction bond (STB) is an insurance policy that guarantees duty, taxes, and fee payment to CBP by an importer for a single shipment (versus a continuous transaction bond that covers all shipments for an importer in a given year). CBP will implement the OIG report recommendations in "*Efficacy of Customs and Border Protection's Bonding Process*," (OIG-11-92) and significantly increase controls and promote a more consistent and effective method for determining and applying STBs. This will help CBP and DHS to maximize collection of customs revenue that support other government programs.

This enhanced implementation of the STB policy will accomplish two key initiatives in FY 2014. First, CBP will have a centralized office to oversee and administer the STB program. This encompasses bond administration, which may include proper bond completion to promote enforceability of the bond against the filer and third party, modernizing and maintaining application procedures, and establishing required minimum bond amounts to be validated and enforced by the ports. Second, the new centralized staffing model will be accompanied by the development of an automated bond application that serves as a platform through which Sureties can file STBs. This application will be designed to improve filing, management, enforcement, and reporting of STBs to address those issues identified in OIG-11-92.

Focus Area: 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.

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

Cornerstone Leader Development Program

Former Secretary Janet Napolitano established the Leader Development Program in May 2010 under the leadership of the Office of the Chief Human Capital Officer (OCHCO) in order to elevate leader effectiveness across DHS, as an investment in mission achievement. OCHCO led a cross-Component development effort resulting in the Leader Development Framework, which identifies a set of DHS-specific Leader Development competencies, and a roadmap of ideal development elements at five tiers of leadership (from Team Member to Executive). The Cornerstone Program, the first and most pivotal Framework tier to be built-out and deployed, sets specific, consistent baseline development requirements for new and seasoned supervisors, managers, and executives at all levels across the Department.

To promote efficient, effective, and collaborative investment across the Department while still supporting Component-specific mission-focused flexibilities, Components are encouraged to optimize current investments by using existing high-quality products to meet the requirements where possible, and supplementing with new, shared, or collaboratively-developed products to offer full-scale development that meets and exceeds the continuum of Cornerstone requirements. Cornerstone includes multiple learning modalities and best-practices such as a suite of onboarding activities for all new DHS supervisors, a Fundamentals of DHS Leadership program offering skill-building in 18 topic areas essential to DHS leadership, and an innovative 2-pronged annual Continuous Supervisory Leader Development requirement for all seasoned supervisors targeting critical competency development for self and investing in others.

During an initial FY 2012 pilot implementation targeting one vital sector of the leadership population, Components reported that 90 percent of first-line supervisors completed a quality training experience under the Cornerstone Program. In FY 2013, the first year of broader implementation, 75 percent of responders agreed that the Cornerstone activity they completed provided knowledge or skills that they had not learned on the job, demonstrating the value of formalized development. In FY 2014, collaborative cross-Component efforts will continue to develop additional Leader Development Framework tiers including Team Member, Team Lead, and an Executive Capstone program, in order to institutionalize a system of leadership talent development at all levels of the workforce, now and into the future.

Looking Forward

Maturing and strengthening DHS and the entire homeland security enterprise—the collective efforts and shared responsibilities of federal, state, local, tribal and 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. Below are a few areas that advance our efforts to mature and strengthen the Department.

Financial Stewardship

Since its inception in 2003, the Department has been diligently working to strengthen financial management to produce timely, reliable financial information. Through the development and implementation of policies, procedures, and internal controls, the Department has been able to achieve substantial progress in ensuring the efficient and effective use of the Department resources and stewardship of taxpayer dollars.

As in FY 2012, all five financial statements were audited in FY 2013. We continued to execute our strategy of targeted risk assessment and strong oversight of corrective actions, ultimately earning an unmodified audit opinion on all five financial statements. Also in FY 2013, the Department was able to provide reasonable assurance that its internal controls over financial reporting are effective, with the exception of four material weaknesses identified in the Acting Secretary's Assurance Statement.

The Department continues working toward our audit goals for FY 2014 and beyond, to include obtaining an unqualified audit opinion of internal controls over financial reporting, and modernizing our financial systems.

DHS will continue to implement a risk-based approach to audit remediation, working closely with Components to mitigate any risk of new material weaknesses or audit qualifications and to sustain prior-year successes. The Department will monitor critical corrective action milestones to ensure they are completed on schedule and assist Components with implementation efforts to remediate and downgrade the severity of internal control deficiencies.

As part of the financial systems modernization (FSM) initiative, the Department is focusing on:

- Improving financial systems for Components with the greatest need;
- Expanding business intelligence capabilities to deliver DHS-wide financial data to leadership to support decision-making;
- Standardizing processes to support internal controls, improve and sustain audit success, and provide governance and oversight of current and future financial management system enhancements; and
- Implementing a Department-wide standard accounting classification structure that aligns with the Department of Treasury's Bureau of Fiscal Service Accounting Data Standards data model.

Consistent with the Office of Management and Budget's "Shared First" initiative, DHS will use shared service providers where possible, rather than continuing to make costly capital investments in duplicative accounting systems. This approach is designed to eliminate duplication and allows

DHS to leverage well-defined financial business enterprise architecture standards to close performance gaps and facilitate decision making.

Integrated Investment Life Cycle Management
Integrated Investment Life Cycle Management (IILCM) is a transformational concept to integrate all phases of the Department's $60 billion budget and investment management process. The framework provides critical linkages between Strategy, Capabilities and Requirements, Programming and Budgeting, and Investment Oversight phases to ensure the effective execution of federal funds to support strategic priorities. Through this model, senior-level decision makers will be brought together in common portfolio teams commissioned by the Secretary. They will be composed of stakeholders from all directorates, Components, and offices within DHS to prioritize, align, and measure progress of investments throughout the planning, programming and execution phases to assess progress against mission needs.

In February 2013, former Secretary Janet Napolitano signed Policy Directive 259-00 establishing IILCM as the department-wide framework to guide executive management of critical investments. The Secretary also identified three portfolios—Common Vetting, Bio-Defense, and Cybersecurity—to pilot elements of IILCM to inform a portion of the FY 2015 budget cycle. These pilots are part of a five-part action plan being executed by the IILCM Executive Steering Committee, chaired by the Under Secretary for Management, to adapt and codify the IILCM framework.

Workforce Initiatives
OCHCO continued to strengthen the human capital line-of-business throughout FY 2013 building on our goals of: 1) build an effective, mission-focused, diverse, and inspiring cadre of leaders; 2) recruit and build a highly qualified and diverse workforce; 3) retain an engaged workforce; and 4) solidify a unified DHS culture of mission performance, adaptability, accountability, equity, and results through linking overall priorities, strategy, risk and investments. Moving forward, OCHCO will: begin training the senior executive service (SES) workforce on the new Federal Government-wide SES Performance Management System; develop workforce plans for select DHS priority mission critical occupations by implementing the recently updated DHS Workforce Planning Guide; continue to seek cost-effective ways to develop employees and expand on the Department-wide rollout of the Homeland Security Rotation Program and the DHS HQ mentoring program; and will refine a human capital dashboard to improve data availability and reliability and analyze information requests to improve responsiveness and decision-making. In addition, OCHCO will develop new approaches to strengthen the human resources workforce; develop a five year project implementation plan that aligns with the approved 2012 Human Resource Information Technology strategic plan; enhance data management across the human capital enterprise; and ensure that human resource specialists are trained in specialty areas.

Financial Overview

DHS's budgetary resources were approximately $95.1 billion for FY 2013, about $15.6 billion more than in FY 2012. 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. Budgetary accounting principles require recognition of the obligation of funds according to legal requirements, which in many cases occurs prior to the occurrence of a transaction under accrual basis. The recognition of budgetary accounting transactions is essential for compliance with legal constraints and controls over the use of federal funds. 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.
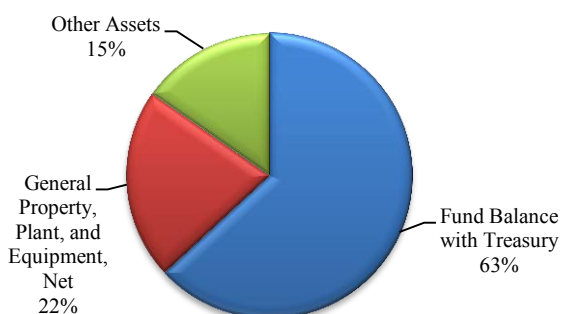
Assets – What We Own and Manage

Assets represent amounts owned or managed by DHS that can be used to accomplish its mission. At September 30, 2013, DHS had $92 billion in assets, representing a $5 billion increase from FY 2012.

Fund Balance with Treasury (FBwT), the Department's largest asset, comprises 63 percent of the total assets. Included in FBwT is the remaining balance of DHS's unspent prior-year budgets plus miscellaneous receipts. While the Department sustained sequester and across-the-board rescissions at CBP, ICE, and TSA, FBwT increased approximately $4 billion in FY 2013 because of additional funding appropriated for the Hurricane Sandy relief efforts, as well as increased funding for Cyber Security.

Total Assets

As of September 30 (in Millions)	FY 2013	FY 2012
Fund Balance with Treasury	$ 58,002	$ 53,875
General Property, Plant, and Equipment, Net	19,878	19,853
Other Assets	14,022	12,790
Total Assets	$ 91,902	$ 86,518

Property, Plant, and Equipment (PP&E) is the second largest asset, comprising 22 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 at cost, and depreciated over the estimated useful life of the asset. PP&E is presented net of accumulated depreciation.
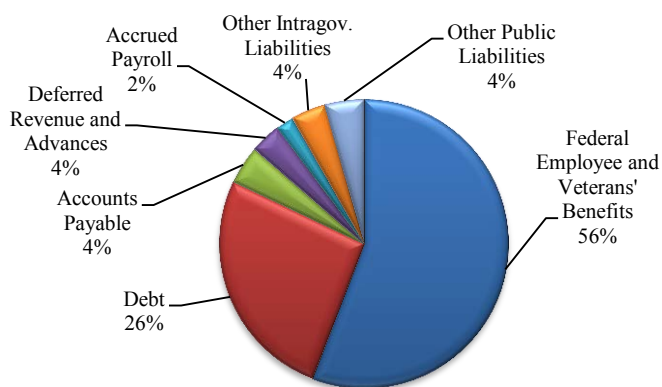
Other Assets represents 15 percent of total assets, and includes investments, accounts receivable, cash and other monetary assets, taxes, duties and trade receivables, direct loans, inventory and related property, and other. The $1 billion increase in Other Assets is primarily attributable to the establishment of accounts receivable for two significant judgments assessed for the Deepwater Horizon oil spill and to an escalation in investments due to increased fines and penalties for the Oil Spill Liability Trust Fund. For more information, see Note 22 in the Financial Information section.

Liabilities – What We Owe

At September 30, 2013, DHS reported approximately $92 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 2013	FY 2012
Federal Employee and Veterans' Benefits	$ 51,223	$ 51,953
Debt	24,076	18,072
Accounts Payable	3,923	3,890
Deferred Revenue and Advances	3,180	2,845
Accrued Payroll	1,807	2,454
Other Intragovernmental Liabilities	3,558	3,628
Other Public Liabilities	3,986	4,529
Total Liabilities	$ 91,753	$ 87,371

DHS's largest liability is for *Federal Employee and Veterans' Benefits*, representing 56 percent of total liabilities. This liability decreased approximately $1 billion from FY 2012. 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. For more information, see Note 16 in the Financial Information section. 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).

Debt is DHS's second-largest liability, representing 26 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 $6 billion from FY 2012 due to additional borrowing required to cover insurance claim payments as a result of Hurricane Sandy. 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.

Accounts Payable, representing 4 percent of total liabilities, includes amounts owed to other federal agencies and the public for goods and services received by the Department.

Deferred Revenue and Advances represents amounts received by the Department for goods or services that have not been fully rendered, which are 4 percent of total liabilities. The $335 million increase in Deferred Revenue in FY 2013 is due to a higher volume of cases processed by USCIS. The increase also reflects funding received from the State of Kansas to support construction of the National Bio and Agro-Defense Facility located in that state.

Accrued Payroll includes unpaid wages and benefits for current DHS employees, and represents 2 percent of total liabilities. Accrued Payroll decreased by $647 million in FY 2013 due to fewer payroll days accrued than in FY 2012.

Other Intragovernmental Liabilities, comprising 4 percent of the Department's liabilities, includes amounts due to the Treasury's general fund, and other. *Other Public Liabilities* includes insurance liabilities, environmental liabilities, refunds and drawbacks, and other, and represents 4 percent of total liabilities. The decrease of $543 million in Other Public Liabilities occurred primarily due to actuarial estimates for claims losses and loss reserves going down at FEMA, and from a decrease in contingent liabilities.

Statement of Net Cost

Net Cost of Operations represents the difference between the costs incurred and revenue earned by DHS programs. The Statement of Net Cost groups the five missions and two focus areas described in the DHS Strategic Plan into four major missions to allow 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 1.B, Basis of Presentation, shows the relationship between the Department's five missions and two focus areas in the DHS Strategic Plan and the major missions presented in the Statements of Net Cost and related footnotes.

Fostering a Safe and Secure Homeland, includes Strategic Plan Missions 1, 2, and 4, *Preventing Terrorism and Enhancing Security, Securing and*

Total Net Cost of Operations

For the Year Ended September 30 (in Millions)	FY 2013	FY 2012
Fostering a Safe and Secure Homeland	$ 26,264	$ 25,840
Ensuring Resilience to Disasters	22,682	9,419
Providing Essential Support to National, Economic, and Homeland Security	8,728	8,970
Enforcing and Administering Our Immigration Laws	5,277	5,329
Net Cost Before (Gain)/Loss	$ 62,951	$ 49,558
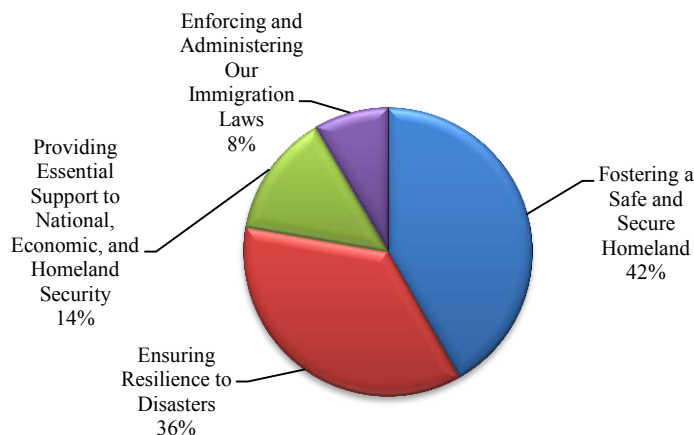
Managing Our Borders, and *Safeguarding and Securing Cyberspace, respectively.* This major mission involves the security and prevention aspects of the DHS Strategic Plan, representing 42 percent of the Department's net cost. *Ensuring Resilience to Disasters* is Mission 5 of the strategic plan and represents 36 percent of total net costs. *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 14 percent of the Department's net cost. *Enforcing and Administering Our Immigration Laws* is Mission 3 of the strategic plan and represents 8 percent of total net costs. Note 23 in the Financial Information section shows costs by responsibility segment aligned to the major missions.

The net cost of Ensuring Resilience to Disasters increased by $13.3 billion in FY 2013 because of Hurricane Sandy relief and recovery efforts.

During FY 2013, the Department earned approximately $11.2 billion in revenue; this is a decrease of about $381 million from $11.6 billion as of September 30, 2012. Revenue decreased primarily because USCG Oil Spill Trust Fund earnings declined in FY 2013. Additionally, FEMA's agreement with the Department of Commerce to support to Public Safety Interoperable Communications under the Digital Television Transition and Public Safety Act of 2005 ended, resulting in FEMA earning less revenue in FY 2013.

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 or Statement of Changes in Net Position, rather than the Statement of Net Cost.
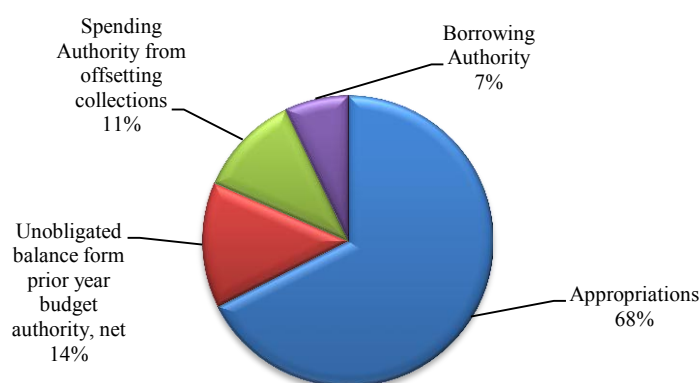
Statement of Changes in Net Position

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 in the section above as well as transfers to other agencies decrease net position. Total net position increased in FY 2013 by approximately $1 billion. This increase is primarily due to a significant increase in appropriations received at FEMA for relief efforts related to Hurricane Sandy.

Statement of Budgetary Resources

This statement provides information on the status of the approximately $95.1 billion in budgetary resources available to DHS during FY 2013. The authority was derived from appropriations of $64.2 billion, $13.3 billion in authority carried forward from FY 2012, $10.9 billion in collections, and $6.7 billion of borrowing authority. The total amount of resources available increased by approximately $15.6 billion from FY 2012. The change is primarily due to substantial increases in FEMA's appropriations and borrowing authority for Hurricane Sandy relief and recovery efforts.

Of the total budget authority available, DHS incurred a total of $76.6 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, 2013, $18.5 billion of the $95.1 billion was not yet obligated. The $18.5 billion represents $14.9 billion in apportioned funds available for future use, and $3.6 billion in unapportioned funds.

Budgetary Resources by Authority Type

For the Year Ended September 30 (in Millions)	FY 2013	FY 2012
Appropriations	$ 64,245	$ 55,399
Unobligated Balance from Prior Budget Authority	13,251	14,029
Spending Authority from Offsetting Collections	10,854	10,028
Borrowing Authority	6,705	47
Total Budgetary Resources	$ 95,055	$ 79,503

Spending Authority from offsetting collections 11%
Borrowing Authority 7%
Unobligated balance form prior year budget authority, net 14%
Appropriations 68%

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 transferred to Treasury's General Fund and other federal agencies. Total cash collections increased by approximately $1 billion in FY 2013 due primarily to increased importing activity and duties collections.

Stewardship Assets and Investments

DHS's stewardship assets primarily consist of USCG 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

USCG has over 500 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 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 for federal agencies and the formats prescribed by the Office of Management and Budget, 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 Information section for *Prompt Payment Act* and *Debt Collection Improvement Act* 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 and Budget revised 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. In FY 2012, DHS controls and financial management continued to improve such that DHS achieved its first qualified opinion on its full set of financial statements. Additionally, DHS was able to report a qualified reasonable assurance over internal controls over financial reporting. This year DHS achieved an unmodified 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), Risk Management and Assurance (RM&A) Division, 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 RM&A Division 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 and overseen by RM&A, 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 OIG and GAO.

Secretary's Assurance Statement

December 11, 2013

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.
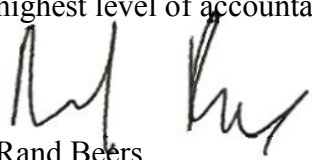
In accordance with the *Federal Managers' Financial Integrity Act* (FMFIA) and the *Department of Homeland Security Financial Accountability Act,* I have directed an evaluation of internal control at the DHS in effect during the Fiscal Year (FY) ending September 30, 2013. This evaluation was conducted 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.

The Department has completed its FY 2013 evaluation of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with 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, 2013, with the exception of three business processes—Financial Reporting; Property, Plant, and Equipment; and Budgetary Accounting—and Information Technology Controls and Systems Functionality, where material weaknesses have been identified and remediation is in process, as further described in the Other Information Section. 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 its efforts to ensure that management control systems are in place to achieve the mission of the Department.

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 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 2013 full scope audit and its resulting unmodified opinion on the Department's financial statements represents a major milestone for DHS management.

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.

Rand Beers
Acting Secretary

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 Office of the CFO 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.

Appendix D to Circular No. A-123 defines new requirements effective in FY 2014 for determining compliance with the FFMIA. The goal of this Appendix is to transform our compliance framework so that it will contribute to efforts to reduce the cost, risk, and complexity of financial system modernizations. The objective of this approach will be to provide additional flexibility for federal agencies to initiate smaller-scale financial modernizations as long as relevant financial management outcomes (e.g., clean audits, proper controls, timely reporting) are maintained.

In accordance with OMB guidance, DHS is executing incremental Component-level financial system modernization projects in order to deliver functionality faster and reduce risks often associated with large, complex Information Technology (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 FSM 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 has adopted a decentralized strategy and will modernize individual Component financial systems, as needed. This incremental approach is consistent with OMB guidance and will allow DHS to leverage existing shared service providers' proven systems and processes in concert with DHS-wide policy and standards for implementations, instead of making costly investments in new systems. DHS will work to ensure programs are planned and executed to meet reporting requirements, minimize costs for financial operations, improve compliance with financial management standards such as FFMIA, and make certain that financial management systems have management controls in place to support the DHS mission. DHS plans to continue forward by executing the financial system modernization activities as described in the Playbook. Specific goals for FY 2014 include continuing to work with Components on FSM efforts with a focus on DNDO, TSA, USCG, ICE, and ICE customers, as well as, FLETC. DNDO, TSA, and USCG will complete a Discovery Phase with Department of Interior's Interior Business Center to determine suitability as the service provider and feasibility of implementation. FLETC will complete a technical refresh of their financial management system.

The DHS financial systems modernization concept is to streamline and adjust its IT financial portfolio so that the DHS CFO and Components have the flexibility to be able to meet their mission and the changing demands for financial visibility and accountability. Financial systems modernization requires having an intelligent transition plan for each system and financial management capability. As part of the decentralized approach, DHS Components are conducting Alternatives Analysis prior to moving forward with their financial system modernization efforts. Through the FSM initiative, DHS is working to improve existing financial systems to better meet FFMIA requirements. Components considering a shared service provider for their financial management system modernization will consult OMB A-123, Appendix D which is effective as of FY 2014 for the minimum requirements an external provider must demonstrate including FFMIA requirements.

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 2013 Federal Information Security Management Act Report and Privacy Management Report consolidate reports from three DHS offices: Chief Information Officer (CIO) / Chief Information Security Officer (CISO); Office of 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 2013. For example, the CISO:

- Implemented a pilot program to migrate the Department from a stagnant paperwork driven security awareness process (i.e. security controls are tested and documentation is updated at fixed intervals) to a dynamic framework that can provide authorization officials access to security related information on demand (e.g., frequent updates to security plans, security assessment reports, hardware and software inventories) to make risk-based authorization decisions.

- Revised the information security scorecard to provide greater focus on risk management and continuous processes. Specifically, the information security scorecard was divided into two key areas: 1) Continuous Diagnostics and 2) Migration and Security Processes.

- Developed and implemented *The Fiscal Year 2013 Information Security Performance Plan*, which defines the Department's information security program performance requirements, priorities, and overall goals throughout the year.

- Drafted an ongoing authorization methodology to help improve the security of the Department's information systems through a new risk management approach.

- Strengthened IT security to address the Administration's Cybersecurity priority by implementing trusted Internet connections, and performing continuous monitoring and strong authentication over DHS's information systems.

- 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 National Institutes of Standards and Technology guidance.

The OIG report, *Evaluation of DHS' Information Security Program for Fiscal Year 2013*, identified five recommendations for information security improvements. The CISO concurred with the recommendations and corrective actions are already underway to address each by the end of FY 2014.