



U.S. Department of Homeland Security Annual Financial Report

Fiscal Year 2011



Homeland
Security

Our Vision

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

About this Report

The *U.S. Department of Homeland Security Annual Financial Report for Fiscal Year (FY) 2011* 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 2011, the Department is using the alternative approach—as identified in the Office of Management and Budget's Circular A-136—to produce its Performance and Accountability Reports, which consists of the following three reports:

- ***DHS Annual Financial Report:*** Publication date – November 11, 2011.
- ***DHS Annual Performance Report:*** Publication date – February 6, 2012. The *DHS Annual Performance Report* is submitted with the Department's Congressional Budget Justification.
- ***DHS Summary of Performance and Financial Information:*** Publication date – February 15, 2012.

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

For more information, contact:

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

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



**Homeland
Security**



Table of Contents

Message from the Secretary2

Management’s Discussion and Analysis.....5

 Mission and Organization.....6

 Implementing 9/11 Commission Recommendations – Executive Summary7

 Performance Overview11

 Financial Overview27

 Management Assurances33

Secretary’s Assurance Statement.....34

Financial Information37

 Message from the Deputy Chief Financial Officer38

 Introduction40

 Financial Statements.....41

Balance Sheets.....41

Statements of Net Cost.....43

Statements of Changes in Net Position.....45

Statements of Budgetary Resources.....47

Statements of Custodial Activity.....49

 Notes to the Financial Statements50

 Required Supplementary Stewardship Information119

 Required Supplementary Information124

 Independent Auditors’ Report132

Other Accompanying Information183

 Tax Burden/Tax Gap184

 Summary of Financial Statement Audit and Management Assurances185

 Improper Payments Information Act.....193

 Other Key Regulatory Requirements212

 Major Management Challenges Facing the Department of Homeland Security.....213

Management’s Response246

Acronym List270

Message from the Secretary

November 11, 2011



I am pleased to submit the Department of Homeland Security's (DHS) Annual Financial Report for Fiscal Year (FY) 2011. This report provides an assessment of the Department's detailed financial information and our stewardship of taxpayer resources in support of our mission of securing the United States. This report also outlines our major goals and priorities within the framework of the Quadrennial Homeland Security Review (QHSR) and the Bottom-Up Review (BUR).

In each mission area identified in the QHSR, we have continued to grow and mature as a department by strengthening our existing capabilities, building new ones where necessary, enhancing our partnerships across all levels of government and with the private sector, and streamlining our operations and increasing efficiency.

Eight years since the Department's creation and ten years after the September 11, 2001 terrorist attacks, the results are clear: 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 evolving threats we face.

Priority Areas

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

Preventing Terrorism and Enhancing Security

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



Securing and Managing Our Borders

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

Enforcing and Administering Our Immigration Laws

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

Safeguarding and Securing Cyberspace

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

Ensuring Resilience to Disasters

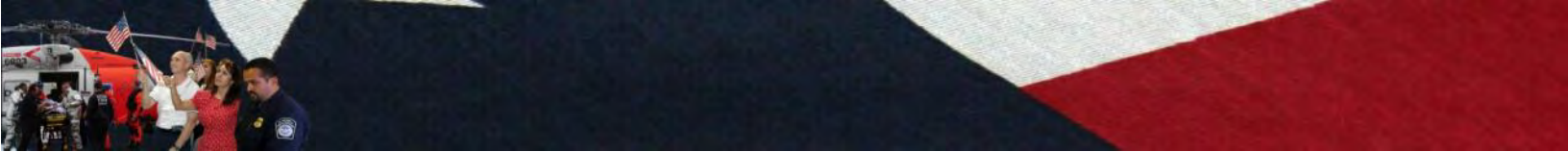
DHS provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready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

Providing Essential Support to National and Economic Security

DHS leads and supports many activities that provide essential support to national and economic security, including, but not limited to: maximizing collection of customs revenue; protecting the financial services sector; maintaining the safety and security of the marine transportation system; preventing the exploitation of children; providing law enforcement training; and coordinating the Federal Government's response to global intellectual property theft. DHS contributes in many ways to these elements of broader U.S. national and economic security while fulfilling its other five homeland security missions.

Maturing and Strengthening the Department

Over the past three years, we have led the development and implementation of a comprehensive, strategic management approach focused on maturing organizational effectiveness within the Department. The QHSR, BUR, and ongoing initiatives under the Secretary's Efficiency Review highlight the Department's steps taken towards greater unification and integration. Since its launch



in March 2009, the DHS Efficiency Review program has implemented 36 separate initiatives to achieve these aims while also promoting greater accountability, transparency, and customer satisfaction. The Efficiency Review has led to improvements in how the Department manages its resources in several areas, including its physical assets and support of its workforce, as well as the day-to-day expenditures required to do business. Additionally, we are continuing our investment and commitment to the Acquisition Workforce—investing in our employees through workforce training and integrated professional and leadership development—and are making significant investments in data center consolidation.

This report highlights the Department’s activities and accomplishments in each of these mission areas in FY 2011 and discusses upcoming initiatives that will build on these efforts to achieve a safer and more secure nation.

Management Assurances and Performance Measurement

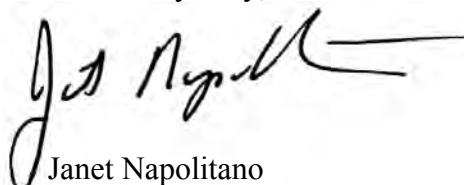
Pursuant to the *Department of Homeland Security Financial Accountability Act*, in FY 2011, the Department focused its efforts on eliminating audit qualifications and executing corrective actions to strengthen Department-wide internal controls over financial reporting. As I wrote last year, we concentrated our efforts on obtaining an audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity by FY 2011, and I am pleased that we have accomplished this goal thanks to the hard work of many dedicated men and women across the Department.

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. Most notably, improvements made by the U.S. Coast Guard and other components increased the Department’s auditable balance sheet balances to approximately 90 percent in FY 2011, allowing the Department to attain a qualified opinion on the balance sheet this year.

Over the past three years, DHS has committed to improving performance measurement and accountability, and I am able to provide assurance that the performance measures reported for the Department are complete and reliable, with the exception of one measure identified in the forthcoming Annual Performance Report. The program office is working to resolve its data collection process for the measure and will report reliable information in FY 2012. DHS’s performance and accountability reports for this and previous years are available on our public website: http://www.dhs.gov/xabout/budget/editorial_0430.shtm.

The men and women of the Department of Homeland Security remain focused on achieving our objectives in the coming year while continuing to be responsible stewards of taxpayer resources. I am proud of the significant improvements to the Department’s financial management systems we have made to date, and I look forward to the progress we will continue to make in the coming years.

Yours very truly,



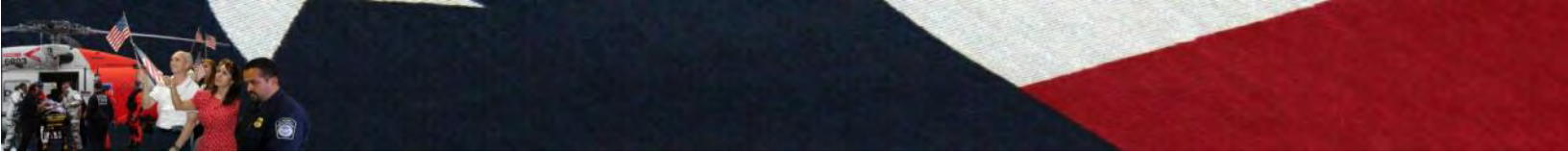
Janet Napolitano



Management's Discussion and Analysis

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

See *inside front cover* for a description of the DHS approach to performance and accountability reporting.



Mission and Organization

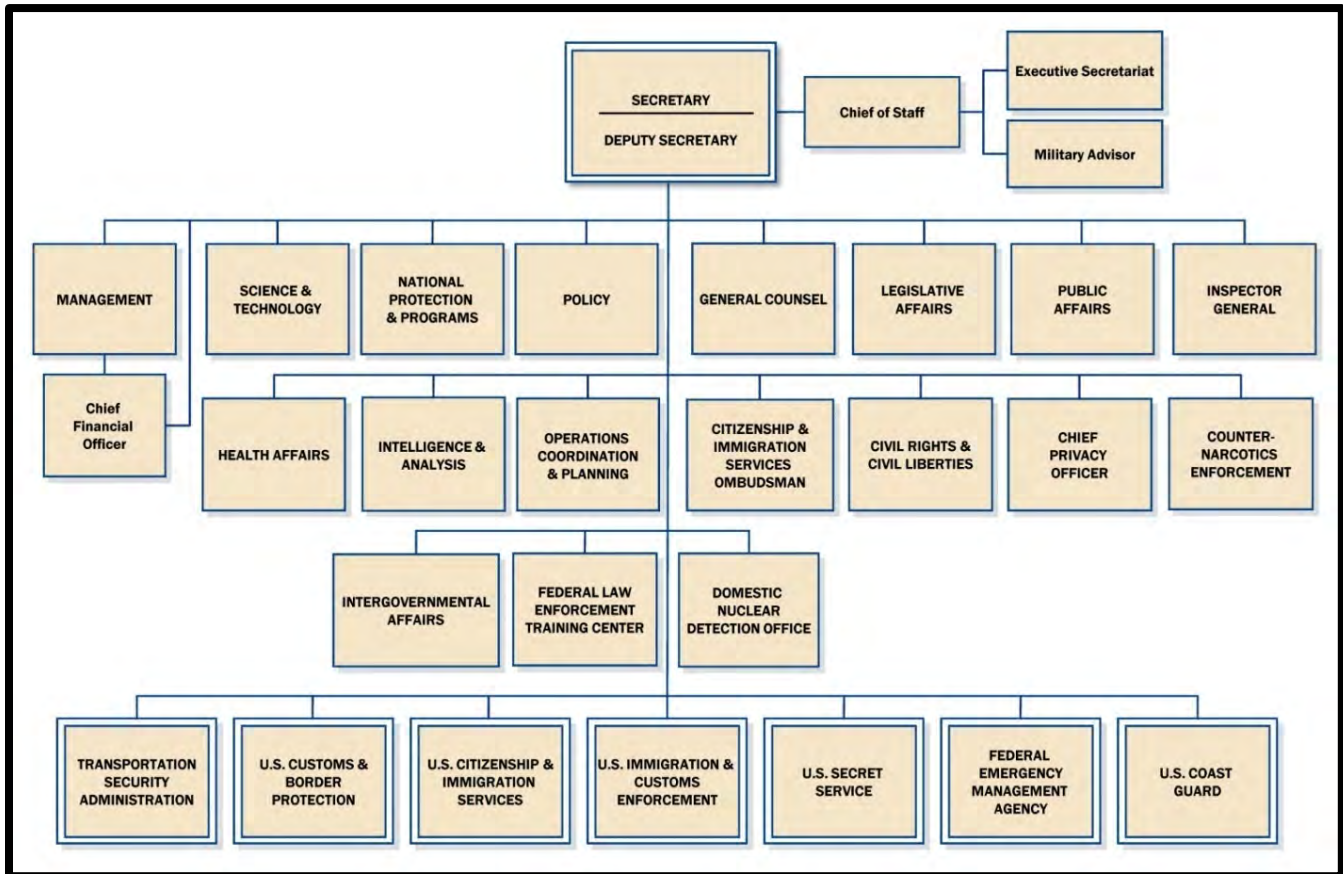
Mission

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 the Department of Homeland Security and the homeland security enterprise.

Our Organization

The Department of Homeland Security’s seven Operational Components, listed along the bottom of the chart below, lead the Department’s operational activities to protect our Nation. The remaining Components of the Department 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/xabout/structure>.

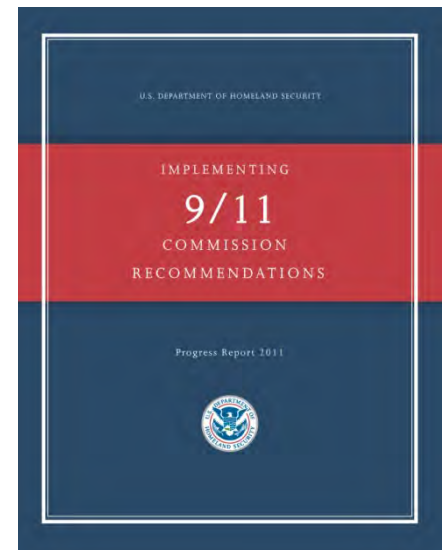
Figure 1. DHS Organization Chart





Implementing 9/11 Commission Recommendations – Executive Summary

Seven years after the release of the 9/11 Commission report and in recognition of the tenth anniversary of the September 11, 2001 terrorist attacks, DHS released a report in July 2011 highlighting the significant progress that the Department, along with its many partners, has made in fulfilling specific recommendations by the 9/11 Commission to build a country that is stronger, safer, and more resilient. The full report, *Implementing 9/11 Commission Recommendations*, can be found at: <http://www.dhs.gov/files/publications/implementing-9-11-commission-recommendations.shtm>.



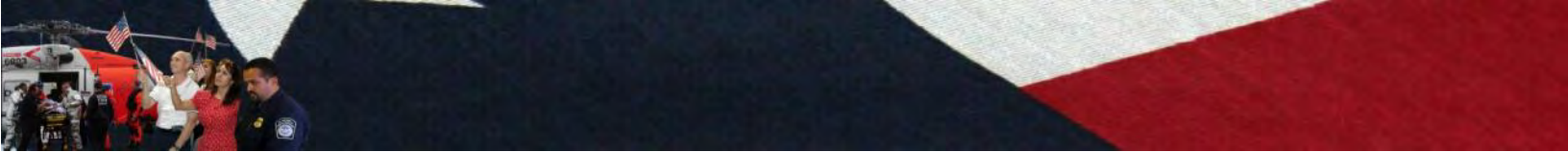
Overview

The United States has made significant progress in securing the Nation from terrorism since the September 11, 2001, attacks. Nevertheless, work remains, as the terrorist threats facing the country have evolved in the last ten years, and continue to change.

Following 9/11, the Federal Government moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, and local capabilities to prepare for, respond to, and recover from threats and disasters at home. A key element of this framework included the creation of DHS in March 2003—initiated by the passage of the *Homeland Security Act of 2002* (Public Law 107-296)—bringing together 22 separate agencies and offices into a single, Cabinet-level department.

Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners across the Federal Government, public and private sectors, and communities throughout the country have strengthened the homeland security enterprise to better mitigate and defend against dynamic threats.

Many of the features of this new, more robust enterprise align with, and respond to, recommendations contained in the *9/11 Commission Report*, released in July 2004 to assess the circumstances surrounding 9/11 and to identify ways to guard against future terrorist attacks. In recognition of the *9/11 Commission Report* and the tenth anniversary of 9/11, the DHS report describes how the Department has addressed specific 9/11 Commission recommendations over the past ten years, making America stronger and more resilient. While challenges remain, the Department continues to focus on minimizing risks while maximizing the ability to respond and recover from attacks and disasters of all kinds. This is a challenge the men and women of DHS commit themselves to every day.



Progress Addressing Key Recommendations of the 9/11 Commission

Expanding Information Sharing

The United States' strengthened homeland security enterprise includes a number of critical features to expand and enhance information sharing that did not exist on 9/11. These include:

- Seventy-two fusion centers throughout the country, which serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and state, local, tribal, territorial and private sector partners;
- The Nationwide Suspicious Activity Reporting Initiative, which trains state and local law enforcement to recognize behaviors and indicators related to terrorism, crime, and other threats and standardizes how those observations are documented, analyzed, and shared with the Federal Government and other communities throughout the country;
- The National Terrorism Advisory System, which provides timely, detailed information about terrorist threats and recommended security measures to the public, government agencies, first responders, transportation hubs, and the private sector;
- The "If You See Something Say Something™" campaign, a program to raise public awareness of indicators of terrorism and crime and to emphasize the importance of reporting suspicious activity to the proper law enforcement authorities; and
- Robust information sharing with international partners, facilitating the exchange of information about terrorists and criminals.

Developing and Implementing Risk-based Transportation Security Strategies

DHS has made significant advances in risk-based security since 9/11, focusing on intelligence-driven, layered security across all transportation modes. This approach emphasizes pre-screening for passengers and cargo, while focusing resources on those who pose the greatest threat to the Nation's transportation networks. Advances include:

- Conducting baseline security assessments across aviation, maritime, and surface transportation sectors;
- Forging international consensus on historic new global aviation standards;
- Strengthening the security of the global supply chain;
- Collecting and analyzing advanced passenger and cargo information; and
- Supporting risk-based state and local prevention efforts.

Strengthening Airline Passenger Pre-screening and Targeting Terrorist Travel

Ten years ago, screening of passengers coming to the United States was limited to the visa process and inspection of a person by an immigration officer at the port of entry. Provision of advance passenger information was voluntary. In response to both 9/11 and evolving threats, and with the help and support of Congress, DHS has significantly adapted and enhanced its ability to detect threats through a multi-layered, risk-based system. Today, DHS requires all airlines flying to the United States from foreign countries to provide advance passenger information and passenger name records prior to departure; checks 100 percent of passengers on flights flying to, from, or within the



United States against government watchlists through its Secure Flight program; and has expanded trusted traveler programs, expediting travel for passengers who provide biometric identification and pass rigorous, recurrent security checks.

Enhancing Screening for Explosives

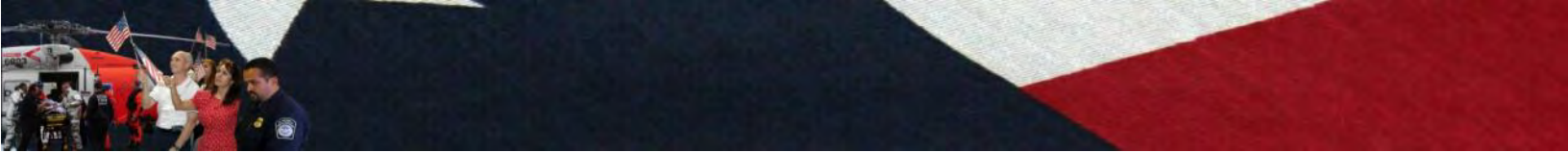
Prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today all checked and carry-on baggage is screened for explosives. The capacity of frontline security personnel and new technologies also has significantly expanded. In March 2002, TSA's first cadre of federal screeners totaled 80 individuals; today more than 52,000 TSA personnel serve on the frontlines at over 450 U.S. airports. Through the *American Recovery and Reinvestment Act of 2009* and annual appropriations, TSA has accelerated the deployment of new technologies to detect evolving threats. In addition, TSA continues to work closely with state and local law enforcement to support surface transportation security through the deployment of Visible Intermodal Prevention and Response Teams, which provide deterrent and detection capabilities across all modes of transportation to prevent or disrupt potential attacks.

Protecting Cyber Networks and Critical Physical Infrastructure

DHS has made significant strides enhancing the security of the Nation's critical physical infrastructure as well as its cyber infrastructure and networks. Current tools include: the National Cybersecurity Protection System, of which the EINSTEIN cyber intrusion detection system is a key component; the National Cybersecurity and Communications Integration Center, which serves as the Nation's principal hub for organizing cyber response efforts; a 2010 landmark agreement between DHS and the Department of Defense to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks; the National Infrastructure Protection Plan, a comprehensive risk management framework for all levels of government, private industry, nongovernmental entities, and tribal partners; and implementation of the Chemical Facility Anti-Terrorism Standards to regulate security at high-risk chemical facilities. In addition, in February 2011, President Obama announced the Wireless Innovation and Infrastructure Initiative to develop and deploy a nationwide, interoperable wireless network for public safety. None of these tools existed prior to 9/11.

Bolstering the Security of U.S. Borders and Identification Documents

Protecting the Nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to homeland security, as well as the Nation's economic prosperity. Over the past several years, DHS has deployed unprecedented levels of personnel, technology, and resources to the Southwest Border, and has made critical security improvements along the Northern and maritime borders. In addition, DHS has taken significant steps to strengthen the security, reliability, and accuracy of personal identification documents and to reduce identity fraud while enhancing privacy safeguards. DHS has fundamentally transformed the way travelers enter the country through the Western Hemisphere Travel Initiative and has prevented potential terrorist and criminal threats from coming to the United States through the Visa Security Program, Visa Waiver Program, and other pre-departure measures.



Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

DHS has the first statutorily required privacy office of any federal agency, and the Department builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development. The DHS Privacy Office partners with every DHS Component to assess policies, programs, systems, technologies, and rulemakings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information. DHS's Office for Civil Rights and Civil Liberties plays a key role in the Department's mission to secure the Nation while preserving individual freedoms through the Civil Rights and Civil Liberties Impact Assessment process. It also engages with communities across the country on civil rights and civil liberties issues.

Challenges that Remain

While DHS has made great progress in securing the Nation since the September 11, 2001, attacks, challenges remain in implementing key recommendations in the *9/11 Commission Report*. Despite significant efforts, including the proposed PASS ID legislation to enhance the security of driver's licenses, many states are still unable to fulfill the congressionally mandated REAL ID requirements. The Department continues to take steps to increase the use of risk based security screening; develop strategies to guard against an increasing volume of cyber attacks; partner with first responders to address interoperability challenges; determine a cost-effective means to implement a biometric exit solution; and guard against potential spillover effects of drug cartel violence in Northern Mexico.

While the demands on DHS have never been greater, the current fiscal climate requires the Department to continue to maximize every security dollar. In order to preserve frontline security operations, DHS has identified more than \$1 billion in cost avoidances and cuts under this Administration. In addition, the Department's fiscal year 2012 budget request included more than \$800 million in further reductions associated with administrative savings and efficiency initiatives currently underway, from efforts to reform acquisition, asset, and real property management to cuts to professional services contracts, supplies and materials, printing, and travel.

Conclusion

While America is stronger and more resilient as a result of these efforts to strengthen the homeland security enterprise, threats from terrorism persist and continue to evolve. Today's threats do not come from any one individual or group. They may originate in distant lands or local neighborhoods. They may be as simple as a homemade bomb or as sophisticated as a biological threat or coordinated cyber attack.

More and more, state, local, and tribal law enforcement officers, as well as citizens, businesses, and communities, are on the front lines of detection and prevention. Protecting the Nation is a shared responsibility, and everyone can contribute by staying informed and aware of the threats the country faces. Homeland security starts with hometown security—and we all have a role to play.



Performance Overview

The performance overview provides a summary of each homeland security mission and focus areas, selected accomplishments, key performance measures, and future initiatives to strengthen the Department’s efforts in achieving a safer and more secure Nation.

Preventing Terrorism and Enhancing Security

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

We will achieve this mission through meeting the following goals:

- **Prevent Terrorist Attacks:** Prevent malicious actors from conducting terrorist attacks within or against the United States.
- **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.
- **Manage Risks to Critical Infrastructure, Key Leadership, and Events:** Reduce the vulnerability of key sectors to attack or disruption.



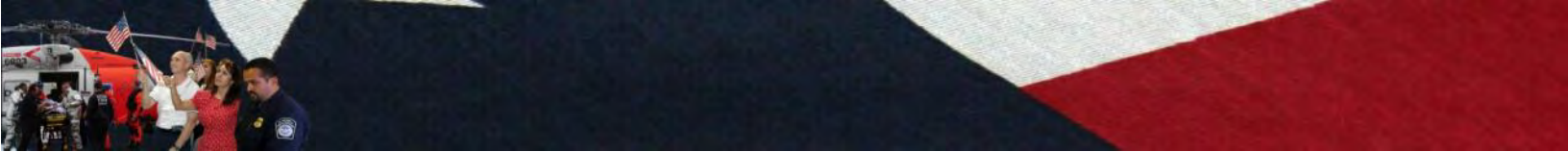
TSA Installs New Privacy Enhancing Software

As part of its commitment to maintain a high level of security while enhancing passenger privacy, the Transportation Security Administration (TSA) is currently in the process of installing new software to further strengthen the privacy protections on its Advanced Imaging Technology (AIT) machines. The software, called Automated Target Recognition, will auto-detect items that could pose a threat using a generic outline of a person for all passengers, eliminating passenger-specific images.

“Our top priority is the safety of the traveling public, and TSA constantly strives to explore and implement new technologies that enhance security and strengthen privacy protections for the traveling public,” TSA Administrator John Pistole said. “This software upgrade enables us to continue providing a high level of security through advanced imaging technology screening, while improving the passenger experience at checkpoints.”

AIT safely screens passengers for both metallic and non-metallic threats, including weapons and explosives. AIT was evaluated and determined to be safe for all passengers by the Food and Drug Administration, National Institute for Standards and Technology and Johns Hopkins University Applied Physics Laboratory.

Below are highlighted performance measures related to *Preventing Terrorism and Enhancing Security*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.



- **Percent of international air enplanements vetted against the terrorist watch list through Secure Flight:** TSA made great strides in vetting international air travelers against the terrorist watch list under the Secure Flight program, achieving 100 percent screening in FY 2011. Secure Flight increases the security of air travel by screening every passenger against the latest intelligence before a boarding pass is issued.
- **Percent of domestic air enplanements vetted against the terrorist watch list through Secure Flight:** TSA vetted 100 percent of all domestic air travelers against the terrorist watchlist in FY 2011, adding an important layer in TSA’s risk-based security operation.
- **Percent of air cargo screened on commercial passenger flights originating from the United States and territories:** TSA is committed to ensuring the security of air cargo while facilitating the flow of legitimate commerce. TSA made significant progress in its processes and technology in FY 2011, screening 100 percent of cargo on commercial passenger flights originating from the United States and territories, up from 50 percent in FY 2009.
- **Percent of targeted urban areas that are monitored for biological threats using BioWatch technology:** The Office of Health Affairs (OHA) uses BioWatch technology to provide an early warning capability in the event of a harmful biological release. OHA met its FY 2011 goal of 100 percent monitoring in targeted high-risk urban areas.
- **Percent of total U.S. Secret Service protection activities that are incident-free for protection of national leaders, foreign dignitaries, designated protectees and others during travel or at protected facilities:** The U.S. Secret Service (USSS) continues to meet its goal of 100 percent incident-free protection for our Nation’s leaders, foreign dignitaries, and others during travel or while at protected facilities.

National Terrorism Advisory System

In April 2011, Secretary Napolitano announced the implementation of DHS’s National Terrorism Advisory System (NTAS)—a robust terrorism advisory system that provides timely information to the public about credible terrorist threats— which replaces the former color-coded alert system. During the announcement, DHS released a [guide](#) outlining the new system to the American public, along with an [example](#) of an NTAS Alert that would be issued to the public if the government were to receive information about a specific or credible terrorist threat.

NTAS is designed to more effectively communicate information about terrorist threats by providing timely, detailed information and recommended security measures to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

Under NTAS, DHS will coordinate with other federal entities to issue detailed alerts to the public when the Federal Government receives information about a specific, credible terrorist threat to the United States. NTAS alerts provide a concise summary of the potential threat, which may include a geographic region, mode of transportation, or critical infrastructure potentially affected by the threat; actions being taken to ensure public safety; and recommended steps that individuals, communities, business and governments can take to help prevent, mitigate or respond to a threat. NTAS Alerts contain a sunset provision indicating a specific date when the alert expires.





Future Initiatives

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

Below are a few focus areas to which the Department is committed in order to achieve our goals:

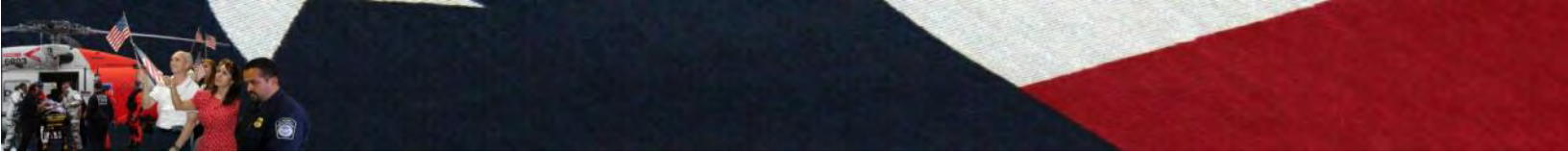
- Understand the current and emerging terrorist threats to the United States, build capability at the state, local, tribal, and territorial level to prevent and disrupt terrorist attacks through programs such as the Nationwide Suspicious Activities Reporting Initiative, and engage communities through campaigns such as "If You See Something, Say Something™."
- Continue TSA's risk-based security initiative through the use of a layered security approach of state-of-the-art technologies, use of existing and proven technology, better passenger identification techniques, and other developments that will continue to strengthen aviation security.
- Continue efforts with respect to threats of nuclear and high-consequence biological attack, consistent with the *National Security Strategy*, while maintaining robust programs for prevention, interdiction, detection, and disruption of chemical and radiological attacks.
- Take a multi-hazard approach to critical infrastructure protection and resilience, as well as protect high-profile events from a variety of threats.

Securing and Managing Our Borders

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

We will achieve this mission through meeting the following goals:

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



SBI^{net} Assessment Leads to New Border Technology Plan

In January 2010, Secretary Napolitano directed a Department-wide assessment to determine if the Secure Border Initiative Network (SBI^{net}) was the most efficient, effective and economical border security technology strategy available. This assessment—which combines an independent, quantitative, science-based review with the input of U.S. Border Patrol agents on the front lines and the Department’s leading science and technology experts from the Science and Technology Directorate—made clear that SBI^{net} cannot meet its original objective of providing a one-size-fits-all border security technology solution.

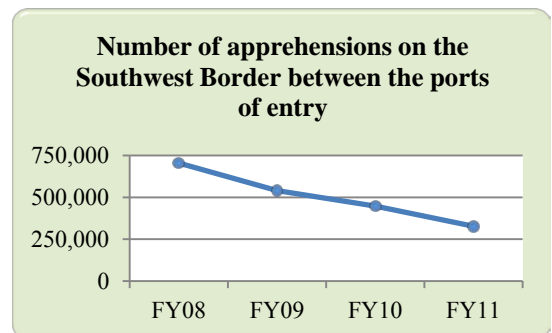
As a result, Secretary Napolitano directed CBP to end SBI^{net} as originally conceived and instead implement a new border security technology plan, which will use existing, proven technology tailored to the distinct terrain and population density of each border region, including commercially available mobile surveillance systems, unmanned aircraft systems, thermal imaging devices, and tower-based remote video surveillance systems. Where appropriate, this plan will also incorporate already existing elements of the former SBI^{net} program that have proven successful, such as stationary radar and infrared and optical sensor towers.

The new plan will use funding previously requested for SBI^{net} and provided in the FY 2011 continuing resolution. CBP intends to acquire all the technologies in the new plan, including the integrated fixed towers, through full and open competition. Independent, quantitative, science-based assessments will continue along each sector of the Southwest Border in 2011 to determine the optimal combination of technology for each region.



Below are highlighted performance measures related to *Securing and Managing Our Borders*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.

- Number of apprehensions on the Southwest Border between the ports of entry:** As a result of unprecedented deployments of personnel, technology, and infrastructure, historic partnerships with law enforcement partners on both sides of the border, and increasing consequences for repeat offenders, apprehensions by the Border Patrol decreased, indicating fewer people are attempting to cross the border. The number of apprehensions on the Southwest Border between the ports of entry was 327,577 in FY 2011, down from 705,022 in FY 2008—a 53.5 percent reduction.



- Percent of detected conventional aircraft incursions resolved along all borders of the United States:** CBP’s Air and Marine Operations Center uses its capabilities, as well as those of the Department of Defense and civilian radar, to identify and track suspect aircraft incursions along our borders. In FY 2011, CBP successfully resolved 95.3 percent of confirmed border incursions and will continue to improve tactics and procedures in order to bring individuals that commit illegal incursions to a successful law enforcement resolution.



- **Percent of foreign airports serving as last point of departure in compliance with leading security indicators:** TSA works with our foreign counterparts to implement security measures at foreign airports that serve as a last point of departure for international flights bound for the United States. TSA made great strides in this area; as of FY 2011, 95.3 percent of foreign airports serving as last point of departure comply with all leading security indicators and DHS will continue its efforts to ensure all international flights bound for the United States are safe and secure.
- **Percent of maritime facilities in compliance with security regulations as they have not received a notice of violation and/or civil penalty:** As part of its border security mission, the U.S. Coast Guard conducts routine and unannounced examinations of Maritime Transportation Security Act regulated facilities. Noncompliance with these security regulations may result in a notice of violation, civil penalty or other restrictions. In FY 2011, 99.9 percent of these examinations were found to be in compliance.



Enhancing Partnerships with Canada to Promote Northern Border Security

In February 2011, President Barack Obama and Prime Minister Stephen Harper announced a landmark “Shared Vision for Perimeter Security and Economic Competitiveness” which sets forth how the two countries will manage shared homeland and economic security in the 21st century. Their vision focuses on addressing threats at the earliest point possible; facilitating

trade, economic growth, and jobs; collaborating on integrated cross-border law enforcement; and partnering to secure and strengthen the resilience of critical infrastructure and cybersecurity.

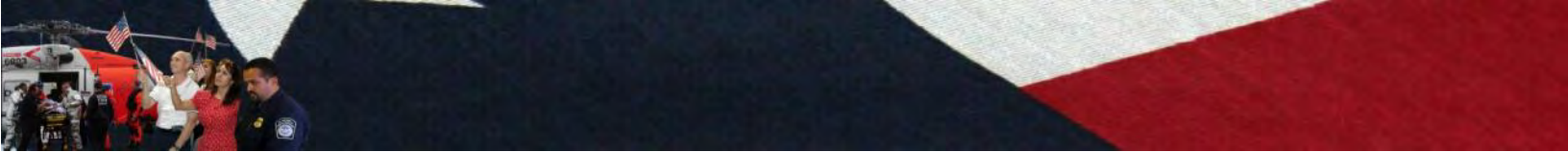
Through the Integrated Cross-Border Maritime Law Enforcement Operations Shiprider agreement, DHS and Canadian joint law enforcement can leverage efforts to bolster cross-border security operations. This agreement enables the Royal Canadian Mounted Police, U.S. Coast Guard, CBP, and Immigration and Customs Enforcement (ICE) to cross-train, share resources and personnel, and use each others’ vessels in the waters of both countries. The Border Patrol, ICE, U.S. Coast Guard, Canadian law enforcement, and other federal partners also collaborate through Integrated Border Enforcement Teams, which work to identify, investigate, and interdict individuals and organizations that may pose a threat to national security or are engaged in organized criminal activity along the Northern Border.

Future Initiatives

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

Below are a few focus areas to which the Department is committed in order to achieve our goals:

- Implement the new border technology plan to further strengthen security along the Southwest Border.



- Implement new investments on the Northern Border to address security needs for the maritime and cold weather environment and deploy innovative technology pilot programs to address the unique needs to secure our Northern Border.
- ICE will continue its partnerships with its federal, state, local, and foreign law enforcement counterparts to enhance the Border Enforcement Security Task Force, a series of multi-agency teams developed to identify, disrupt, and dismantle criminal organizations posing significant threats to border security.

Enforcing and Administering Our Immigration Laws

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

We will achieve this mission through meeting the following goals:

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

Enhancing Employment Vetting through VIBE



In February 2011, U.S. Citizenship and Immigration Services (USCIS) fully deployed the Validation Instrument for Business Enterprises (VIBE), a Web-based tool designed to enhance the adjudication of most employment-based immigration petitions. VIBE uses commercially available data from independent information providers to verify the petitioner’s existence and confirm key information about the organization, such as its location, annual revenue, number of employees, and its general organizational history. VIBE also enables adjudicators to confirm that the organizations are engaged in ongoing business activities while accelerating the adjudicative vetting process and enhancing the agency’s anti-fraud capabilities.

The additional information provided in VIBE improved USCIS’s ability to distinguish eligible petitioners more easily from those who are ineligible. Due to VIBE, known ineligible petitioners are removed from the normal Immigration Services Officer (ISO) casework, thus streamlining the ISO production and increasing quality and consistency. VIBE promotes a more consistent review of employment-based petitions across all four of USCIS’s Service Centers. Preliminary results show that VIBE increased the quality of adjudications and fraud detection.

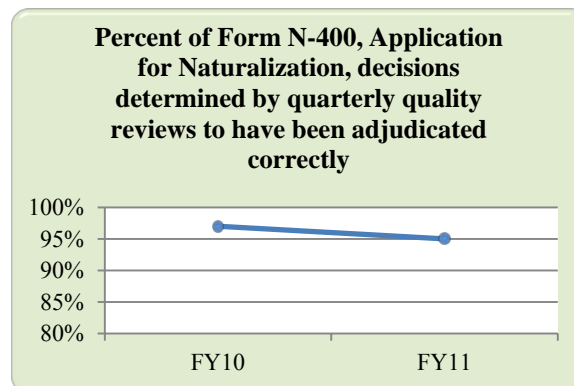
Below are highlighted performance measures related to *Enforcing and Administering Our Immigration Laws*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.

- **Percent of Form I-485, Application to Register for Permanent Residence or to Adjust Status, decisions determined by quarterly quality reviews to have been adjudicated correctly:** Using a panel of subject matter experts, USCIS conducts quarterly reviews of



previously processed applications to determine if they were adjudicated correctly. The results of these reviews are used to improve the methods and training to ensure fraudulent applicants are identified and denied immigration benefits in a timely and efficient manner. In FY 2011, USCIS met their goal, achieving 91 percent.

- Percent of Form N-400, Application for Naturalization, decisions determined by quarterly quality reviews to have been adjudicated correctly:** Similar to the I-485 form, USCIS conducts quarterly quality reviews of the Application for Naturalization. USCIS achieved 95 percent, narrowly missing their target of 96 percent. *Note: USCIS met or exceeded the target the last three quarters of the year.*



- Number of convicted criminal aliens removed per fiscal year:** ICE’s Secure Communities program enhances the Department’s ability to target criminal aliens through an information-sharing partnership between DHS and the FBI that uses fingerprints taken when individuals are booked into state prisons and local jails to identify removable aliens who were arrested and booked for the commission of a non-immigration related criminal offense as part of the Department’s focus on identifying and removing convicted criminal aliens who pose a public safety threat to American communities. In FY 2011, ICE removed 216,698 convicted criminal aliens from the United States, representing 55 percent of all individuals removed.

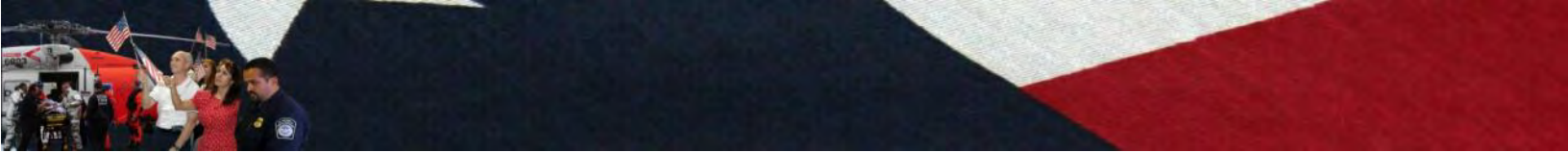


ICE Removes Former Member of Guatemalan Army Linked to Massacre

On July 12, 2011, ICE deported [Pedro Pimentel Rios](#), a former member of the Guatemalan army whom witnesses say participated in the murder of dozens of men, women and children in the village of Las Dos Erres in December 1982. The deportation represents a victory for ICE’s [Human Rights Violators and War Crimes Center](#), which investigated the case.

ICE charged Pimentel Rios in immigration court with being deportable for having assisted or otherwise participated in extrajudicial killings during the Dos Erres massacre. In May, an immigration judge in Los Angeles cleared the way for Pimentel Rios’ repatriation to Guatemala, ruling he was deportable based upon his participation in the killings at Las Dos Erres. The judge’s ruling capped an intensive legal effort by ICE to gain Pimentel Rios’ removal from the United States following his arrest by ICE’s Homeland Security Investigations agents in Orange County, California a year ago.

“For the families who lost loved ones at Dos Erres, justice has been a long time coming, but they can take consolation in the fact that those responsible for this tragedy are now being held accountable for their crimes,” said ICE Director John Morton. “I applaud the outstanding work by ICE attorneys and investigators to bring a successful conclusion to this case. We will not allow our country to serve as a safe haven for those who commit human rights abuses and war crimes.”



Future Initiatives

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

Below are a few focus areas to which the Department is committed in order to achieve our goals:

- Continue to support the Secure Communities program by deploying interoperability to state prisons and local jails. ICE is working with DHS's Office for Civil Rights and Civil Liberties, and in communication with the Department of Justice, on an oversight and evaluation process of Secure Communities and providing additional training to state and local law enforcement.
- Bolster USCIS's effort to support immigrant integration efforts, including funding to enhance programs supporting English language acquisition and citizenship education.
- Continue support for E-Verify operations and enhancements, including continued funding for new monitoring, compliance, and outreach positions necessitated by program expansion.

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. If these cyber tools and networks cannot function properly, we will not be able to effectively communicate, travel, power our homes, run our economy, or obtain government services. By statute and Presidential directive, DHS is the lead for the Federal Government to secure civilian government computer systems; working with industry to defend privately owned and operated critical infrastructure; and, working with state, local, tribal, and territorial governments to secure their information systems.

We will achieve this mission through meeting the following goals:

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



National Cybersecurity Incident Response

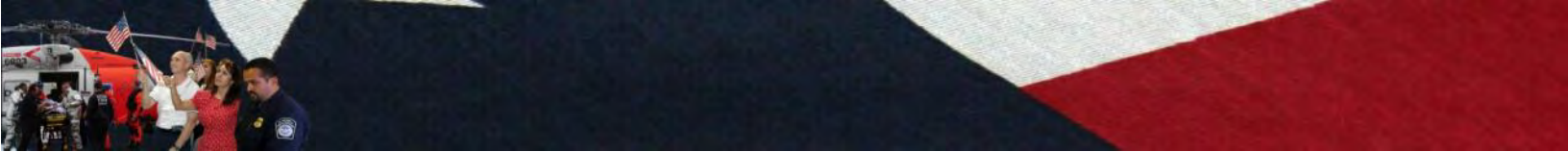
In March 2011, a U.S. oil and natural gas organization was victimized by a series of successful cybersecurity attacks, and subsequently contacted the Federal Bureau of Investigation (FBI). Under the framework established in the National Cybersecurity Incident Response Plan, the FBI reached out to DHS to provide assistance through the National Cybersecurity and Communications Integration Center.



At the company's request, DHS deployed cyber experts on-site to provide hands-on incident response, analysis, and mitigation solutions. Using custom tools and unique knowledge of known threats, the DHS team soon discovered malicious activity on the company's network. DHS proposed network changes that would help mitigate the damage and defend from future attacks. DHS also disseminated recommendations from this engagement to other critical infrastructure owners and operators, to better secure our Nation for the future.

Below are highlighted performance measures related to *Safeguarding and Securing Cyberspace*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.

- Percent of Federal Executive Branch civilian networks monitored for cyber intrusions with advanced technology:** This measure assesses DHS's increased vigilance in identifying malicious activity across Federal Executive Branch civilian agency networks. DHS operators monitor Federal Executive Branch networks using EINSTEIN intrusion detection system sensors, which are deployed to Trusted Internet Connections locations at agencies or Internet Service Providers. In FY 2011, 31.9 percent of Federal Executive Branch civilian networks were monitored for cyber intrusion using advanced technology, exceeding our target of 28 percent. *Note: This program is in its early stages of implementation—targets and results will continue to increase.*
- Percent of unique vulnerabilities detected during cyber incidents where mitigation strategies were provided by DHS:** The National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US-CERT) provides mitigation strategies when cyber vulnerabilities are detected during a cyber incident to address the vulnerability and prevent the incident from recurring. In FY 2011, when a cyber incident was detected, US-CERT provided mitigation strategies 93 percent of the time, exceeding the target of 90 percent. In the second half of 2011, US-CERT improved its efficiency and provided mitigation strategies to 100 percent of unique vulnerabilities detected to close out the year.
- Average amount of time required for initial response to a request for assistance from public and private sector partners to prevent or respond to major cyber incidents:** DHS's National Cyber Security Division strives to respond within two hours of a request for assistance to a major cyber incident. The program narrowly missed its target with an overall average response time of 2.3 hours; however, US-CERT exceeded the target response time by averaging 1.83 hours in the second through fourth quarters of FY 2011.



DOD/DHS Cybersecurity Agreement

In September 2010, Secretary Napolitano and Secretary of Defense Robert Gates signed a Memorandum of Agreement (MOA) to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks. The Agreement embeds

Department of Defense (DOD) cyber analysts within DHS and sends DHS privacy, civil liberties, and legal personnel to DOD's National Security Agency (NSA) to strengthen the nation's cybersecurity posture and ensure the protection of fundamental rights. Pursuant to the MOA, DHS and NSA are engaged in an activity to grant temporary security clearances to select Chief Information Officers of private sector organizations in several critical infrastructure sectors. This allows DHS and NSA to share specific threat and risk information with sector officials, enabling them to incorporate cyber risks in their long-term decision making and investments.

Future Initiatives

Below are a few focus areas to which the Department is committed in order to achieve our goals:

- Strengthen federal network security through network assessments to improve security across the Federal Executive Branch.
- Provide high-quality, cost-effective virtual cybersecurity education and training to develop and grow a robust cybersecurity workforce that is able to protect against and respond to national cybersecurity threats and hazards.
- Coordinate national cybersecurity operations and interface with interagency partners to protect against threats to critical civilian and military computer systems and networks.
- Enhance bi-directional information sharing processes with critical infrastructure owners and operators to create shared situational awareness of cyber threats across sectors and facilitate collaborative incident response.
- Expedite the deployment of EINSTEIN 3 to prevent and detect intrusions on computer systems and to upgrade the National Cybersecurity Protection System, building an intrusion detection capability and analysis capabilities to protect federal networks.
- Build on the National Cyber Incident Response Plan, which enables DHS to coordinate the response of multiple federal agencies, state and local governments, international partners, and private industry to incidents at all levels. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines.
- Build on the Comprehensive National Cybersecurity Initiative to support research and development projects focused on strengthening the Nation's cybersecurity.
- Increase outreach to Critical Infrastructure and Key Resource owners and improve control systems cybersecurity awareness, incident response, coordination, and information sharing.

Ensuring Resilience to Disasters

Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as terrorist attacks, may occur. The challenge is to build the capacity of American society to be resilient in the face of natural disasters and terrorist threats. Our vision of a resilient



Nation is one with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

We will achieve this mission through meeting the following goals:

- **Mitigate Hazards:** Strengthen capacity at all levels of society to withstand threats and hazards.
- **Enhance Preparedness:** Engage all levels and segments of society in improving preparedness.
- **Ensure Effective Emergency Response:** Strengthen response capacity nationwide.
- **Rapidly Recover:** Improve the Nation's ability to adapt and rapidly recover.

Establishing Effective Communications during a Response

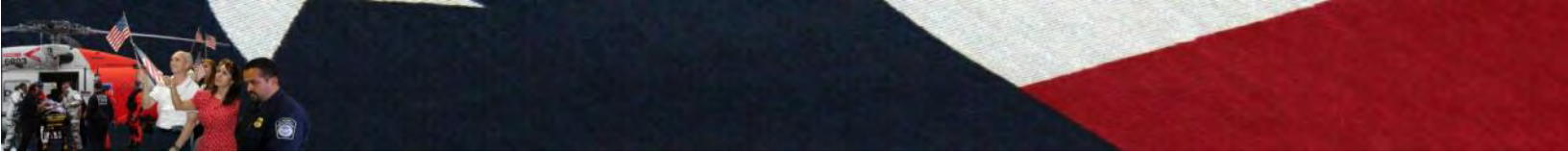
In a disaster situation, communications between the Federal Emergency Management Agency (FEMA), federal, state, and local agencies is critical. It is important that members of the emergency management team communicate with one another in real time during life saving operations and recovery efforts. In preparation for this year's historic flooding in Minot, North Dakota, FEMA's Mobile Emergency Response Support Detachment (Denver) was deployed to provide radios to agencies involved in the flood fight so they could all operate on a single frequency, enabling interoperable communications.



The Fire Chief from Minot credited FEMA with assisting in developing a communications plan that helped meet the needs of the emergency management team, resulting in communications that were deemed "excellent."

Below are highlighted performance measures related to *Ensuring Resilience to Disasters*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.

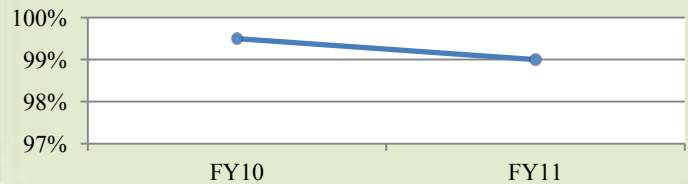
- **Percent of time that critical communications for response operations are established within 12 hours:** This measure reflects the percent of time that critical communications are established for FEMA's on-site emergency responders within 12 hours of the deployment of Mobile Emergency Response Support. FEMA met its target of achieving this in 100 percent of response operations in FY 2011.
- **Percent of essential incident command functions (enabled through response teams and operations centers) that are established within 12 hours:** This measure gauges the percent of time that response teams and operations centers are established within 12 hours to successfully perform essential incident command functions to respond to disasters effectively and in a unified manner. FEMA met its target of achieving this in 100 percent of response operations in FY 2011.
- **Percent of orders for required life-sustaining commodities (meals, water, tarps, plastic sheeting, cots, blankets, and generators) and key operational resources delivered by the agreed upon date:** FEMA distribution centers and logistics partners provide life-sustaining commodities in the event of a disaster. Reliable delivery systems are in place to ensure that



life-sustaining commodities will be there when needed. For those disasters where FEMA was called into action in FY 2011, 96 percent of orders were delivered on time, exceeding their annual target of 85 percent.

- **Percent of eligible applicants provided temporary housing (including non-congregate shelters, hotel/motel, rental assistance, repair and replacement assistance, or direct housing) assistance within 60 days of a disaster:** FEMA temporary housing assistance includes transitional sheltering assistance (hotel/motel), rental assistance, repair and replacement assistance, or direct housing (temporary housing units). In FY 2011, FEMA placed eligible applicants in temporary housing within 60 days 99 percent of the time, meeting their target of 94 percent.

Percent of eligible applicants provided temporary housing (including non-congregate shelters, hotel/motel, rental assistance, repair and replacement assistance, or direct housing) assistance within 60 days of a disaster



- **Government Emergency Telecommunications Service call completion rate during emergency communication periods:** This measure gauges the Government Emergency Telecommunications Service (GETS) call completion rate. The GETS call completion rate is the percent of calls that a national security/emergency preparedness user completes via public telephone network to communicate with the intended user, location, or system, during an emergency situation. In FY 2011, the GETS call completion rate was 97.8 percent, meeting our target of 90 percent.

Increasing Household Preparedness

Presidential Preparedness Directive-8 requires a comprehensive campaign to build and sustain national preparedness, including public outreach and community and private sector programs. A key step is to understand the current state of preparedness. FEMA is tracking nationwide preparedness through its Citizen Corps Household Survey to better understand how and why we prepare for disasters. In 2011, 42 percent of households had a plan of what they would do in the event of a disaster and had discussed it with their household; 33 percent could list up-to-date supplies set aside in case of disaster; and 39 percent were informed of key information like local hazards, local alert, and warning systems or knew what to do based on training.

FEMA recognizes that it takes a whole community to prepare and respond to disasters, and that preparedness starts with the individual. FEMA's Ready.gov and Citizen Corps encourage and support preparedness through national campaigns and local programs, including Citizen Corps Councils and Community Emergency Response Teams training. Recent FEMA initiatives to engage the whole community—particularly populations traditionally not engaged in preparedness—resulted in increasing registrations of organizations and individuals committing to get their community involved in National Preparedness Month from under 5,000 registrations in 2010 to more than 8,000 this year.





Future Initiatives

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

Below are a few focus areas to which the Department is committed in order to achieve our goals:

- Continue the dissemination of plans and preparedness standards through training and technical assistance, and validate their effectiveness through exercises.
- Sustain federal funding for state and local preparedness grants, highlighting the Department's commitment to moving resources out of Washington, DC and into the hands of state and local first responders who are often best positioned to detect and respond to terrorism, other threats, and natural disasters.
- Implement the Staffing for Adequate Fire and Emergency Response grants to rehire laid-off firefighters and retain veteran first responders.

Providing Essential Support to National and Economic Security

DHS leads and supports many activities that provide essential support to national and economic security including, but not limited to: maximizing collection of customs revenue; maintaining the safety and security of the marine transportation system; preventing the exploitation of children; providing law enforcement training; and coordinating the Federal Government's response to global intellectual property theft.

DHS contributes in many ways to these elements of broader U.S. national and economic security:

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



Operation Stone Face II

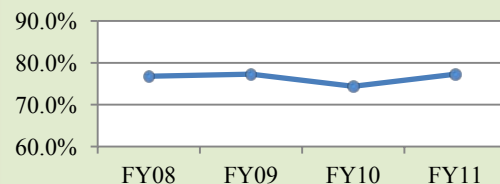
Imports of polished granite from Brazil and India were often misclassified in order to claim Generalized System of Preferences (GSP), a trade preference program which allows for significantly diminished duty rates. CBP conducted Operation Stone Face I in 2008 which targeted those imports. The Operation was successful, however recently CBP discovered that some importers adopted a different GSP eligible provision for imports of polished granite in order to once

again evade customs collection. The many discrepancies discovered through CBP's targeting made it abundantly clear that another special operation would be necessary to address the misclassification of stone, which gave rise to Operation Stone Face II in April 2010. As part of this ongoing operation, CBP targeted the misclassified stone, which were similarly being entered conditionally free due to the GSP claim. CBP's targeting associated with Operation Stone Face II generated an estimated \$457,105 in recovered revenue and \$20,000 in penalty assessments.

Below are highlighted performance measures related to *Ensuring Resilience to Disasters*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.

- Percent of revenue directed by trade laws, regulations, and agreements successfully collected:** This measure estimates the collected duties expressed as a percent of the all collectable revenue due from commercial imports to the United States directed by trade laws, regulations, and agreements. In FY 2011, 99.1 percent of collectable revenue was collected, slightly missing the program's aggressive target of 100 percent.
- Percent of people in imminent danger saved in the maritime environment:** This measure is the percent of people who were in imminent danger on the oceans and other waterways and whose lives were saved by U.S Coast Guard after requesting help. The U.S. Coast Guard makes every effort to save 100 percent of all people in imminent danger. The FY 2011 results were 77.3 percent, up from the FY 2010 results of 74.4 percent. Performance results are affected by multiple variables, including initial case information received by the U.S. Coast Guard, weather conditions, location of an incident relative to response assets, incident severity, and life saving devices and alerting technologies utilized by the distress party.

Percent of people in imminent danger saved in the maritime environment



Defense Readiness

U.S. Coast Guard Cutters *Bertholf*, *Sycamore*, and *Long Island* participated in Exercise Northern Edge, a training event held annually in Alaska. Sponsored by United States Northern Command, Northern Edge is a multi-service training exercise designed to practice operations, tactics, and procedures aimed at enhancing interoperability among U.S. military forces. Throughout the exercise, U.S. Coast Guard ships assumed offensive and defensive postures in response to aerial and surface threats. In both roles, U.S. Coast Guard ships utilized their unique capabilities to work alongside Department of Defense counterparts, exercising tactics, techniques, and procedures involving engineering casualty control, medical response, helicopter landing operations, underway replenishment, and visit, board, search, and seizure. The common objective among all scenarios was to improve communications, interoperability, and command and control procedures.





Future Initiatives

Below are a few focus areas to which the Department is committed in order to achieve our goals:

- Continue the U.S. Coast Guard's recapitalization of cutters; boats; aircraft; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems; and infrastructure to improve mission readiness and response capability.
- Bolster the U.S. Coast Guard's Marine Safety Performance Plan and Marine Environmental Response Mission Performance Plan. As witnessed on a national scale during the response to the BP Deepwater Horizon oil spill, when maritime emergencies occur, U.S. Coast Guard incident responders rapidly establish and execute the Incident Command System to lead an effective, unified effort.

Maturing and Strengthening the Homeland Security Enterprise

The strategic aims and objectives for maturing and strengthening the homeland security enterprise 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.



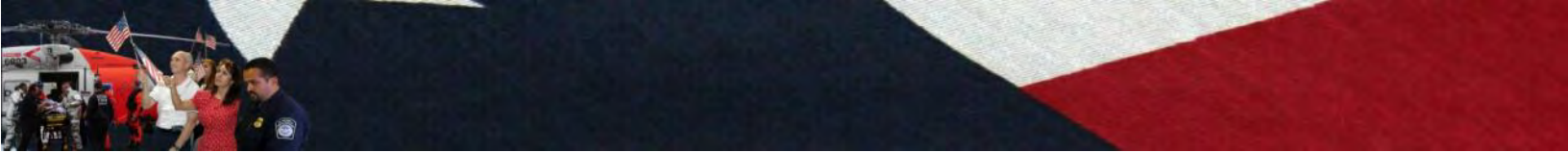
Improved Efficiency

On September 14, 2011, as part of the Administration's Campaign to Cut Waste, Vice President Biden highlighted the DHS Efficiency Review (ER) as a model effort for other agencies across the Federal Government.

Secretary Napolitano launched the Department-wide review in March 2009, and to date, DHS launched 36 initiatives designed to reduce costs, improve communication, and streamline processes. DHS ER develops initiatives based on employee input, including ideas submitted to the President's Securing Americans' Value and Efficiency award competition and successful initiatives implemented at the Component level. DHS identified more than \$1 billion in cost avoidances through the ER, as well as Component-specific cost-saving initiatives.

"Over the last two years, we have made an unprecedented commitment to efficiency in order to support frontline operations by building a culture of fiscal discipline and accountability throughout the Department," said Secretary Napolitano. "Through the Department of Homeland Security's Efficiency Review, we've taken a hard look at how we do business, and identified ways to maximize the effectiveness and efficiency of limited taxpayer dollars we receive."

Throughout the summer of 2011, the DHS Efficiency Review Office sponsored the Think Efficiency Campaign, which asked all DHS employees to submit ideas for new efficiency initiatives. More than 1,600 ideas were submitted by employees focusing on ways to avoid costs, streamline processes, and improve customer service. The top ideas were reviewed by the DHS Efficiency Review Steering Committee, and six innovative ideas were selected as finalists for further evaluation by cross-Component subject matter experts for possible implementation.



Future Initiatives

Maturing and strengthening the homeland security enterprise—the collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private-sector partners, as well as individuals, families, and communities—is critical to our long term objectives. This includes enhancing shared awareness of risks and threats, building capable communities, and fostering innovative approaches and solutions through cutting-edge science and technology, while continuing to improve Department management and accountability.

Below are a few focus areas to which the Department is committed in order to achieve our goals:

- Continue the execution of the Balanced Workforce Strategy, which is designed to ensure the Department has the appropriate mix of federal employees and contractors to fulfill our mission in a manner that is cost-effective and ensures appropriate federal oversight.
- Enhance the Department's ability to ensure program cost estimates are reasonable reflections of the program's requirements. Reliable and credible independent cost estimates will increase the Department's capability for informed investment decision making, budget formulation, progress measurement, and accountability.
- Increase the Department's acquisition workforce capacity—including additional systems engineers, program managers, logisticians, and business cost estimators, to ensure operational requirements are properly developed and included in DHS contracts and to provide greater oversight and accountability.
- Continue the implementation and expansion of the Secretary's Department-wide Efficiency Review to do more with less and maximize the effectiveness and efficiency of limited resources.

Veterans at DHS

Our Nation's veterans possess unique talents, experiences, and dedication that can be invaluable to the Department's mission of securing our homeland. That is why the Department works every day to cultivate a stronger relationship with the veteran community. The Department of Homeland Security is proud to count more than 50,020 veterans—25 percent of all civilian employees—among its workforce. This is on top of the more than 40,000 active duty members of the U.S. Coast Guard. In addition, in each of the past two years the Department awarded approximately \$900 million in prime contracts to non-disabled and service-disabled veteran-owned small businesses.

The Office of the Chief Human Capital Officer, in close collaboration with the Office for Civil Rights and Civil Liberties (CRCL), provides the Department's efforts in veteran recruiting. They develop recruitment materials, identify and participate in job fairs, and coordinate with other departments on [special veteran programs](#). They are also responsible for teaching Components to use veteran hiring tools and developing standardized training materials for recruiters to be used by Components. CRCL provides leadership, guidance, and technical assistance for the Disabled Veterans Affirmative Action Program.





Financial Overview

DHS’s budgetary resources were approximately \$78 billion for FY 2011, \$5 billion less than in FY 2010. 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. DHS primarily uses the cash basis for its budgetary accounting. The cash basis is an accounting method in which income is recorded when cash is received and expenses are recorded when cash is paid out. These financial statements provide the results of our operations and financial position, including long-term commitments and obligations. The independent accounting firm KPMG LLP audited the Balance Sheet and Statement of Custodial Activity and Internal Controls over Financial Reporting.

The Department received supplemental appropriations during FY 2009 as a result of *The American Recovery and Reinvestment Act of 2009* (Recovery Act) (Pub. L. 111-5). Seven DHS Components received funding to carry out Recovery Act programs in support of the Department’s mission. MGMT received funding for the consolidation of DHS headquarters; CBP received funding to modernize infrastructure and enhance border security technology; ICE received funding for tactical communications upgrades; TSA received funding for enhanced security technology; the U.S. Coast Guard received funding for bridge alteration construction and shore, facility and vessel modernization; FEMA received funding for port, transit, and fire station construction grants and additional funding for the Emergency Food and Shelter program; and OIG received funding for oversight and audit of programs, grants, and projects funded under the Recovery Act. Additional Recovery Act information can be found at www.recovery.gov.

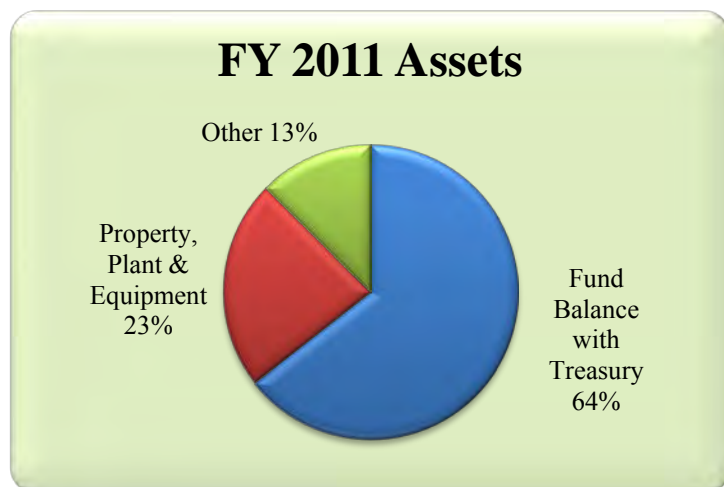
Balance Sheet

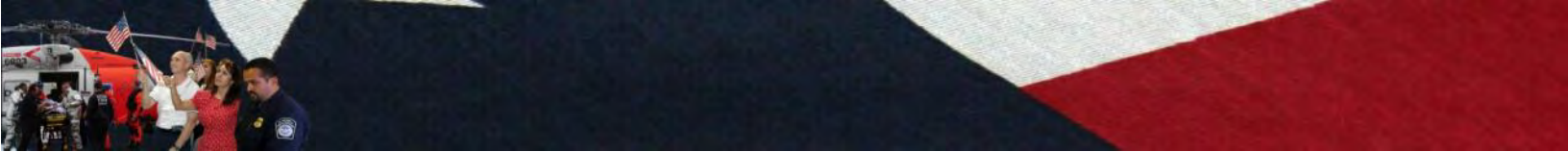
The Balance Sheet presents the resources owned or managed by DHS that have future economic benefits (assets) and the amounts owed by DHS that will require future payments (liabilities). The difference between DHS’s assets and liabilities is the residual amount retained by DHS (net position) that is available 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, 2011, DHS had \$87 billion in assets, representing a \$3 billion decrease from FY 2010 assets of \$90 billion.

As of September 30 (in Millions)	FY 2011	FY 2010
Fund Balance with Treasury	\$55,960	\$60,822
General Property, Plant, and Equipment, Net	20,037	19,074
Other	10,892	10,201
Total Assets	\$86,889	\$90,097





Fund Balance with Treasury (FBwT), the Department’s largest asset, comprises 64 percent (\$56 billion) of the total assets. Included in FBwT is the remaining balance of DHS’s unspent prior-year budgets plus miscellaneous receipts. FBwT decreased approximately \$5 billion from FY 2010 due primarily to a decrease in FEMA’s disaster funding levels and a decrease in appropriations received for several Components in FY 2011.

Property, Plant, and Equipment (PP&E) is the second largest asset, comprising 23 percent of total assets. The major items in this category include construction in progress, buildings and facilities, vessels, aircraft, and other equipment. In acquiring these assets, DHS either spent cash or incurred a liability to make payment at a future date; however, because these assets should provide future benefits to help accomplish the DHS mission, DHS



reports these items as assets rather than expenses. PP&E is recorded net of accumulated depreciation. Recording the net value of the PP&E items is intended to approximate its remaining useful life. During FY 2011, PP&E increased by approximately \$1 billion. A large part of this increase was due to CBP’s Office of Technology and Acquisition Electronic System (formerly known as the recently cancelled *SBI_{net}*; Virtual Fence) software development and physical fence construction. In addition, the U.S. Coast Guard contributed with an increase in Rescue 21, an advanced command, control and communications system that improves the ability to assist mariners in distress and save lives and property at sea. The U.S. Coast Guard also capitalized the *Stratton*, the third National Security Cutter. Also contributing to the PP&E increase is TSA, which procured additional Explosive Trace Detection (ETD) systems in order to expand the use of ETDs at new airports as well as replace older ETDs at existing airports.

Liabilities – What We Owe

At September 30, 2011, DHS reported approximately \$88 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. Eighty-eight percent of these liabilities will need to be paid with future funding sources. Liabilities increased approximately \$4 billion from FY 2010 liabilities which totaled \$84 billion.

As of September 30 (in Millions)	FY 2011	FY 2010
Federal Employee and Veterans’ Benefits	\$49,664	\$48,317
Debt	17,754	18,505
Employee-related and Other	15,522	12,029
Accounts Payable	5,007	4,745
Total Liabilities	\$87,947	\$ 83,596

DHS’s largest liability is for Federal Employee and Veterans’ Benefits, representing 56 percent of total liabilities. This liability increased approximately \$1 billion from FY 2010. This increase primarily relates to U.S. Coast Guard changing its discount rate and assumptions used to calculate the Retired Pay and Military Care Actuarial liability. DHS owes these amounts to current and past civilian and military personnel for pension and other post-employment benefits. The liability also includes medical costs for approved workers’ compensation cases and an estimate for incurred but



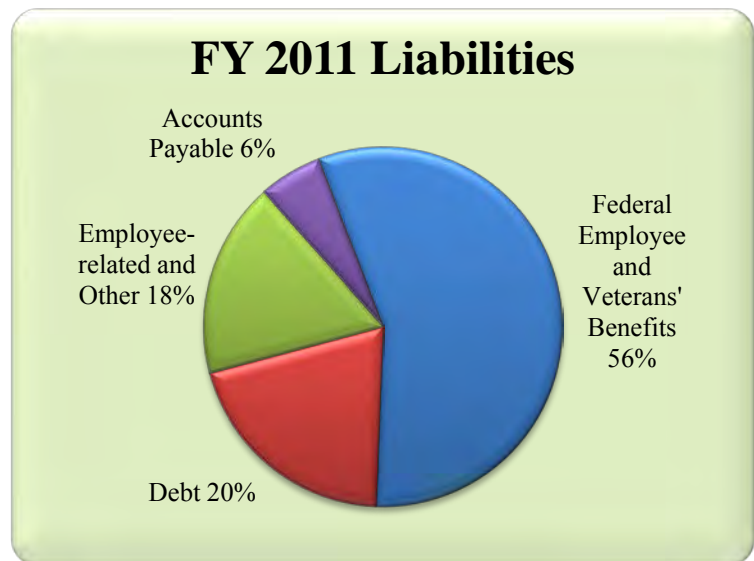
not yet reported workers' compensation costs. This liability is not covered by current budgetary resources, and DHS will use future appropriations to cover these liabilities.

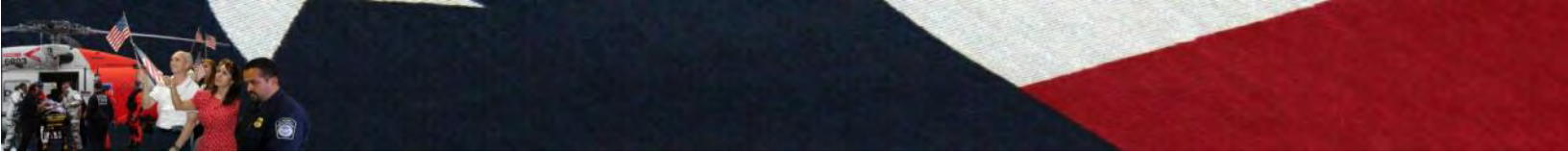
Debt is DHS's second-largest liability, representing 20 percent of total liabilities. This debt results from Department of Treasury loans and related interest payable to fund the National Flood Insurance Program (NFIP) and Disaster Assistance Direct Loan Program operations of FEMA. Total debt decreased approximately \$751 million from FY 2010 due repayment of loans used to fund the NFIP. 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.

Employee-related and other liabilities, comprising 18 percent of the Department's liabilities, increased approximately \$4 billion from FY 2010. The change primarily relates to an increase in the NFIP reserve for claim loss relating to Hurricanes Irene and Lee and an increase in importing taxes due to the Treasury. Also included in these liabilities are unpaid wages and benefits for current DHS employees. Six percent of total liabilities results from accounts payable, which are actual or estimated amounts DHS owes to vendors for goods and services provided for which we have not yet paid. These liabilities are covered by current budgetary resources.

Statement of Net Cost

Net Cost of Operations represents the difference between the costs incurred by DHS programs less revenues. FEMA represents 25 percent of the Department's net cost, a 28 percent increase from FY 2010, which is due to an increase in the actuarial liability for future estimated losses relating to the flood activity from Hurricanes Irene and Lee. Net costs for CBP represent 22 percent of Department total and went to protecting our Nation's borders. The U.S. Coast Guard incurred 21 percent of total net costs in ensuring maritime safety, security, and stewardship. TSA net costs represent ten percent of the Department total and went to protecting the nation's transportation systems to ensure freedom of movement for people and commerce. Net costs for ICE represent ten



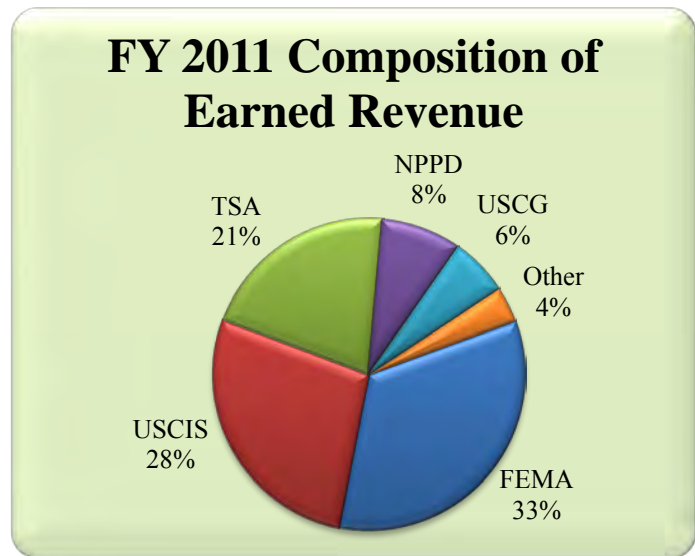
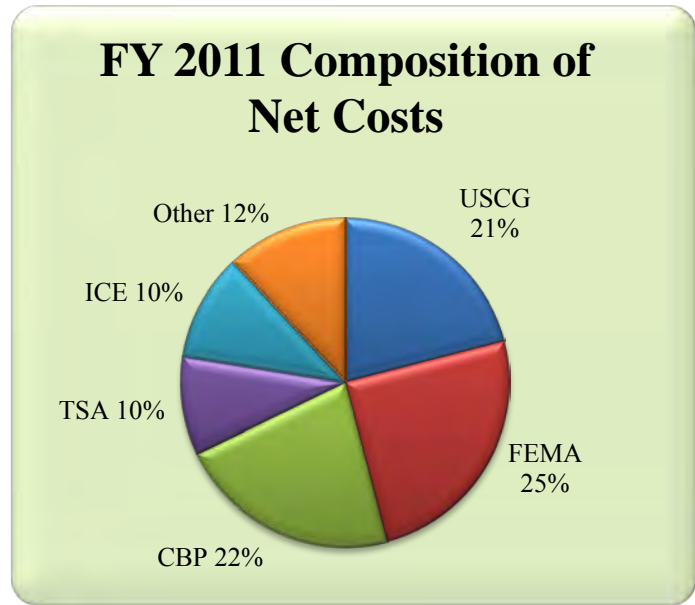


percent of the total and went to promoting homeland security and public safety through enforcement of federal laws governing border control, customs, trade, and immigration.

During FY 2011, the Department earned approximately \$11 billion in revenues; this is an increase of about \$604 million from \$10.4 billion as of September 30, 2010. The Department classifies revenues as either exchange (“earned”) or non-exchange revenue. Exchange revenues arise 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 revenues on behalf of the Federal Government. These non-exchange revenues are presented in the Statement of Custodial Activity rather than the Statement of Net Cost.

Statement of Changes in Net Position

Net position represents the accumulation of revenue, expenses, budgetary and other financing sources since inception, as represented by an agency’s balances in unexpended appropriations and cumulative results of operations on the Statement of Changes in Net Position. Financing sources increase net position and include, but are not limited to, appropriations, user fees, and excise taxes. The net costs discussed above and transfers to other agencies decrease net position. In FY 2011, FEMA had higher costs due to an increase in the actuarial liability for future estimated losses relating to flood activity from Hurricanes Irene and Lee.



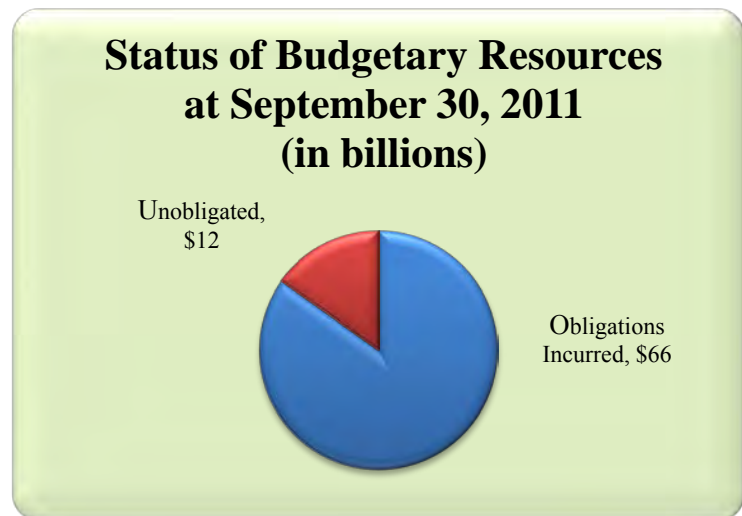
TSA made key investments in aviation security during FY 2011, including portable ETD machines.



Statement of Budgetary Resources

This statement provides information on the status of the approximately \$78 billion in budgetary resources available to DHS during FY 2011. This authority was derived from appropriations of \$50 billion, \$15 billion in authority carried forward from FY 2010, \$10 billion in collections, and \$3 billion of miscellaneous authority.

The total amount of resources available decreased by approximately \$5 billion from FY 2010 levels. This difference is primarily related to a decrease in FEMA's disaster funding levels from FY 2010.



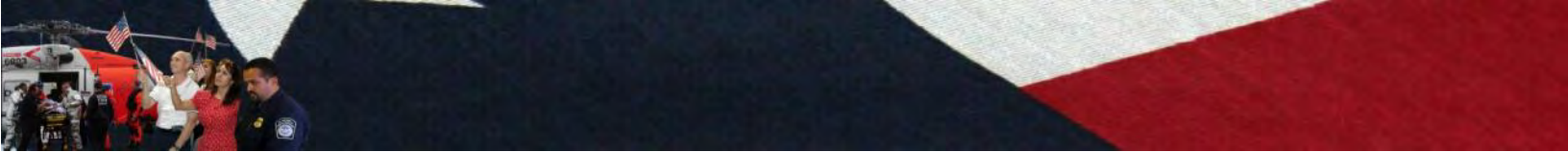
Of the total budget authority available, DHS incurred a total of \$66 billion in obligations from purchase orders placed, contracts awarded, salaries and benefits, or similar transactions. These obligations will require payments during the same or future period. As of September 30, 2011, \$12 billion of the \$78 billion was not yet obligated. The \$12 billion represents \$5 billion in unavailable funding and \$7 billion in apportioned funds available for future use.

Statement of Custodial Activities

This statement presents the disposition of revenues 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 revenues are either retained by the Department to further its mission or returned to Treasury's General Fund. For FY 2010, this statement includes USCIS user fees that were subsequently remitted to the Treasury's General Fund or to other entities. In FY 2011, these user fees are reported on the Statement of Net Cost to more fairly present the Department's results of operations and changes in net position. For additional information on these activities, see Note 31 and Note 1.X., Exchange and Non-exchange Revenue in the financial section. Total cash collections increased by more than \$4 billion in FY 2011. This is due to increased importing into the United States during FY 2011, which resulted in additional cash collections for customs duties at CBP with a minor offsetting reduction in USCIS user fees.

Stewardship Assets and Investments

DHS's stewardship assets primarily consist of U.S. Coast Guard heritage assets, which include ship equipment, lighthouses and other aids to navigation, communication items, military uniforms, ordnance, artwork, and display models. A heritage asset is any personal property that is retained by DHS because of its historic, cultural, educational, or artistic value as opposed to its current



usefulness to carrying out the mission of the Department. The U.S. Coast Guard has over 700 memorials, recreational areas, and other historical areas designated as multi-use heritage assets. CBP has four multi-use heritage assets located in Puerto Rico, and FEMA has one multi-use heritage asset that is used by the United States Fire Administration for training in Emmitsburg, Maryland. In addition, CBP, USCIS, and TSA have collection-type assets that consist of documents, artifacts, immigration and naturalization files, as well as architectural and building artifacts used for education.

Stewardship investments are substantial investments made by the Federal Government for the benefit of the Nation. When incurred, stewardship investments are treated as expenses in calculating net cost, but they are separately reported as Required Supplementary Stewardship Information (RSSI) to highlight the extent of investments that are made for long-term benefits. Included are investments in research and development, human capital, and non-federal physical property.

Limitations of Financial Statements

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

Other Key Regulatory Requirements

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



Management Assurances

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

DHS is responsible for establishing, maintaining, and assessing internal control to provide reasonable assurance that the internal control 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. 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.

In addition, the *Department of Homeland Security Financial Accountability Act* (Pub. L. 108-330) requires a separate assertion and an audit opinion of the Department's internal controls over its financial reporting. 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.

The DHS Accountability Structure includes a Senior Management Council (SMC), an Internal Control Coordination Board (ICCB), and a Senior Assessment Team (SAT). The SMC approves the level of assurances for the Secretary's consideration and is comprised of the Department's Under Secretary for Management, Chief Financial Officer, Chief Administrative Services Officer, Chief Human Capital Officer, Chief Information Officer, Chief Information Security Officer, Chief Security Officer, and Chief Procurement Officer. The ICCB seeks to integrate and coordinate internal control assessments with other internal control related activities and includes representatives from all DHS lines of business to address crosscutting internal control issues. Finally, the SAT, led by the Chief Financial Officer, is comprised of senior-level financial managers assigned to carry out and direct Component-level internal control over financial reporting assessments.

Individual Component assurance statements serve as the primary basis for the Secretary's assurance statements. The assurance statements are also based on information gathered from various sources including management-initiated internal control assessments, program reviews, and evaluations. In addition, the DHS Office of Inspector General (OIG) and the Government Accountability Office (GAO) conduct reviews, audits, inspections, and investigations.

Secretary's Assurance Statement

November 11, 2011




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

In accordance with the *Federal Managers' Financial Integrity Act* (FMFIA) and the *Department of Homeland Security Financial Accountability Act* (DHS FAA), I have directed an evaluation of internal control at the Department of Homeland Security in effect during the fiscal year (FY) ending September 30, 2011. This evaluation was conducted in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*. The Department can provide assurance that the objectives of FMFIA Section 2 over nonfinancial operations have been achieved, with the exception of four material weaknesses listed in the Other Accompanying Information Section of this report.

The Department's approach for implementing Appendix A of OMB Circular No A-123 focused on implementing corrective actions to obtain a qualified audit opinion on its balance sheet. Due to the five material weaknesses listed in the Other Accompanying Information Section of this report, the Department is unable to provide assurance that internal controls over financial reporting were operating effectively as of September 30, 2011. In addition, DHS does not currently have a consolidated financial management system that conforms to the objectives of FMFIA Section 4 and the *Federal Financial Management Improvement Act*.

At the inception of DHS, the U.S. Government Accountability Office reported 18 legacy material weaknesses in internal control over financial reporting. Last year, I committed the Department to obtain a qualified audit opinion of the Balance Sheet and Statement of Custodial Activity. Based on the quality, dedication, professionalism, and hard work of the U.S. Coast Guard, the DHS Office of the Chief Financial Officer, and Components across the Department who continue to improve financial management, we have met that commitment. The result of the FY 2011 financial statement audit is a significant milestone that highlights how we have significantly improved financial management at DHS. The Department has reduced our material weaknesses in internal controls over financial reporting to five. Looking forward, to further demonstrate our commitment, we are concentrating our efforts on expanding the scope of our audit to our remaining Statements of Budgetary Resources, Net Cost, and Changes in Net Position in FY 2012. We will continue to ensure taxpayer dollars are managed with integrity, diligence, and accuracy, and that the systems and processes used for all aspects of financial management demonstrate the highest level of accountability and transparency.


Janet Napolitano
Secretary, Department of Homeland Security



Federal Financial Management Improvement Act

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

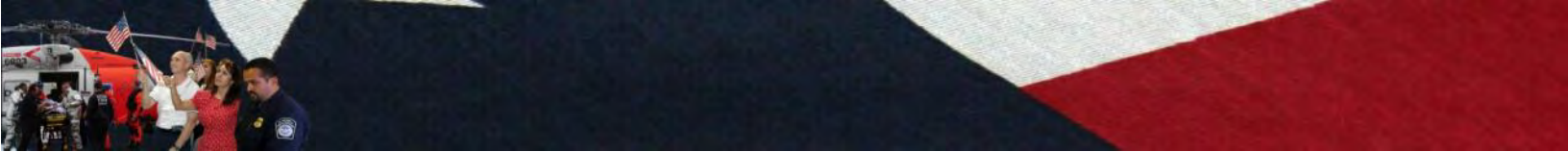
- Federal financial management system requirements;
- Applicable federal accounting standards; and
- The U.S. Standard General Ledger at the transaction level.

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

Financial Management Systems

Since it was created in 2003, DHS has worked to modernize its financial systems. DHS has twice launched efforts to do so, first under an approach called eMerge² and then Transformation and Systems Consolidation (TASC). The most recent effort concluded in March 2011, with the Government Accountability Office sustaining a bid protest that challenged the award of the contract to implement a Department-wide financial, asset, and acquisition management system. Following this decision, and a recognition that our requirements have changed, DHS cancelled the TASC program. In keeping with the Deputy Secretary's information technology efficiency direction and OMB's financial system reform guidance, as well as acknowledging the current austere fiscal environment, DHS is currently working on a more measured approach as the most prudent way forward.

The Department will leverage the work done to prepare for TASC and continue to work with Components to standardize business processes and internal controls, implement a common line of accounting, maintain data quality standards, and provide oversight and approval for any proposed efforts for financial system upgrade or replacement projects. The Office of the Chief Financial Officer (OCFO) along with the Office of the Chief Information Officer, Office of the Chief Procurement Officer, Program Accountability and Risk Management, and Components will work together to ensure programs are planned and executed to meet reporting requirements, minimize costs for financial operations, and make certain, consistent with the intent of the *DHS Financial Accountability Act*, that financial management systems provide for the systematic measurement of performance and have management controls in place to support the DHS mission. The Department will continue to lead this effort by providing guidance and policy for financial system modernization projects, the first of which will be issued in the near future. In addition, the Department will continue to work with all Components to ensure financial systems meet Government-wide requirements.



Federal Information Security Management Act (FISMA)

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 2010 Federal Information Security Management Act Report* and *Privacy Management Report* consolidates reports from three DHS offices:

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

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, the OIG reported that DHS continued to improve its information security program during FY 2011. For example, the CISO:

- Developed the *DHS IT Security Continuous Monitoring Strategy: An Enterprise View in January 2011*. This document outlined the Department's strategy for implementing an enterprise-wide continuous monitoring and response capability for IT security.
- Revised 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 Institute of Standards and Technology (NIST) guidance.
- Revised the FISMA scorecard to better evaluate the Department's information security program with increased emphasis on continuous monitoring, further aligning with OMB and NIST priorities. The revised FISMA scorecard includes asset reporting, security authorization, weakness management, vulnerability management, configuration management, Security Operations Center effectiveness, and log integration. These seven metrics contribute to the Component's overall information security grade.

The OIG report, "Evaluation of DHS' Information Security Program for Fiscal Year 2011," identified five recommendations for information security improvements. DHS plans to update the DHS Information Security Performance Plan with enhanced metrics, further improving compliance in these areas.