



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 Secretary	2
Management’s Discussion and Analysis.....	5
Mission and Organization.....	6
Implementing 9/11 Commission Recommendations – Executive Summary	7
Performance Overview	11
Financial Overview	27
Management Assurances	33
<i>Secretary’s Assurance Statement</i>	34
Financial Information	37
Message from the Deputy Chief Financial Officer	38
Introduction	40
Financial Statements.....	41
<i>Balance Sheets</i>	41
<i>Statements of Net Cost</i>	43
<i>Statements of Changes in Net Position</i>	45
<i>Statements of Budgetary Resources</i>	47
<i>Statements of Custodial Activity</i>	49
Notes to the Financial Statements	50
Required Supplementary Stewardship Information	119
Required Supplementary Information	124
Independent Auditors’ Report	132
Other Accompanying Information	183
Tax Burden/Tax Gap	184
Summary of Financial Statement Audit and Management Assurances	185
Improper Payments Information Act.....	193
Other Key Regulatory Requirements	212
Major Management Challenges Facing the Department of Homeland Security.....	213
<i>Management’s Response</i>	246
Acronym List	270

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

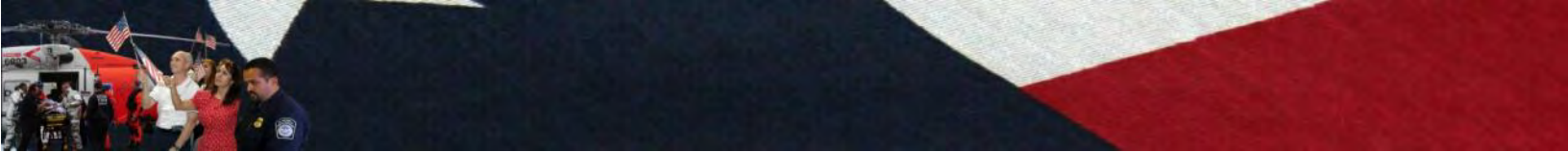
DHS provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready 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

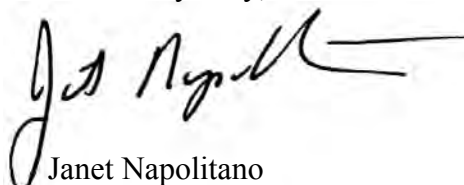
Pursuant to the *Department of Homeland Security Financial Accountability Act*, in FY 2011, the Department focused its efforts on eliminating audit qualifications and executing corrective actions to strengthen Department-wide internal controls over financial reporting. As I wrote last year, we concentrated 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,



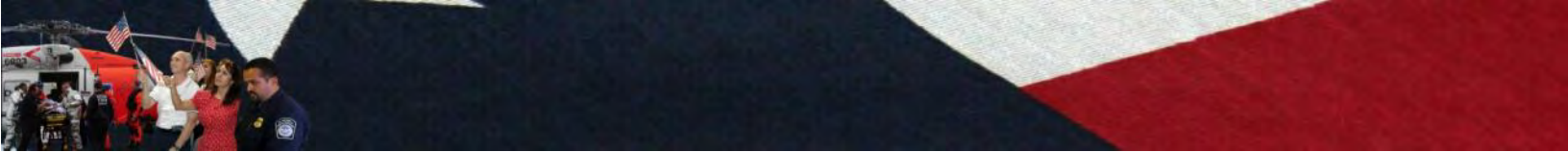
Janet Napolitano



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

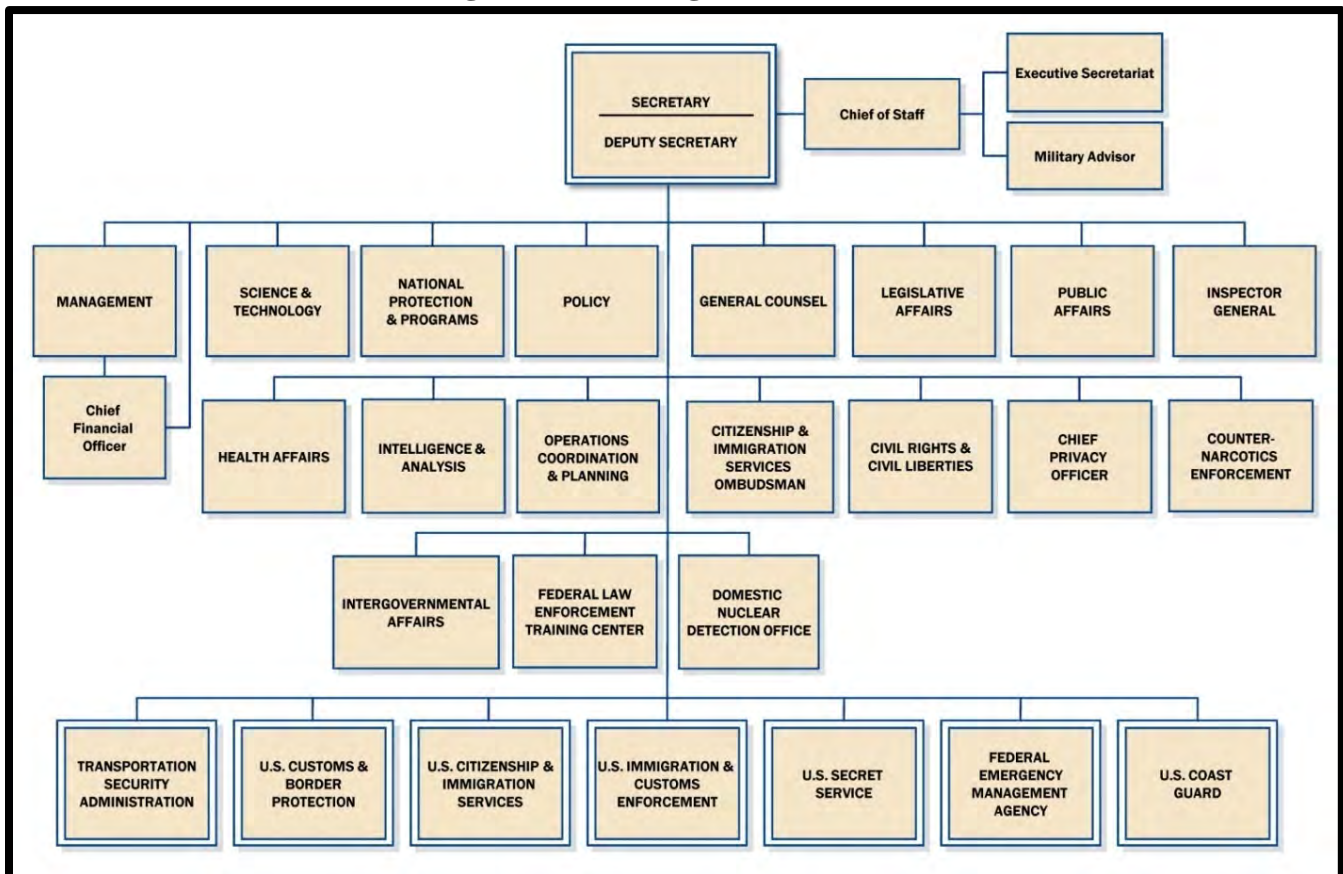
Mission

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>.

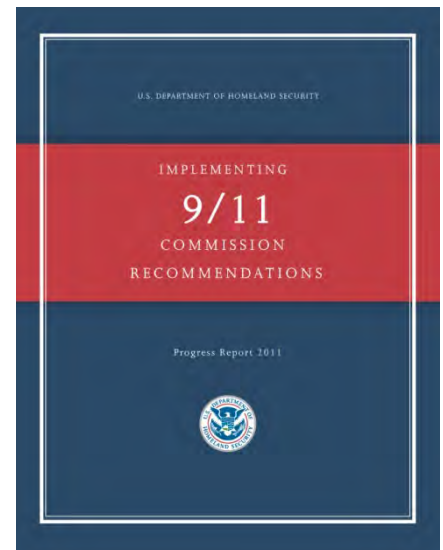
Figure 1. DHS Organization Chart





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>.



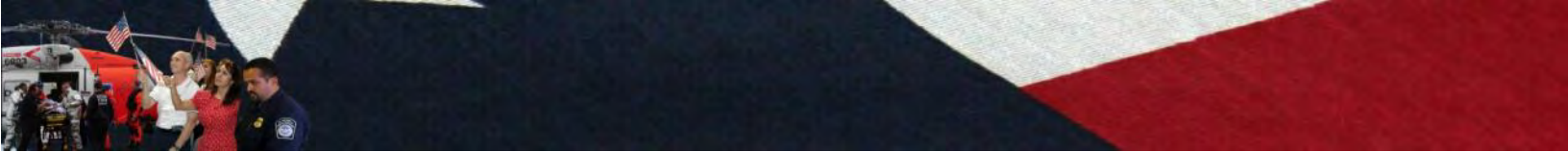
Overview

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

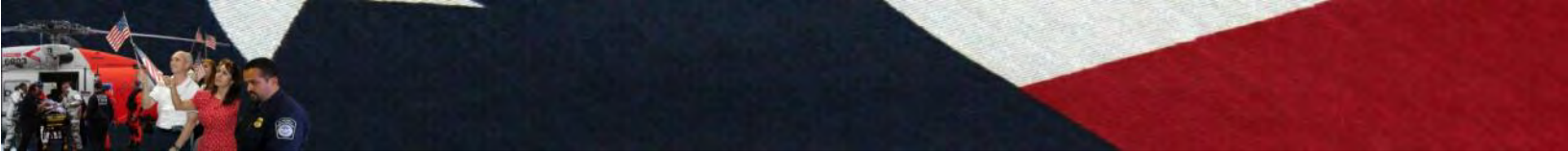
Prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today all checked and carry-on baggage is screened for explosives. The capacity of frontline security personnel and new technologies also has significantly expanded. In March 2002, TSA's first cadre of federal 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

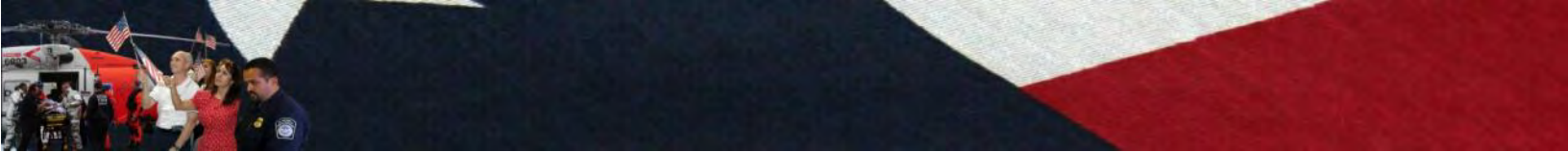
As part of its commitment to maintain a high level of security while enhancing passenger privacy, the Transportation Security Administration (TSA) is currently in the process of installing new software to further strengthen the privacy protections on its Advanced Imaging Technology (AIT) machines. The 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:

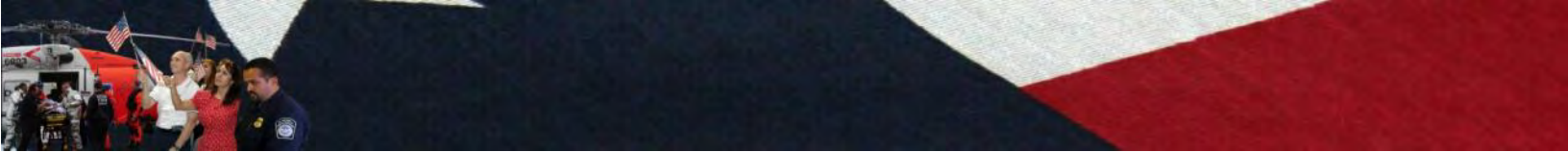
- Understand the current and emerging terrorist threats to the United States, build capability at the state, local, tribal, and territorial level to prevent and disrupt terrorist attacks through programs such as the Nationwide Suspicious Activities Reporting Initiative, and engage communities through 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.

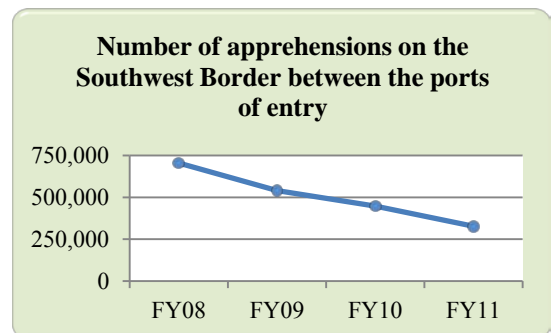
As a result, Secretary Napolitano directed CBP to end SBI^{net} as originally conceived and instead implement a new border security technology plan, which will use existing, proven technology tailored to the distinct terrain and population density of each border region, including commercially available 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.

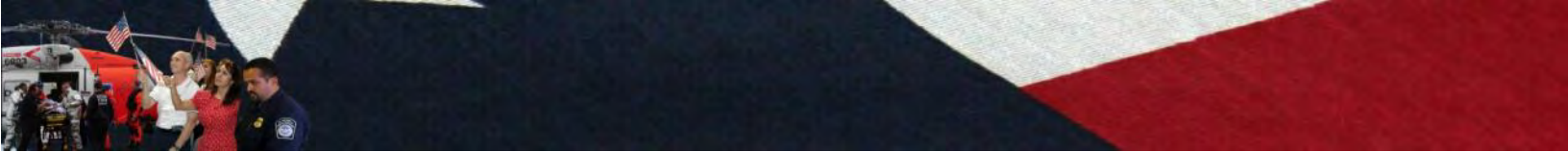
Through the Integrated Cross-Border Maritime Law Enforcement Operations Shiprider agreement, DHS and Canadian joint law enforcement can leverage efforts to bolster cross-border security operations. This agreement enables the Royal Canadian Mounted Police, U.S. Coast Guard, CBP, and Immigration and Customs 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.

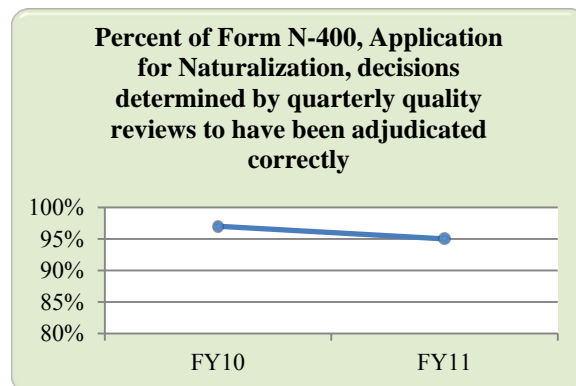
Below are highlighted performance measures related to *Enforcing and Administering Our Immigration Laws*. A complete list of all the performance measures, with full descriptions and explanations, will be published in the DHS Annual Performance Report in February 2012.

- **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.

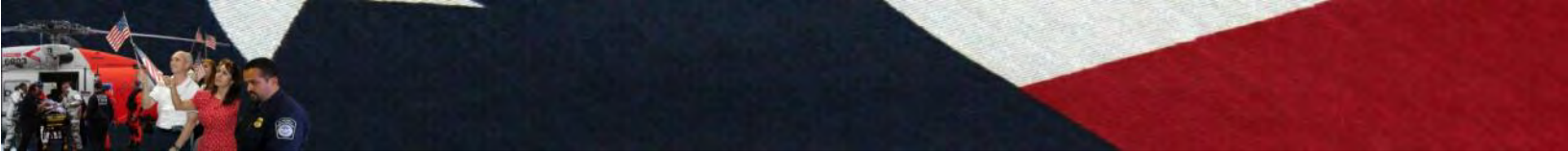


ICE Removes Former Member of Guatemalan Army Linked to Massacre

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

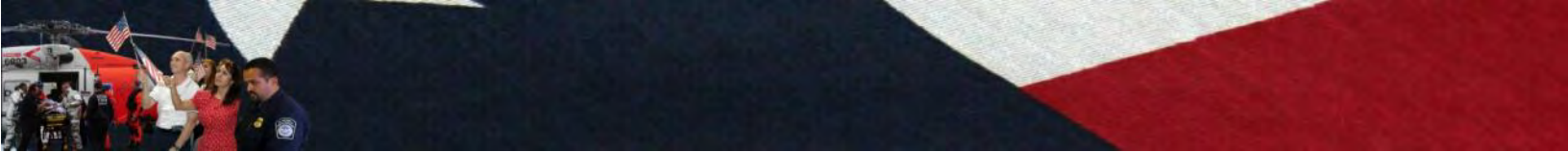
In March 2011, a U.S. oil and natural gas organization was victimized by a series of successful cybersecurity attacks, and subsequently contacted the Federal Bureau of Investigation (FBI). Under the framework established in the National Cybersecurity Incident Response Plan, the FBI reached out to DHS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

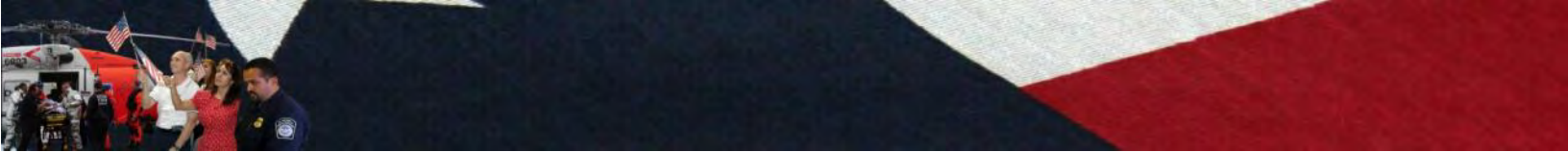
In a disaster situation, communications between the Federal Emergency Management Agency (FEMA), federal, state, and local agencies is critical. It is important that members of the emergency management team communicate with one another in real time during life saving operations and recovery efforts. In 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.

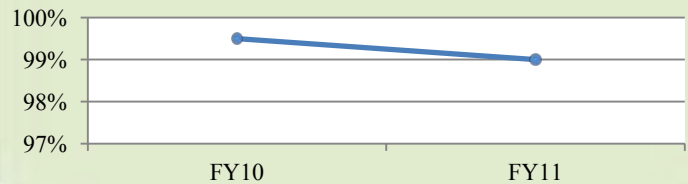
- **Percent of time that critical communications for response operations are established within 12 hours:** This measure reflects the percent of time that critical communications are established for FEMA's on-site emergency responders within 12 hours of the deployment of Mobile Emergency Response Support. 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:

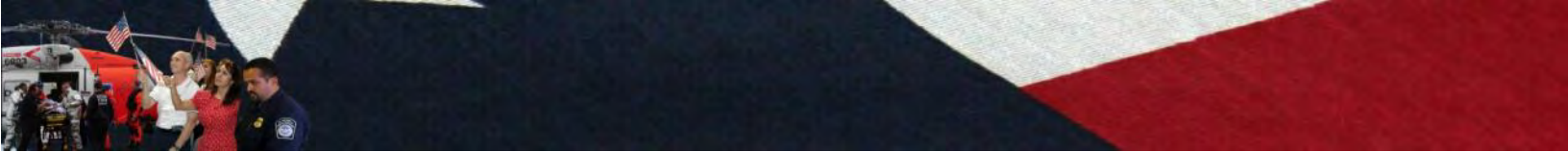
- Continue the dissemination of plans and preparedness standards through training and technical assistance, and validate their effectiveness through exercises.
- Sustain federal funding for state and local preparedness grants, highlighting the Department's commitment to moving resources out of Washington, 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

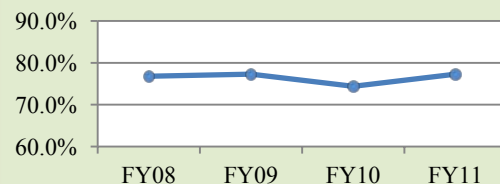
Imports of polished granite from Brazil and India were often misclassified in order to claim Generalized System of Preferences (GSP), a trade preference program which allows for significantly diminished duty rates. CBP conducted Operation Stone Face I in 2008 which targeted those imports. The Operation 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.



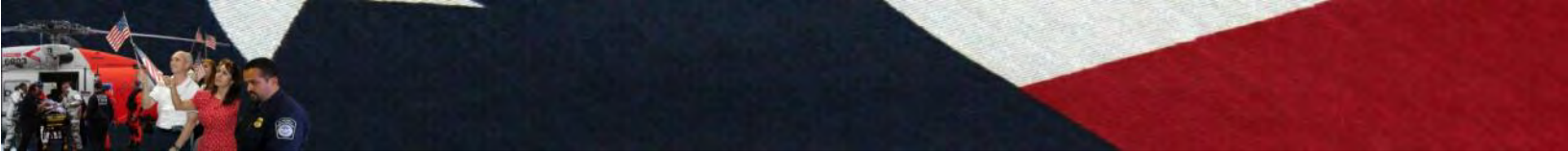
Improved Efficiency

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.

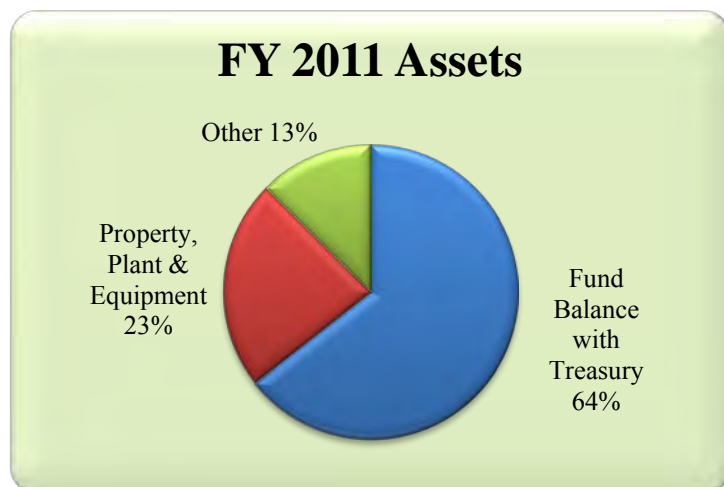
Balance Sheet

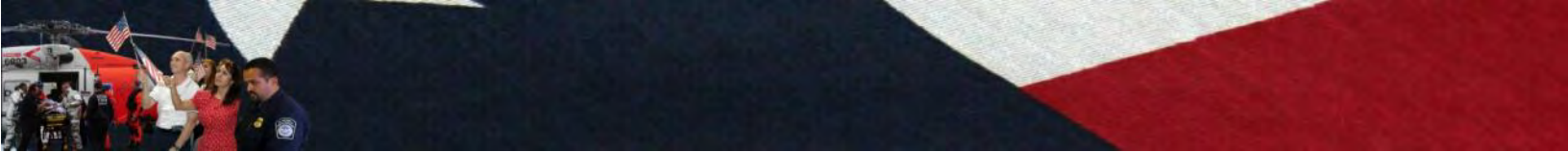
The Balance Sheet presents the resources owned or managed by DHS that have future economic benefits (assets) and the amounts owed by DHS that will require future payments (liabilities). The difference between DHS’s assets and liabilities is the residual amount retained by DHS (net position) that is available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

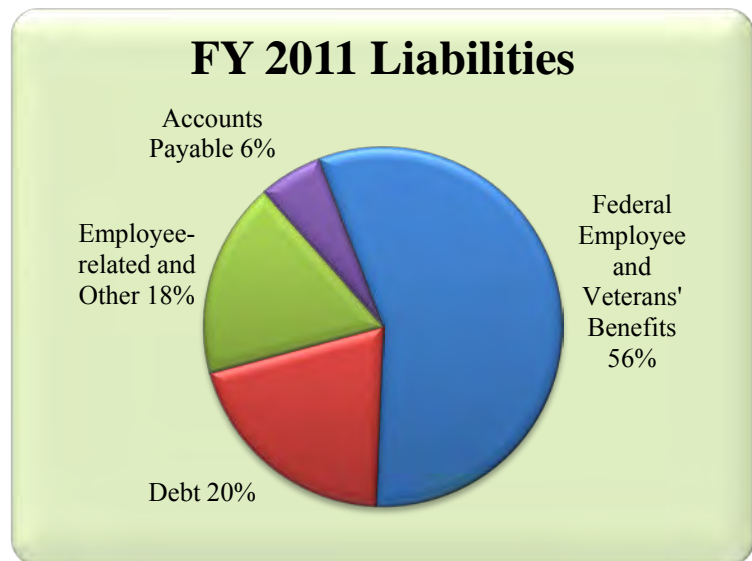
DHS’s largest liability is for Federal Employee and Veterans’ Benefits, representing 56 percent of total liabilities. This liability increased approximately \$1 billion from FY 2010. This increase primarily relates to U.S. Coast Guard changing its discount rate and assumptions used to calculate the Retired 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.

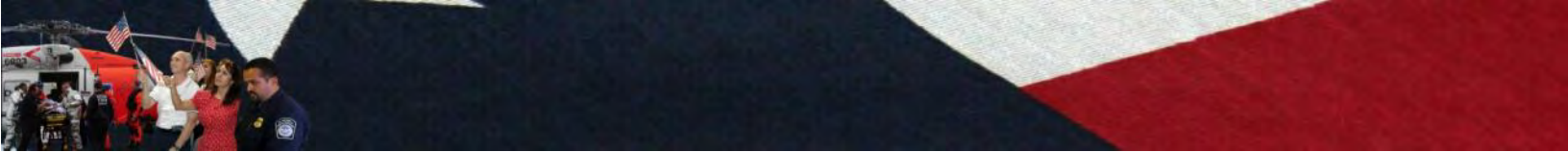
Debt is DHS's second-largest liability, representing 20 percent of total liabilities. This debt results from Department of Treasury loans and related interest payable to fund the National Flood Insurance Program (NFIP) and Disaster Assistance Direct Loan Program operations of FEMA. Total debt decreased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



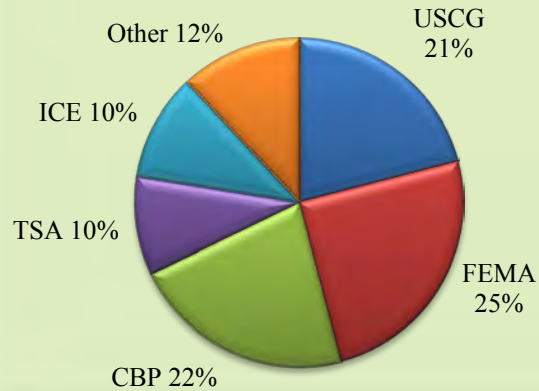
percent of the total and went to promoting homeland security and public safety through enforcement of federal laws governing border control, customs, trade, and immigration.

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.

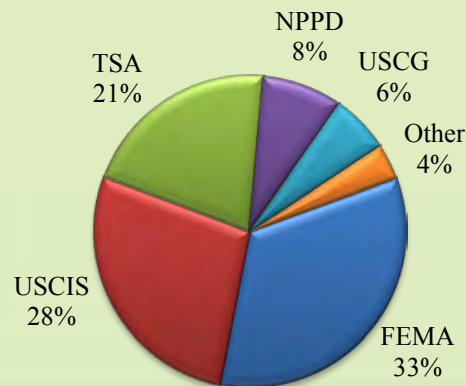
Statement of Changes in Net Position

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.

FY 2011 Composition of Net Costs



FY 2011 Composition of Earned Revenue



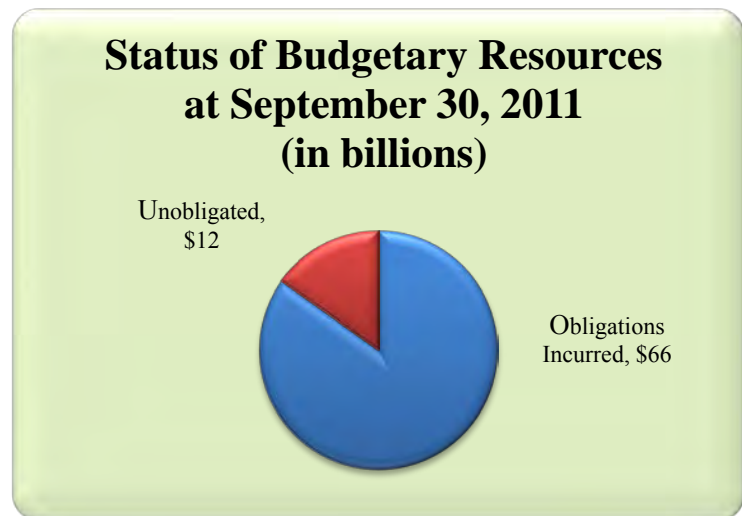
TSA made key investments in aviation security during FY 2011, including portable ETD machines.



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.



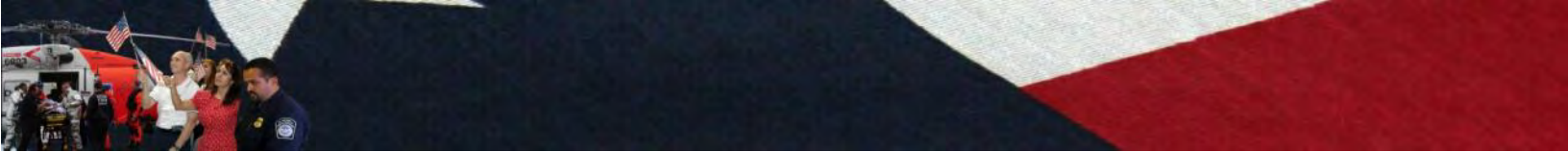
Of the total budget authority available, DHS incurred a total of \$66 billion in obligations from purchase orders placed, contracts awarded, salaries and benefits, or similar transactions. These obligations will require payments during the same or future period. As of September 30, 2011, \$12 billion 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:

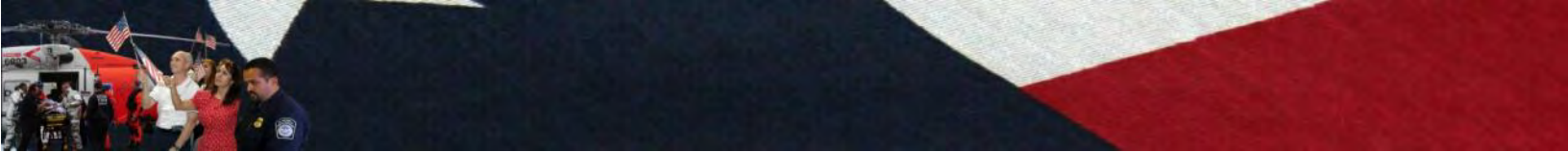
- Federal financial management system requirements;
- Applicable federal accounting standards; and
- The U.S. Standard General Ledger at the transaction level.

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.



Financial Information

The *Financial Information* section demonstrates our commitment to effective stewardship over the funds DHS receives to carry out its mission, including compliance with relevant financial management legislation. It includes the *Independent Auditors' Report*—an independent auditors' report on the Balance Sheet and Statement of Custodial Activity—as well as the Department's *Annual Financial Statements* and accompanying *Notes to the Financial Statements*. The audit report is provided by the Department's Office of Inspector General.

Message from the Deputy Chief Financial Officer

November 11, 2011



This Annual Financial Report is our principal financial statement of accountability to the American taxpayer, the President of the United States, and the Congress, and demonstrates the Department of Homeland Security's commitment to ensuring strong financial management and proper stewardship of taxpayer dollars.

Since the Department stood up in 2003, we have worked diligently to strengthen financial management to support our mission and to produce timely, reliable financial data in support of a clean audit. We have developed strong policies and internal controls and critical workforce training programs—fundamental building blocks for effective financial management. Using the internal control tools provided by the *DHS Financial Accountability Act*, we have established a culture of integrity, accountability, and risk management in all that we do. From the start, we

designed our corrective actions to build on previous successes and to ensure we could sustain improvements made in prior years. The results of the FY 2011 financial statement audit demonstrate that DHS financial management continues to improve. Since FY 2005, the Department has reduced material weaknesses in internal controls over financial reporting by half.

In January 2011, Secretary Napolitano committed to obtaining an opinion on the Consolidated Balance Sheet and the Statement of Custodial Activity this fiscal year. We set the bar high, declaring FY 2011 “The Year of the Opinion,” and for the first time since FY 2003, we can report that most of the line items in Department's Consolidated Balance Sheet are materially correct. This opinion is a pivotal step to increasing transparency and accountability and accurately accounting for the Department's resources.

Our success is possible largely because of impressive improvements at the U.S. Coast Guard. Four years ago, the U.S. Coast Guard had disclaimer conditions on all its balances. By executing corrective action plans, implementing new processes, and monitoring audit risk throughout the fiscal year, the U.S. Coast Guard can now assert to more than 80 percent of its balance sheet. For the first time, the independent auditors were able to audit Fund Balance with Treasury, Accounts Payable, Accounts Receivable, and Undelivered Orders at Coast Guard. In that sense, we view FY 2011 as the first year the Department has undergone a complete audit of its balance sheet, from stem to stern.

The U.S. Coast Guard set, and achieved, ambitious goals to be able to support the financial statement line items that have the greatest impact on the Department's balance sheet. This accomplishment—driven by strong leadership and continued commitment to developing the expertise of its financial management workforce—put the Department on a path to attaining an opinion on the Consolidated Balance Sheet and the Statement of Custodial Activity.

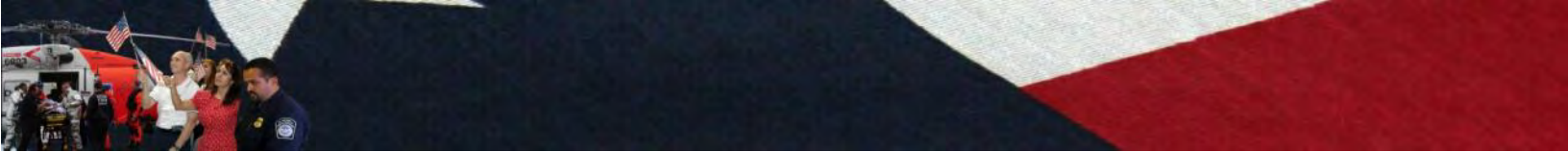


DHS Components have worked hard to sustain prior-year progress and will continue to anticipate and mitigate additional audit risks as we prepare for new challenges in FY 2012. We are now well-positioned to expand the audit to all financial statements, moving us closer to our goal of obtaining a clean opinion on a full-scope audit. Continued diligence from senior leadership and financial managers across the Department is vital as we work toward our audit goals for FY 2012 and beyond.

I am extremely proud of the dedication, hard work, and historic achievements of the DHS financial management community this year. We will continue to demonstrate our commitment to good governance as we strengthen and mature financial management across the Department.

Sincerely,

Peggy Sherry
Deputy Chief Financial Officer



Introduction

The principal financial statements included in this report are prepared pursuant to the requirements of the *Government Management Reform Act of 1994* (Pub. L. 103-356) and the *Chief Financial Officers Act of 1990* (Pub. L. 101-576), as amended by the *Reports Consolidation Act of 2000* (Pub. L. 106-531), and the *Department of Homeland Security Financial Accountability Act of 2004* (Pub. L. 108-330). Other requirements include the Office of Management and Budget (OMB) Circular No. A-136, *Financial Reporting Requirements*, as amended. The responsibility for the integrity of the financial information included in these statements rests with the management of DHS. The Department's Inspector General selected an independent certified public accounting firm to audit the Balance Sheet and the Statement of Custodial Activity and Internal Controls over Financial Reporting. The independent auditors' report accompanies the principal financial statements. These financial statements include the following:

- The **Balance Sheets** present, as of September 30, 2011 and 2010, those resources owned or managed by DHS that represent future economic benefits (assets), amounts owed by DHS that will require payments from those resources or future resources (liabilities), and residual amounts retained by DHS comprising the difference (net position).
- The **Statements of Net Cost** present the net cost of DHS operations for the fiscal years ended September 30, 2011 and 2010. DHS net cost of operations is the gross cost incurred by DHS less any exchange revenue earned from DHS activities.
- The **Statements of Changes in Net Position** present the change in DHS's net position resulting from the net cost of DHS operations, budgetary financing sources, and other financing sources for the fiscal years ended September 30, 2011 and 2010.
- The **Statements of Budgetary Resources** present how and in what amounts budgetary resources were made available to DHS during FY 2011 and FY 2010, the status of these resources at September 30, 2011 and 2010, the changes in the obligated balance, and outlays of budgetary resources for the fiscal years ended September 30, 2011 and 2010.
- The **Statements of Custodial Activity** present the disposition of custodial revenue collected and disbursed by DHS on behalf of other recipient entities for the fiscal years ended September 30, 2011 and 2010.
- The **Notes to the Financial Statements** provide detail and clarification for amounts on the face of the financial statements for the fiscal years ended September 30, 2011 and 2010.

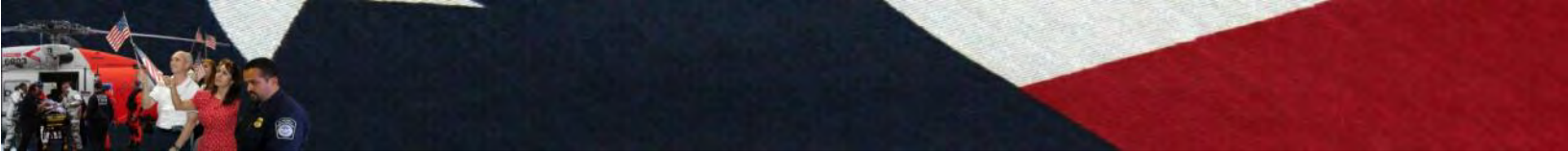


Financial Statements

**Department of Homeland Security
Balance Sheets
As of September 30, 2011 and 2010
(In Millions)**

	<u>2011</u>	<u>2010</u> (Unaudited)
ASSETS		
Intragovernmental		
Fund Balance with Treasury (Notes 2 and 3)	\$55,960	\$60,822
Investments, Net (Note 5)	4,159	3,482
Accounts Receivable (Note 6)	271	326
Other (Note 13)		
Advances and Prepayments	1,832	2,225
Total Intragovernmental	\$62,222	\$66,855
Cash and Other Monetary Assets (Notes 2 and 4)	76	61
Accounts Receivable, Net (Notes 2 and 6)	645	491
Taxes, Duties, and Trade Receivables, Net (Notes 2 and 7)	2,732	2,459
Direct Loans, Net (Note 8)	10	85
Inventory and Related Property, Net (Note 9)	527	499
General Property, Plant, and Equipment, Net (Note 11)	20,037	19,074
Other (Note 13)		
Advances and Prepayments	640	573
TOTAL ASSETS	\$86,889	\$90,097
Stewardship Property, Plant, and Equipment (Note 12)		
LIABILITIES		
Intragovernmental		
Accounts Payable	\$2,154	\$2,174
Debt (Note 15)	17,754	18,505
Other (Note 18)		
Due to the General Fund	2,844	2,475
Accrued FECA Liability	374	374
Other	532	501
Total Intragovernmental	\$23,658	\$24,029
Accounts Payable	2,853	2,571
Federal Employee and Veterans' Benefits (Note 16)	49,664	48,317
Environmental and Disposal Liabilities (Note 17)	1,047	1,061
Other (Notes 18, 19, 20, and 21)		
Accrued Payroll and Benefits	2,198	2,217
Deferred Revenue and Advances from Others	2,716	2,650
Insurance Liabilities	3,537	482

Department of Homeland Security



Balance Sheets
As of September 30, 2011 and 2010
(In Millions)

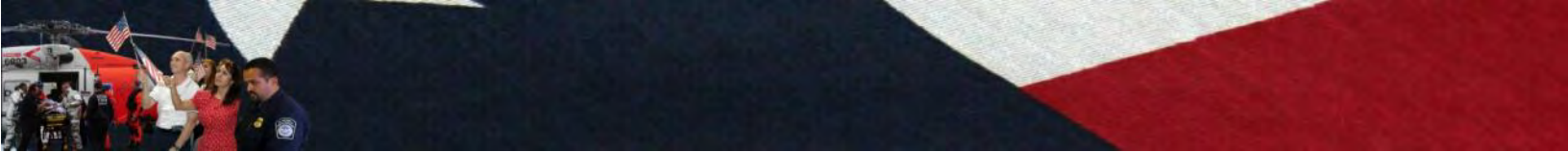
	<u>2011</u>	<u>2010</u> (Unaudited)
Refunds and Drawbacks	131	129
Other	2,143	2,140
Total Liabilities	\$87,947	\$83,596
Commitments and Contingencies (Notes 18, 19, 20, and 21)		
NET POSITION		
Unexpended Appropriations		
Unexpended Appropriations-Other Funds	\$45,274	\$51,612
Cumulative Results of Operations		
Cumulative Results of Operations-Earmarked Funds (Note 22)	(14,840)	(13,816)
Cumulative Results of Operations-Other Funds	(31,492)	(31,295)
Total Net Position	\$(1,058)	\$6,501
TOTAL LIABILITIES AND NET POSITION	\$86,889	\$90,097

The accompanying notes are an integral part of these statements.



Department of Homeland Security
Statements of Net Cost
For the Years Ended September 30, 2011 and 2010
(In Millions)

Directorates and Other Components (Notes 23 and 24)	<u>2011</u> (Unaudited)	<u>2010</u> (Unaudited)
<i>U.S. Customs and Border Protection</i>		
Gross Cost	\$12,042	\$11,775
Less Earned Revenue	(178)	(152)
Net Cost	<u>11,864</u>	<u>11,623</u>
<i>U.S. Coast Guard</i>		
Gross Cost	11,689	12,975
Less Earned Revenue	(668)	(897)
Net Cost	<u>11,021</u>	<u>12,078</u>
<i>U.S. Citizenship and Immigration Services</i>		
Gross Cost	2,513	2,531
Less Earned Revenue	(3,046)	(2,418)
Net Cost	<u>(533)</u>	<u>113</u>
<i>Federal Emergency Management Agency</i>		
Gross Cost	17,158	14,207
Less Earned Revenue	(3,705)	(3,681)
Net Cost	<u>13,453</u>	<u>10,526</u>
<i>Federal Law Enforcement Training Center</i>		
Gross Cost	441	410
Less Earned Revenue	(37)	(36)
Net Cost	<u>404</u>	<u>374</u>
<i>National Protection and Programs Directorate</i>		
Gross Cost	2,417	2,061
Less Earned Revenue	(914)	(828)
Net Cost	<u>1,503</u>	<u>1,233</u>
<i>U.S. Immigration and Customs Enforcement</i>		
Gross Cost	5,763	5,750
Less Earned Revenue	(149)	(229)
Net Cost	<u>5,614</u>	<u>5,521</u>



Department of Homeland Security
Statements of Net Cost
For the Years Ended September 30, 2011 and 2010
(In Millions)

Directorates and Other Components (Notes 23 and 24)	<u>2011</u> (Unaudited)	<u>2010</u> (Unaudited)
<i>Office of Health Affairs</i>		
Gross Cost	290	231
Less Earned Revenue	-	-
Net Cost	290	231
<i>Departmental Operations and Other</i>		
Gross Cost	1,924	1,880
Less Earned Revenue	(8)	(6)
Net Cost	1,916	1,874
<i>U.S. Secret Service</i>		
Gross Cost	1,848	1,782
Less Earned Revenue	(14)	(15)
Net Cost	1,834	1,767
<i>Science and Technology Directorate</i>		
Gross Cost	888	887
Less Earned Revenue	(18)	(5)
Net Cost	870	882
<i>Transportation Security Administration</i>		
Gross Cost	7,469	6,631
Less Earned Revenue	(2,279)	(2,145)
Net Cost	5,190	4,486
<i>Total Department of Homeland Security</i>		
Gross Cost	64,442	61,120
Less Earned Revenue	(11,016)	(10,412)
Net Cost Before Loss on Pension, ORB, or OPEB	53,426	50,708
Assumption Changes	53,426	50,708
Loss on Pension, ORB, or OPEB Assumption Changes (Note 16)	400	5,675
NET COST OF OPERATIONS	\$53,826	\$56,383

The accompanying notes are an integral part of these statements.



Department of Homeland Security
Statement of Changes in Net Position
For the Year Ended September 30, 2011
(In Millions)

	2011 (Unaudited)			Consolidated Total
	Earmarked Funds	All Other Funds	Eliminations	
Cumulative Results of Operations				
Beginning Balances	\$(13,816)	\$(31,295)	\$ -	\$(45,111)
Budgetary Financing Sources				
Appropriations Used	-	47,840	-	47,840
Non-exchange Revenue	1,735	8	-	1,743
Donations and Forfeitures of Cash and Cash Equivalents	3	-	-	3
Transfers In/Out Without Reimbursement	(2,546)	1,909	-	(637)
Other Financing Sources				
Transfers In/Out Without Reimbursement	(70)	184	-	114
Imputed Financing	70	1,644	192	1,522
Other	2,249	(229)	-	2,020
Total Financing Sources	1,441	51,356	192	52,605
Net Cost of Operations	(2,465)	(51,553)	(192)	(53,826)
Net Change	(1,024)	(197)	-	(1,221)
Cumulative Results of Operations	(14,840)	(31,492)	-	(46,332)
Unexpended Appropriations				
Beginning Balance	-	51,612	-	51,612
Budgetary Financing Sources				
Appropriations Received	-	42,704	-	42,704
Appropriations Transferred In/Out	-	61	-	61
Other Adjustments	-	(1,263)	-	(1,263)
Appropriations Used	-	(47,840)	-	(47,840)
Total Budgetary Financing Sources	-	(6,338)	-	(6,338)
Total Unexpended Appropriations	-	45,274	-	45,274
NET POSITION	\$(14,840)	\$13,782	\$ -	\$(1,058)

The accompanying notes are an integral part of these statements.

Department of Homeland Security
Statement of Changes in Net Position
For the Year Ended September 30, 2010
(In Millions)

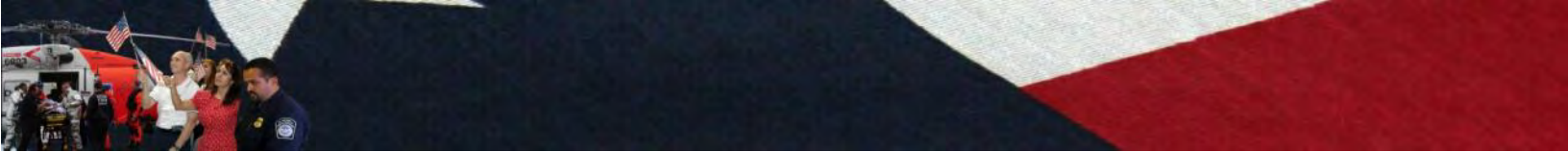
	2010 (Unaudited)			Consolidated Total
	Earmarked Funds	All Other Funds	Eliminations	
Cumulative Results of Operations				
Beginning Balances	\$(15,410)	\$(23,571)	\$ -	\$(38,981)
Budgetary Financing Sources				
Appropriations Used	-	45,757	-	45,757
Non-exchange Revenue (Note 32)	1,607	5	-	1,612
Donations and Forfeitures of Cash and Cash Equivalents	2	-	-	2
Transfers In/Out Without Reimbursement	(1,964)	1,738	-	(226)
Other	(5)	-	-	(5)
Other Financing Sources				
Donations and Forfeitures of Property	-	3	-	3
Transfers In/Out Without Reimbursement	(13)	133	-	120
Imputed Financing	76	1,179	191	1,064
Other (Note 32)	2,004	(78)	-	1,926
Total Financing Sources	1,707	48,737	191	50,253
Net Cost of Operations	(113)	(56,461)	(191)	(56,383)
Net Change	1,594	(7,724)	-	(6,130)
Cumulative Results of Operations	(13,816)	(31,295)	-	(45,111)
Unexpended Appropriations				
Beginning Balances	-	49,283	-	49,283
Budgetary Financing Sources				
Appropriations Received	-	48,824	-	48,824
Appropriations Transferred In/Out	-	47	-	47
Other Adjustments	-	(785)	-	(785)
Appropriations Used	-	(45,757)	-	(45,757)
Total Budgetary Financing Sources	-	2,329	-	2,329
Total Unexpended Appropriations	-	51,612	-	51,612
NET POSITION	\$(13,816)	\$20,317	\$ -	\$6,501

The accompanying notes are an integral part of these statements.



Department of Homeland Security
Statements of Budgetary Resources
For the Years Ended September 30, 2011 and 2010
(In Millions)

	<u>2011</u> (Unaudited)		<u>2010</u> (Unaudited)	
	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Budgetary	Non-Budgetary Credit Reform Financing Accounts
BUDGETARY RESOURCES				
Unobligated Balance, Brought Forward, October 1	\$15,188	\$ -	\$13,383	\$ -
Recoveries of Prior Year Unpaid Obligations	4,492	35	4,463	-
Budget Authority:				
Appropriations	50,110	-	55,852	-
Spending Authority from Offsetting Collections:				
Earned:				
Collected	10,338	37	9,913	33
Change in Receivables from Federal Sources	5	-	(79)	-
Change in Unfilled Customer Orders:				
Advances Received	(28)	-	(230)	-
Without Advance from Federal Sources	(159)	(37)	418	(33)
Previously Unavailable	35	-	30	-
Expenditure Transfers from Trust Funds	48	-	48	-
Subtotal	60,349	-	65,952	-
Nonexpenditure Transfers, Net	510	-	1,105	-
Temporarily Not Available Pursuant to Public Law	(41)	-	(32)	-
Permanently Not Available	(2,109)	-	(1,671)	-
TOTAL BUDGETARY RESOURCES	\$78,389	\$35	\$83,200	\$ -
STATUS OF BUDGETARY RESOURCES				
Obligations Incurred (Note 25):				
Direct	\$61,666	\$2	\$63,344	\$ -
Reimbursable	4,870	-	4,668	-
Subtotal	66,536	2	68,012	-
Unobligated Balance:				
Apportioned	6,667	-	10,190	-
Exempt from Apportionment	6	-	5	-
Subtotal (Note 3)	6,673	-	10,195	-
Unobligated Balance Not Available (Note 3)	5,180	33	4,993	-
TOTAL STATUS OF BUDGETARY RESOURCES	\$78,389	\$35	\$83,200	\$ -



**Department of Homeland Security
Statements of Budgetary Resources
For the Years Ended September 30, 2011 and 2010
(In Millions)**

	<u>2011</u> (Unaudited)		<u>2010</u> (Unaudited)	
	Budgetary	Non- Budgetary Credit Reform Financing Accounts	Budgetary	Non- Budgetary Credit Reform Financing Accounts
CHANGE IN OBLIGATED BALANCE				
Obligated Balance, Net				
Unpaid Obligations Brought Forward, October 1	\$48,641	\$261	\$46,764	\$294
Uncollected Customer Payments from Federal Sources, Brought Forward, October 1	(2,384)	(260)	(2,044)	(293)
Total Unpaid Obligated Balance, Net	46,257	1	44,720	1
Obligations Incurred, Net	66,536	2	68,012	-
Gross Outlays	(63,581)	(20)	(61,646)	(34)
Obligated Balance Transferred, Net				
Actual Transfers, Unpaid Obligations	(22)	-	(26)	-
Total Unpaid Obligated Balance Transferred, Net	(22)	-	(26)	-
Recoveries of Prior Year Unpaid Obligations, Actual Change in Uncollected Customer Payments from Federal Sources	(4,492) 154	(35) 37	(4,463) (340)	- 34
Obligated Balance, Net, End of Period				
Unpaid Obligations	47,082	208	48,641	261
Uncollected Customer Payments from Federal Sources	(2,230)	(223)	(2,384)	(260)
Total, Unpaid Obligated Balance, Net, End of Period	\$44,852	\$(15)	\$46,257	\$1
NET OUTLAYS				
Gross Outlays	\$63,581	\$20	\$61,646	\$34
Offsetting Collections	(10,359)	(37)	(9,731)	(33)
Distributed Offsetting Receipts	(6,246)	-	(6,328)	-
NET OUTLAYS	\$46,976	\$(17)	\$45,587	\$1

The accompanying notes are an integral part of these statements.



Department of Homeland Security
Statements of Custodial Activity
For the Years Ended September 30, 2011 and 2010
(In Millions)

	2011	2010 (Unaudited)
Revenue Activity (Note 31)		
Sources of Cash Collections:		
Duties	\$29,254	\$25,284
User Fees	1,533	1,508
Excise Taxes	2,894	2,880
Fines and Penalties	69	64
Interest	42	6
Miscellaneous	171	179
Total Cash Collections	33,963	29,921
Accrual Adjustments	339	636
Total Custodial Revenue	34,302	30,557
Disposition of Collections		
Transferred to Others:		
Federal Entities:		
U.S. Department of Agriculture	9,870	8,490
U.S. Department of Labor	-	146
U.S. Department of State	-	70
National Science Foundation	-	91
Treasury General Fund Accounts	22,495	19,749
Other Federal Agencies	28	27
Non-Federal Entities:		
Government of Puerto Rico	7	-
Government of the U.S. Virgin Islands	2	-
Other Non-Federal Entities	124	26
(Increase)/Decrease in Amounts Yet to be Transferred	428	597
Refunds and Drawbacks (Notes 18 and 31)	1,348	1,279
Retained by the Department	-	82
Total Disposition of Custodial Revenue	34,302	30,557
Net Custodial Activity	\$ -	\$ -

The accompanying notes are an integral part of these statements.

Notes to the Financial Statements

Table of Contents for Notes to the Financial Statements

Note No.	Title of Note	Page No.
1.	Summary of Significant Accounting Policies	51
<u>Notes Disclosures Related to the Balance Sheets</u>		
2.	Non-Entity Assets	67
3.	Fund Balance with Treasury	68
4.	Cash and Other Monetary Assets	70
5.	Investments, Net	71
6.	Accounts Receivable, Net	72
7.	Taxes, Duties, and Trade Receivables, Net	73
8.	Direct Loans, Net	73
9.	Inventory and Related Property, Net	77
10.	Seized and Forfeited Property	78
11.	General Property, Plant, and Equipment, Net	80
12.	Stewardship Property, Plant, and Equipment	82
13.	Other Assets	85
14.	Liabilities Not Covered by Budgetary Resources	86
15.	Debt	87
16.	Federal Employee and Veterans' Benefits	88
17.	Environmental and Disposal Liabilities	91
18.	Other Liabilities	92
19.	Leases	94
20.	Insurance Liabilities	96
21.	Commitments and Contingent Liabilities	96
22.	Earmarked Funds	98
<u>Notes Disclosures Related to the Statements of Net Cost</u>		
23.	Intragovernmental Costs and Exchange Revenue	106
24.	Suborganization Costs by DHS Missions and Goals	110
<u>Notes Disclosures Related to the Statements of Budgetary Resources</u>		
25.	Apportionment Categories of Obligations Incurred: Direct versus Reimbursable Obligations	111
26.	Available Borrowing Authority	111
27.	Permanent Indefinite Appropriations	111
28.	Legal Arrangements Affecting the Use of Unobligated Balances	112
29.	Explanation of Differences between the Statement of Budgetary Resources and the Budget of the U.S. Government	113
30.	Undelivered Orders, Unpaid, End of Period	114
<u>Notes Disclosures Related to the Statements of Custodial Activity</u>		
31.	Custodial Revenues	114
<u>Notes Disclosures Not Pertaining to a Specific Statement</u>		
32.	Reclassifications and Other Reporting Changes	115
33.	Reconciliation of Net Cost of Operations (Proprietary) to Budget	117



Notes to the Financial Statements

1. Summary of Significant Accounting Policies

A. Reporting Entity

The Department of Homeland Security (DHS or the Department) was established by the *Homeland Security Act of 2002* (HSA), Pub. L. 107-296, dated November 25, 2002, as an executive department of the U.S. Federal Government. DHS leads efforts to achieve a safe, secure, and resilient homeland by countering terrorism and enhancing our security; securing and managing our borders; enforcing and administering our immigration laws; protecting our cyber networks and critical infrastructure; and ensuring resilience from disasters. In addition, DHS contributes in many ways to elements of broader U.S. national and economic security while also working to mature and strengthen the Department and the homeland security enterprise. The Department includes the following financial reporting Components¹:

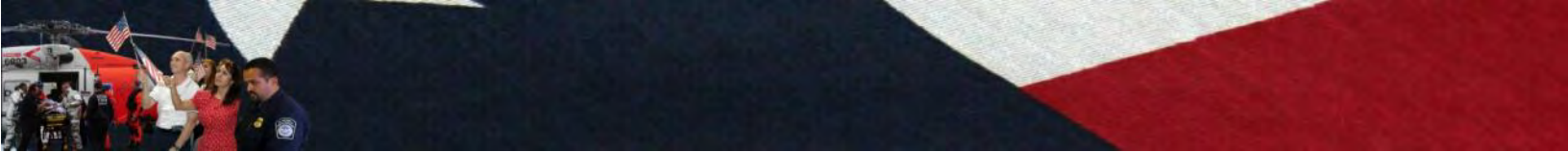
- **U.S. Customs and Border Protection (CBP)**
- **U.S. Coast Guard (USCG)**
- **U.S. Citizenship and Immigration Services (USCIS)**
- **Federal Emergency Management Agency (FEMA)**
- **Federal Law Enforcement Training Center (FLETC)**
- **National Protection and Programs Directorate (NPPD)**, including the Federal Protective Service (FPS)
- **U.S. Immigration and Customs Enforcement (ICE)**
- **Office of Health Affairs (OHA)**
- **Departmental Operations and Other**, including the Management Directorate (MGMT), the Office of the Secretary, the Office of the Inspector General (OIG), the Domestic Nuclear Detection Office (DNDO), the Office of Intelligence and Analysis, and the Office of Operations Coordination and Planning
- **U.S. Secret Service (USSS)**
- **Science and Technology Directorate (S&T)**
- **Transportation Security Administration (TSA)**

B. Basis of Presentation

These financial statements are prepared to report the consolidated financial position, net cost of operations, changes in net position, custodial activity, and combined budgetary resources of the Department pursuant to the *Government Management Reform Act of 1994* and the *Chief Financial Officers Act of 1990*, as amended by the *Reports Consolidation Act of 2000*.

The Department's financial statements have been prepared from the accounting records of the Department based on guidance in U.S. generally accepted accounting principles (GAAP) and OMB Circular A-136, *Financial Reporting Requirements*, as amended. GAAP for federal entities are the

¹ Financial reporting Components are to be distinguished from direct report Components presented in the Department's organization chart.



standards prescribed by the Federal Accounting Standards Advisory Board, the official accounting standards-setting body of the Federal Government.

The Department's financial statements reflect the reporting of Departmental activities, including appropriations received to conduct operations and revenue generated from operations. The financial statements also reflect the reporting of certain non-entity (custodial) functions performed by the Department on behalf of the Federal Government.

Intragovernmental assets and liabilities result from activity with other federal entities. All other assets and liabilities result from activity with parties outside the Federal Government, such as domestic and foreign persons, organizations, or governments. Intragovernmental earned revenues are collections or revenue accruals from other federal entities, and intragovernmental costs are payments or expense accruals to other federal entities. Transactions and balances among the Department's Components have been eliminated in the consolidated presentation of the Balance Sheets, Statements of Net Cost, Statements of Changes in Net Position, and the Statements of Custodial Activity. The Statements of Budgetary Resources are reported on a combined basis; therefore, intradepartmental balances have not been eliminated.

While these financial statements have been prepared from the books and records of the Department in accordance with the formats prescribed by OMB, these financial statements are in addition to the financial reports used to monitor and control budgetary resources, which are prepared from the same books and records.

These financial statements should be read with the realization that they are for a component of the U.S. Government, a sovereign entity, whose liabilities not covered by budgetary resources cannot be liquidated without the enactment of an appropriation, and that the payment of all liabilities other than for contracts can be abrogated by the U.S. Government acting in its capacity as a sovereign entity.

C. Basis of Accounting

Transactions are recorded on an accrual and a budgetary basis of accounting. Under the accrual basis, revenues are recorded when earned, and expenses are recognized when a liability is incurred, regardless of when cash is exchanged. Budgetary accounting facilitates compliance with legal constraints and the controls over the use of federal funds. The balances and activity of budgetary accounts are used to prepare the Statements of Budgetary Resources. The Statements of Custodial Activity are reported using the modified cash basis. With this method, revenue from cash collections is reported separately from receivable accruals, and cash disbursements are reported separately from payable accruals.

D. Use of Estimates

Preparation of the consolidated financial statements requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities, disclosure of contingent assets and liabilities at the date of consolidated financial statements, and the reported amounts of revenues and claims and expenses during the reporting period. Actual results could differ from those estimates. Significant estimates include: the year-end accruals of accounts and grants payable; contingent legal and environmental liabilities; accrued workers' compensation; allowance for doubtful accounts receivable; allowances for obsolete inventory and operating materials and



supplies (OM&S) balances; allocations of indirect common costs to construction-in-progress; capitalized property, plant, and equipment; depreciation; subsidy re-estimates; deferred revenues; National Flood Insurance Program (NFIP) insurance liability; actuarial assumptions related to workers' compensation; military and other pension, retirement and post-retirement benefit assumptions; allowances for doubtful duties, fines, penalties, and certain non-entity receivables; and payables related to custodial activities and undeposited collections.

E. Entity and Non-Entity Assets

Entity assets are assets the Department has the authority to use in its operations. The authority to use funds in an entity's operations means either Department management has the authority to decide how funds are used or management is legally obligated to use funds to meet entity obligations (e.g., salaries and benefits).

Non-entity assets are assets held by the Department but not available for use by the Department. An example of a non-entity asset is the portion of Fund Balance with Treasury that consists of special and deposit funds, permanent appropriations, and miscellaneous receipts that are available to pay non-entity liabilities.

For additional information, see Note 2, Non-Entity Assets.

F. Fund Balance with Treasury

Fund Balance with Treasury represents the aggregate amount of the Department's accounts with the U.S. Department of the Treasury (Treasury) available to pay current liabilities and finance authorized purchases, except as restricted by law. The Department's Fund Balance with Treasury balances are primarily appropriated, revolving, trust, deposit, receipt, and special fund amounts remaining as of the end of the fiscal year. Fund Balance with Treasury does not include fiduciary amounts (see Note 1.Y., Fiduciary Activities).

For additional information, see Note 3, Fund Balance with Treasury.

G. Cash and Other Monetary Assets

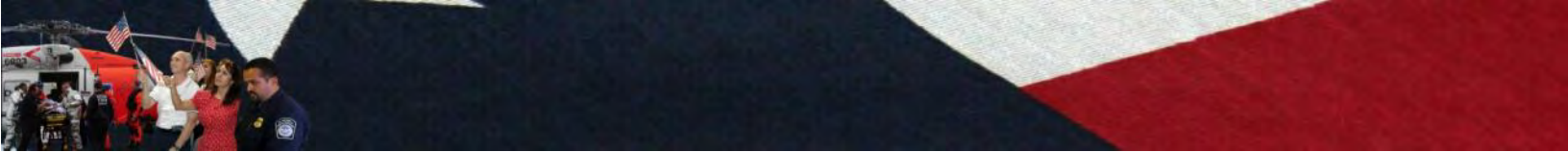
The Department's cash and other monetary assets primarily consist of undeposited collections, imprest funds, cash used in undercover operations, cash held as evidence, cash held by insurance companies, and seized cash and monetary instruments.

The Department does maintain cash in commercial bank accounts. Insurance companies receive and process certain receipts and disbursements on behalf of FEMA. Treasury processes the remainder of the receipts and disbursements.

For additional information, see Note 4, Cash and Other Monetary Assets.

H. Investments, Net

Investments consist of U.S. Government nonmarketable par value and market-based Treasury securities and are reported at cost or amortized cost net of premiums or discounts. Premiums or discounts are amortized into interest income over the terms of the investment using the effective



interest method or the straight-line method, which approximates the interest method. No provision is made for unrealized gains or losses on these securities because it is the Department's intent to hold these investments to maturity.

For additional information, see Note 5, Investments, Net.

I. Accounts Receivable, Net

Accounts receivable represents amounts due to the Department from other federal agencies and the public. In general, intragovernmental accounts receivable arise from the provision of goods and services to other federal agencies and are expected to be fully collected.

Accounts receivable due from the public typically result from various immigration and user fees, premiums and policy fees from insurance companies and policyholders, breached bonds, reimbursable services, and security fees. Public accounts receivable are presented net of an allowance for doubtful accounts, which is based on analyses of debtors' ability to pay, specific identification of probable losses, aging analysis of past-due receivables, or historical collection experience.

Taxes, duties, and trade receivables consist of duties, user fees, fines and penalties, refunds and drawback overpayments, and interest associated with import/export activity, which have been established as a specifically identifiable, legally enforceable claim which remain uncollected as of year-end.

For additional information, see Note 6, Accounts Receivable, Net and Note 7, Taxes, Duties, and Trade Receivables.

J. Advances and Prepayments

Intragovernmental advances, presented as a component of other assets in the accompanying Balance Sheets, consist primarily of disaster recovery and assistance advances to other federal agencies.

Advances and prepayments to the public, presented as a component of other assets in the accompanying Balance Sheets, consist primarily of disaster recovery and assistance grants to states, allowances and commission expenses to insurance companies, and other grant activity. The allowances and commission expenses are amortized over the life of the policy. Disaster recovery and assistance grant advances are expensed as they are used by the recipients.

For additional information, see Note 13, Other Assets.

K. Direct Loans, Net

Direct loans are loans issued by the Department to local governments. FEMA, the only DHS Component with loan activity, operates the Community Disaster Loan Program to support local governments that have suffered a substantial loss of tax and other revenue as a result of a major disaster and demonstrate a need for federal financial assistance in order to perform their municipal operating functions. Under the program, FEMA transacts direct loans to local governments that



meet statutorily set eligibility criteria. Loans are accounted for as receivables as funds are disbursed.

All of the Department's loans are post-1991 obligated direct loans, and the resulting receivables are governed by the *Federal Credit Reform Act of 1990* (FCRA) (Pub. L. 101-508). Under FCRA, for direct loans disbursed during a fiscal year, the corresponding receivable is adjusted for subsidy costs. Subsidy costs are estimated long-term costs to the U.S. Government for its loan programs. The subsidy cost is equal to the present value of the estimated cash outflows over the life of the loans minus the present value of the estimated cash inflows, discounted at the applicable Treasury interest rate. Administrative costs such as salaries and contractual fees are not included. Subsidy costs can arise from interest rate differentials, interest subsidies, delinquencies and defaults, and other cash flows. The Department calculates the subsidy costs based on a subsidy calculator model created by OMB.

Loans receivable are recorded at the present value of the estimated net cash flows. The difference between the outstanding principal of the loans and the present value of their net cash inflows is recorded in the allowance for subsidy, which is estimated and adjusted annually, as of year-end. Interest receivable is the total interest that has accrued on each of the outstanding loans, less any cancellations that may have been recorded due to the FEMA cancellation policy as described in 44 Code of Federal Regulations (CFR) Section 206.366.

For additional information, see Note 8, Direct Loans, Net.

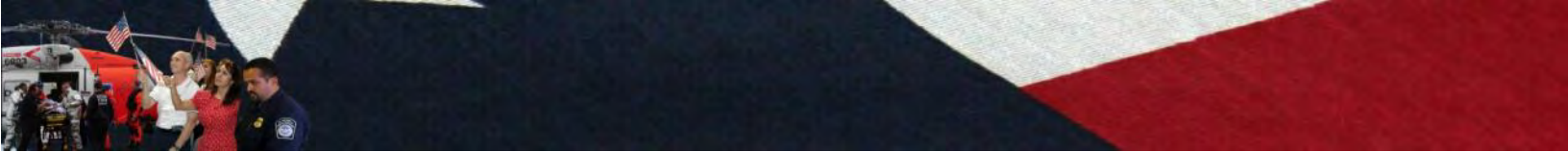
L. Inventory and Related Property, Net

Department operating materials and supplies (OM&S) consist primarily of goods consumed during the service of vessels and aircraft. OM&S at the U.S. Coast Guard aircraft warehouses in Elizabeth City, North Carolina, and vessel warehouses in Baltimore, Maryland is valued using a moving average pricing method and expensed upon issuance. OM&S held at the U.S. Coast Guard field units is accounted for using the purchase method and expensed upon issuance. Excess, obsolete, and unserviceable OM&S are stated at net realizable value.

OM&S held at CBP sites consists of aircraft, marine, and Office of Technology Innovation and Acquisition (OTIA) operating materials and supplies to be used in CBP's operations. CBP's OM&S, which includes repairable spares, are accounted for using the consumption method. As CBP uses repairable spares, they are relieved from inventory and depreciated as part of the major property, plant, and equipment (PP&E) assets repaired.

OM&S held at TSA consists of consumable products and supplies used in providing transportation security screening services at airports and other locations. TSA follows the purchase method of accounting, and OM&S items are expensed at the time of purchase.

The U.S. Coast Guard repairable spares are classified as PP&E. Repairable spares consist of repairable components that are repeatedly repaired and put back into service. Repairable spares are valued based on a moving average cost flow assumption. The cost is depreciated along with the major PP&E asset (e.g., aircraft, vessel, boat) they support. Normal repair costs are expensed in the period incurred.



Inventory is tangible personal property held for sale or used in the process of production for sale. Inventories on hand at year-end are stated at cost using standard price/specific identification, first-in/first-out, or moving average cost methods, which approximates historical cost. Revenue on inventory sales and associated cost of goods sold are recorded when merchandise is sold to the end user. Department inventories consist primarily of the U.S. Coast Guard Supply Fund—which provides uniform clothing, subsistence provisions, retail stores, technical material, and fuel—and the U.S. Coast Guard Industrial Fund, which provides inventory for the repair of U.S. Coast Guard and other Government agency ships and vessels.

Stockpile materials are critical materials held due to statutory requirements for use in national emergencies. The Department's stockpile materials held by FEMA include goods that would be used to respond to national disasters (e.g., water, meals, cots, blankets, tarps, and blue roof sheeting). Inventory at year-end is stated at historical cost using the weighted average method.

For additional information, see Note 9, Inventory and Related Property, Net.

M. Seized and Forfeited Property

Seized property falls into two categories: prohibited and nonprohibited. Prohibited seized property includes illegal drugs, contraband, and counterfeit items that cannot legally enter into the commerce of the United States. Prohibited seized property results primarily from criminal investigations and passenger/cargo processing. Nonprohibited seized property includes items that are not inherently illegal to possess or own, such as monetary instruments, real property, and tangible personal property of others.

Seized property is not considered an asset of the Department and is not reported as such in the Department's financial statements. However, the Department has a stewardship responsibility until the disposition of the seized items is determined (i.e., judicially or administratively forfeited or returned to the entity from which it was seized).

Forfeited property is seized property for which the title has passed to the U.S. Government. Prohibited forfeited items such as counterfeit goods, narcotics, or firearms are held by the Department until disposed of or destroyed. Nonprohibited seized and forfeited property is transferred to, held, and maintained by the Treasury Forfeiture Fund.

An analysis of changes in seized and forfeited property of prohibited items is presented in Note 10, Seized and Forfeited Property.

N. General Property, Plant, and Equipment, Net

The Department's PP&E consists of aircraft, vessels, vehicles, land, structures, facilities, leasehold improvements, software, information technology, and other equipment. PP&E is recorded at cost. The Department capitalizes PP&E acquisitions when the cost equals or exceeds an established threshold and has a useful life of two years or more.

Costs for construction projects are recorded as construction-in-progress until the asset is placed in service. Costs are valued at actual (direct) costs plus applied overhead and other indirect costs. In cases where historical cost information was not maintained, PP&E is capitalized using an estimated



cost methodology consistent with Statement of Federal Financial Accounting Standards (SFFAS) No. 35, *Estimating the Historical Cost of General Property, Plant, and Equipment*. Estimated cost may be based on the cost of similar assets at the time of acquisition or the current cost of similar assets discounted for inflation since the time of acquisition. The U.S. Coast Guard uses market analysis as a reasonable alternative valuation method to record PP&E assets when the historical cost is unknown. For unique or uncommon assets, formal appraisals are conducted to determine acquisition cost. The Department owns some of the buildings in which Components operate. Other buildings are provided by the General Services Administration (GSA), which charges rent equivalent to the commercial rental rates for similar properties.

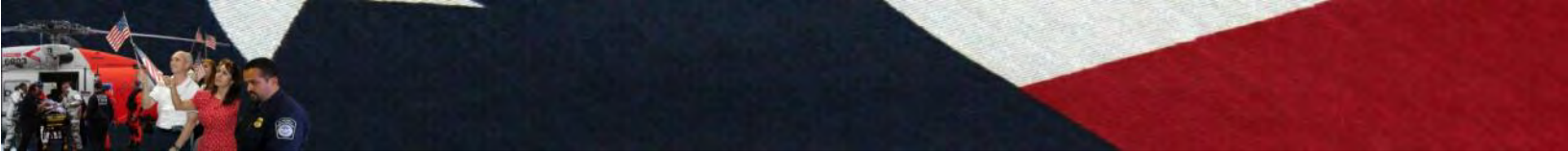
Internal-use software includes purchased commercial off-the-shelf (COTS) software, contractor-developed software, and internally developed software. For COTS software, the capitalized costs include the amount paid to the vendor for the software. For contractor-developed software, the capitalized costs include the amount paid to a contractor to design, program, install, and implement the software. For internally developed software, capitalized costs include the full costs (direct and indirect) incurred during the software development phase. Costs incurred during the preliminary design and post-implementation/operational phases are expensed in the period incurred. In addition, CBP applies capital lease accounting concepts to software license fee agreements that give CBP the “right to use” internal-use software.

The schedule of capitalization thresholds shown below is a summary of the range of capitalization rules used by the Components. DHS policy allows Components to continue using legacy thresholds and capitalization rules for assets acquired prior to October 1, 2007. For assets acquired on or after October 1, 2007, Components use the DHS capitalization policy unless: 1) adopting it would cause a material misstatement of the standalone financial statements or 2) it would cause the Component to not be in compliance with GAAP. Bulk purchases are subject to a \$1 million capitalization threshold, unless one of the above Component criteria is met.

The ranges of capitalization thresholds and service life used by Components, by primary asset category, are as follows:

Asset Description	Capitalization Threshold	Service Life
Land	Zero to \$200,000	Not Applicable
Improvements to land	Zero to \$200,000	2 years to 40 years
Buildings	\$50,000 to \$200,000	2 years to 40 years
Equipment	Zero to \$200,000	2 years to 74 years
Capital leases and leasehold improvements	\$50,000 to \$200,000	2 years to 40 years
Software	\$50,000 to \$750,000	3 years to 10 years

The Department begins to recognize depreciation expense once the asset has been placed in service. Depreciation is calculated on a straight-line method for all asset classes over their estimated useful lives. Land is not depreciated. Leasehold improvements are depreciated over the shorter of the term of the remaining portion of the lease or the useful life of the improvement. Buildings and equipment acquired under capital leases are amortized over the lease term. Amortization of capitalized software is calculated using the straight-line method and begins on the date of acquisition if purchased, or when the module or component has been placed in use (i.e., successfully



installed and tested) if contractor or internally developed. There are no restrictions on the use or convertibility of general PP&E.

For additional information, see Note 11, General Property, Plant, and Equipment, Net.

O. Stewardship Property, Plant, and Equipment

Stewardship PP&E includes heritage assets that generally are not included in general PP&E presented on the Balance Sheet. Heritage assets are unique due to their historical or natural significance; cultural, educational, or artistic importance; or significant architectural characteristics. In general, heritage assets are expected to be preserved indefinitely. The Department's heritage assets consist primarily of historical artifacts, artwork, buildings, and structures owned by the U.S. Coast Guard. The cost of improving, reconstructing, or renovating heritage assets is recognized as an expense in the period incurred. Similarly, the cost to acquire or construct a heritage asset is recognized as an expense in the period incurred. Due to their nature, heritage assets are not depreciated because matching costs with specific periods would not be meaningful.

Heritage assets can serve two purposes: a heritage function and a general government operational function. If a heritage asset serves both purposes, but is predominantly used for general government operations, the heritage asset is considered a multi-use heritage asset, which is included in general PP&E on the Balance Sheet. DHS depreciates its multi-use heritage assets over their useful life. The Department's multi-use heritage assets consist of buildings and structures, memorials, and recreation areas owned by CBP, U.S. Coast Guard, and FEMA.

For additional information, see Note 12, Stewardship Property, Plant, and Equipment.

P. Liabilities

Liabilities represent the probable and measurable future outflow or other use of resources as a result of past transactions or events. Liabilities covered by budgetary resources are those liabilities for which Congress has appropriated funds or for which funding is otherwise available to pay amounts due. Liabilities not covered by budgetary or other resources represent amounts owed in excess of available congressionally appropriated funds or other amounts, where there is no certainty that the appropriations will be enacted. The U.S. Government, acting in its sovereign capacity, can annul liabilities of the Department arising from any transaction or event other than contracts.

Q. Contingent Liabilities

The Department accrues contingent liabilities where a loss is determined to be probable and the amount can be reasonably estimated. The Department discloses contingent liabilities where the conditions for liability recognition have not been met and the likelihood of unfavorable outcome is more than remote. Disclosures are made for probable loss contingencies that cannot be reasonably estimated, as well as reasonably possible loss contingencies. Contingent liabilities considered remote are generally not disclosed unless they involve guarantees, in which case the nature of the guarantee is disclosed.

For additional information, see Note 21, Commitments and Contingent Liabilities.



Environmental Cleanup Costs. Environmental liabilities consist of environmental remediation, cleanup, and decommissioning. The liability for environmental remediation is an estimate of costs necessary to bring a known contaminated asset into compliance with applicable environmental standards. Accruals for environmental cleanup costs are the costs of removing, containing, and/or disposing of hazardous wastes or materials that, because of quantity, concentration, or physical or chemical characteristics, may pose a substantial present or potential hazard to human health or the environment.

For all PP&E in service as of October 1, 1997, DHS recognizes the estimated total cleanup costs associated with the PP&E when the cleanup costs are probable and reasonably estimable. The estimate may be subsequently adjusted for material changes due to inflation/deflation or changes in regulations, clean up plans, or technology. The applicable costs of decommissioning DHS's existing and future vessels are considered cleanup costs.

For additional information, see Note 17, Environmental and Disposal Liabilities.

R. Liabilities for Grants and Cooperative Agreements

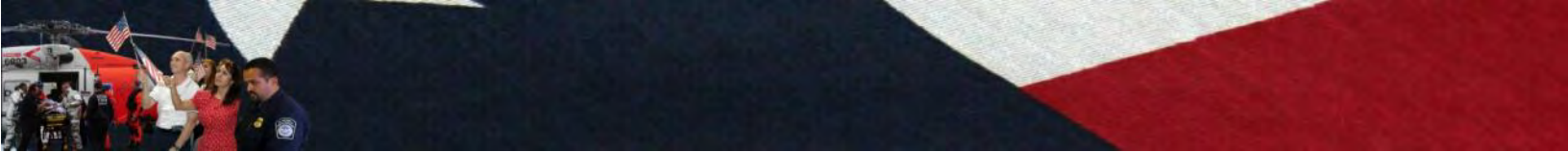
The Department awards grants and cooperative agreements to state and local governments, universities, nonprofit organizations, and private-sector companies to build their capacity to respond to disasters and emergencies; conduct research into preparedness; enhance and ensure the security of passenger and cargo transportation by air, land, or sea; and support other Department-related activities. The Department estimates the year-end grant and cooperative agreement accrual for unreported recipient expenditures using historical disbursement data in compliance with Technical Release 12. Grants and cooperative agreement liabilities are combined with accounts payable to the public in the accompanying Balance Sheets.

S. Insurance Liabilities

Insurance liabilities are the result of the Department's sale or continuation-in-force of flood insurance policies within the NFIP, which is managed by FEMA. The NFIP insurance liability is an unfunded commitment and represents an estimate based on the loss and loss adjustment expense factors inherent to the NFIP Insurance Underwriting Operations. Actual incurred losses and loss adjustment expenses may not conform to the assumptions inherent in the estimation of the liability. Accordingly, the ultimate settlement of losses and the related loss adjustment expenses may vary from the estimate reported in the financial statements.

NFIP premium rates are generally established for actuarially rated policies with the intent of generating sufficient premiums to cover losses and loss adjustment expenses of a historical average loss year and to provide a surplus to compensate Insurance Underwriting Operations for the loss potential of an unusually severe loss year due to catastrophic flooding.

Notwithstanding the foregoing, subsidized rates have historically been charged on a countrywide basis for certain classifications of the insured. These subsidized rates produce a premium less than the loss and loss adjustment expenses expected to be incurred in a historical average loss year. The subsidized rates do not include a provision for losses from catastrophic flooding. Subsidized rates are used to provide affordable insurance on construction or substantial improvements started on or before December 31, 1974, or before the effective date of the initial Flood Insurance Rate Map



(i.e., an official map of a community on which NFIP has delineated both the special hazard areas and the nonsubsidized premium zones applicable to the community).

For additional information, see Note 14, Liabilities Not Covered by Budgetary Resources, Note 18, Other Liabilities, and Note 20, Insurance Liabilities.

T. Debt and Borrowing Authority

Debt is reported within Intragovernmental Liabilities and results from Treasury loans and related interest payable to fund NFIP and Disaster Assistance Direct Loan Program (DADLP) operations of FEMA. Most of this debt is not covered by current budgetary resources. The premiums collected by FEMA for the NFIP are not sufficient to cover the debt repayments. Legislation will need to be enacted to provide funding to repay the Bureau of the Public Debt or to forgive the debt.

Borrowing authority is in budgetary status for use by FEMA for NFIP purposes, and community disaster loans and transfers have been made to the Fund Balance with Treasury for these purposes.

For more information, see Note 15, Debt and Note 26, Available Borrowing Authority.

U. Accrued Payroll and Benefits

Accrued Payroll. Accrued payroll consists of salaries, wages, and other compensation earned by the employees but not disbursed as of September 30. The liability is estimated for reporting purposes based on historical pay information.

Leave Program. Earned annual and other vested compensatory leave is accrued as it is earned and reported on the Balance Sheet. The liability is reduced as leave is taken. Each year, the balances in the accrued leave accounts are adjusted to reflect the liability at current pay rates and leave balances. Sick leave and other types of nonvested leave are not earned benefits. Accordingly, nonvested leave is expensed when used.

Federal Employees Compensation Act. The *Federal Employees Compensation Act* (FECA) (Pub. L. 103-3) provides income and medical cost protection to covered federal civilian employees injured on the job, to employees who have incurred work-related occupational diseases, and to beneficiaries of employees whose deaths are attributable to job-related injuries or occupational diseases. The FECA program is administered by the U.S. Department of Labor (DOL), which pays valid claims and subsequently seeks reimbursement from the Department for these paid claims.

The FECA liability consists of two elements. The first element, accrued FECA liability, is based on actual claims paid by DOL but not yet reimbursed by the Department. The Department reimburses DOL for the amount of actual claims as funds are appropriated for this purpose. In general, there is a two- to three-year time period between payment by DOL and reimbursement to DOL by the Department. As a result, the Department recognizes an intragovernmental liability for the actual claims paid by DOL and to be reimbursed by the Department. The second element, actuarial FECA liability, is the estimated liability for future benefit payments and is recorded as a component of federal employee and veterans' benefits.



For additional information on the accrued FECA liability, accrued payroll, and accrued leave, see Note 18, Other Liabilities.

V. Federal Employee and Veterans' Benefits

The Department's federal employee and veterans' benefits consist of civilian employees' pension programs, other retirement benefits (ORB), and other post-employment benefits (OPEB), as well as the Military Retirement System (MRS), post-employment military travel benefits, and USSS's Uniformed Division and Special Agent Pension and the actuarial FECA liability. Civilian employees' pension programs, ORB and OPEB are administered by the Office of Personnel Management (OPM) and do not represent a liability for the Department.

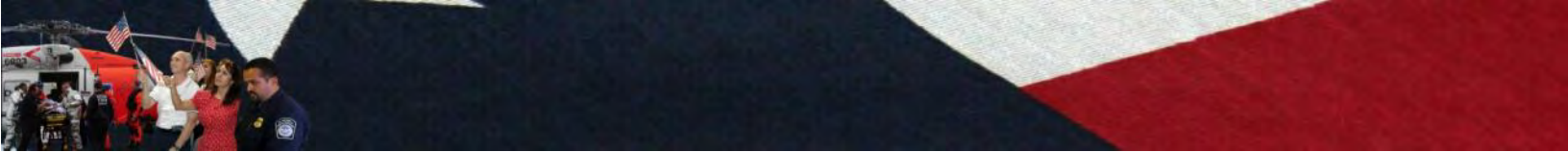
This actuarial FECA liability includes the expected liability for death, disability, medical, and miscellaneous costs for approved compensation cases. DOL determines the actuarial FECA liability annually, as of September 30, using an actuarial method that considers historical benefit payment patterns, wage inflation factors, medical inflation factors, and other variables. The projected annual benefit payments are discounted to present value using the OMB economic assumptions for 10-year Treasury notes and bonds. The actuarial FECA liability is not covered by budgetary resources and will require future funding. For more information on the actuarial FECA liability, see Note 16, Federal Employee and Veterans' Benefits.

The Department recognizes liabilities and expenses for MRS, post-employment military travel benefits, and Uniformed Division and Special Agent Pension. Gains and losses from changes in long-term assumptions used to measure these liabilities are reported as a separate line item on the Statement of Net Cost, consistent with SFFAS No. 33, *Pensions, Other Retirement Benefits, and Other Postemployment Benefits: Reporting the Gains and Losses from Changes in Assumptions and Selecting Discount Rates and Valuation Dates*.

Civilian Pension and Other Post-Employment Benefits. The Department recognizes the full annual cost of its civilian employees' pension benefits; however, the assets of the plan and liability associated with pension costs are recognized by OPM rather than the Department. Accordingly, DHS does not display gains and losses from changes in long-term assumptions used to measure these liabilities on the Statement of Net Cost.

Most federal employees of DHS hired prior to January 1, 1984, participate in the Civil Service Retirement System (CSRS), to which the Department contributes seven percent of base pay for regular CSRS employees and 7.5 percent of base pay for law enforcement agents. The majority of employees hired after December 31, 1983, are covered by the Federal Employees Retirement System (FERS) and Social Security. For the FERS basic annuity benefit, the Department contributes 11.7 percent of base pay for regular FERS employees and 25.7 percent for law enforcement agents. A primary feature of FERS is that it also offers a defined contribution plan (Federal Thrift Savings Plan) to which the Department automatically contributes one percent of base pay and matches employee contributions up to an additional four percent of base pay. The Department also contributes the employer's Social Security matching share for FERS participants.

Similar to CSRS and FERS, OPM reports the liability for future payments to retired employees who participate in the Federal Employees Health Benefits Program and Federal Employees Group Life Insurance Program. The Department reports both the full annual cost of providing these ORB for



its retired employees and reporting contributions made for active employees. In addition, the Department recognizes the cost for OPEB, including all types of benefits provided to former or inactive (but not retired) employees, their beneficiaries, and covered dependents.

The difference between the full annual cost of CSRS and FERS retirement, ORB, and OPEB and the amount paid by the Department is recorded as an imputed cost and offsetting imputed financing source in the accompanying financial statements.

Military Retirement System Liability. The U.S. Coast Guard MRS is a defined benefit plan that includes pension benefits, disability benefits, and survivor benefits and covers all retired active duty and reserve military members of the U.S. Coast Guard. The plan is a pay-as-you-go system funded through annual appropriations. The actuarial accrued liability is the portion of the present value of the future benefits expected to be paid that is attributed to past service (service by participants rendered prior to the date of determination). The remaining portion of that present value is attributed to future service (service by participants rendered on or after the date of determination) and is the present value of the future employer normal costs. The normal cost (current period expense) and the attribution of the present value of the future benefits between past service and future service are determined using the individual entry age normal actuarial cost method.

Effective October 1, 2009, discount rates used to measure the actuarial liabilities for U.S. Coast Guard and USSS are based on the seven year average historical rate yield curve on marketable Treasury securities at September 30 of each year for the seven year historical period with maturities consistent with the period of expected future payments. The method used to measure the liabilities provides for consistency in the underlying relationship between discount rate, COLA, and other economic assumptions. Beginning in FY 2010, valuation techniques used to measure fair value of the actuarial liabilities were consistently applied compared to prior years.

Military Health System for Retirees and Beneficiaries Liability. There are two categories of the Military Healthcare liability for the U.S. Coast Guard retirees and beneficiaries. The first category of military healthcare liability is for the Medicare-eligible U.S. Coast Guard military retirees and beneficiaries. The U.S. Department of Defense (DOD) is the administrative entity for the Medicare-Eligible Retiree Health Care Fund (MERHCF) and, in accordance with SFFAS No. 5, *Accounting for Liabilities of the Federal Government*, is required to recognize the liability on the MERHCF's financial statements. The U.S. Coast Guard makes annual payments to fund benefits for the current active duty members and their spouses who will receive benefits when they reach Medicare-eligibility. The future cost and liability of the MERHCF is determined using claim factors and claims cost data developed by DOD, adjusted for U.S. Coast Guard retiree and actual claims experience. The DOD Board of Actuaries calculates all MERHCF assumptions, and the Defense Finance and Accounting Service provides accounting and investment services for the fund. The U.S. Coast Guard receives per-member amounts (reserve and active duty member amounts separately) to be contributed to the MERHCF from the DOD Board of Actuaries office and pays its share, depending on its demography.

The second category of military healthcare liability is for the pre-Medicare-eligible retirees and beneficiaries. The U.S. Coast Guard is the administrative entity for its Military Health System, and in accordance with SFFAS No. 5, recognizes the liability on its financial statements. Benefits are funded on a pay-as-you-go basis from the current year U.S. Coast Guard appropriations.



Post-Employment Military Travel Benefit. U.S. Coast Guard uniformed service members and their family or survivors are authorized a one-time permanent-change-of-station (PCS) transfer benefit to the members' home of record upon separation or retirement, including permanent disability and preretirement death in service. The benefit is provided whether or not the member is on active duty at the time of travel and without regard to the comparative costs of the various modes of transportation.

Prior to October 1, 2010, the U.S. Coast Guard recognized an actuarial unfunded liability for this benefit in the same manner as the liability for the MRS. The liability was calculated by subtracting the sum of the present value of future normal costs from the present value of the future entitlements expected to be paid. Beginning October 1, 2010, the U.S. Coast Guard no longer recognizes an actuarial liability, but instead records obligations for separation PCS orders in the fiscal year in which they are issued. A separation PCS order obligation amount is based on a historical usage rate and is carried until the PCS costs are settled or the appropriation is closed.

Uniformed Division and Special Agent Pension Liability. The District of Columbia Police and Fireman's Retirement System (the DC Pension Plan) is a defined benefit plan that covers USSS Uniformed Division and Special Agents. The DC Pension Plan makes benefit payments to retirees and/or their beneficiaries. USSS receives permanent, indefinite appropriations each year to pay the excess of benefit payments over salary deductions. The DC Pension Plan is a pay-as-you-go system funded through annual appropriations. The unfunded accrued liability reported on the accompanying Balance Sheet is actuarially determined by subtracting the present value of future employer/employee contributions, as well as any plan assets, from the present value of future cost of benefits. Current period expense is computed using the aggregate cost method.

For more information on civilian pension and OPEB, MRS liability, post-employment military travel benefits, and Uniformed Division and Special Agent Pension liability, see Note 16, Federal Employee and Veterans' Benefits.

W. Earmarked Funds

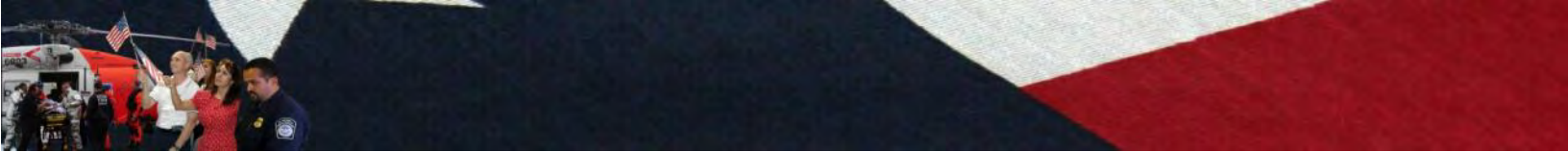
Earmarked funds are financed by specifically identified revenues, often supplemented by other financing sources that remain available over time. These specifically identified revenues and other financing sources are required by statute to be used for designated activities, benefits, or purposes and must be accounted for separately from the Federal Government's general revenues.

Earmarked non-exchange revenue and other financing sources, including appropriations and net cost of operations, are shown separately on the Statements of Changes in Net Position. The portion of cumulative results of operations attributable to earmarked funds is shown separately on both the Statements of Changes in Net Position and the Balance Sheets.

For additional information, see Note 22, Earmarked Funds, and Note 5, Investments, Net.

X. Revenue and Financing Sources

Appropriations. The Department receives the majority of funding to support its programs through Congressional appropriations. The Department receives annual, multi-year, and no-year appropriations that may be used, within statutory limits, for operating and capital expenditures.



Additional funding is obtained through exchange revenues, non-exchange revenues, and transfers-in.

Appropriations are recognized as financing sources when related expenses are incurred or assets are purchased. Revenue from reimbursable agreements is recognized when the goods or services are provided by the Department. Prices for goods and services sold to the public are based on recovery of full cost or are set at a market price. Reimbursable work between federal agencies is subject to the *Economy Act* (31 United States Code (U.S.C.) 1535). Prices for goods and services sold to other Federal Government agencies are generally limited to the recovery of direct cost.

Appropriations Received on the Statement of Changes in Net Position differs from that reported on the Statement of Budgetary Resources because Appropriations Received on the Statement of Changes in Net Position do not include appropriated dedicated and earmarked receipts. Dedicated and earmarked receipts are accounted for as either exchange or non-exchange revenue.

Allocation Transfers. The Department is a party to allocation transfers with other federal agencies as both a transferring (parent) entity and a receiving (child) entity. Allocation transfers are legal delegations by one department of its authority to obligate budget authority and outlay funds to another department. A separate fund account (allocation account) is created in the U.S. Treasury as a subset of the parent fund account for tracking and reporting purposes. All allocation transfers of balances are credited to this account, and subsequent obligations and outlays incurred by the child entity are charged to this allocation account as they execute the delegated activity on behalf of the parent entity. In general, all financial activity related to these allocation transfers (e.g., budget authority, obligations, outlays) is reported in the financial statements of the parent entity, from which the underlying legislative authority, appropriations, and budget apportionments are derived. The Department allocates funds, as the parent, to the Department of Health and Human Services. During FY 2008, OMB granted an exemption from reporting this fund as a parent for FY 2008 and future periods. Therefore, financial activity related to these funds is not reported in the DHS financial statements and related footnotes. DHS receives allocation transfers, as the child, from GSA, the U.S. Department of Transportation, and the Environmental Protection Agency.

Exchange and Non-exchange Revenue. Exchange revenues are recognized when earned and are derived from transactions where both the Government and the other party receive value (i.e., goods have been delivered or services have been rendered). Non-exchange revenues from user fees are recognized as earned in accordance with the *Consolidated Omnibus Budget Reconciliation Act of 1985* (COBRA) (Pub. L. 99-272), as amended. Non-exchange revenues also arise from transfers-in with and without financing sources and donations from the public. Other financing sources, such as donations and transfers of assets without reimbursements, are recognized on the Statements of Changes in Net Position during the period in which the donations and transfers occurred.

Deferred revenue is recorded when the Department receives payment for goods or services which have not been fully rendered. Deferred revenue is reported as a liability on the Balance Sheet until earned. Fees for flood mitigation products and services, such as insurance provided through FEMA's NFIP, are established at rates with the intent of generating sufficient premiums to cover losses and loss adjustment expenses of a historical average loss year and to provide a surplus to compensate Insurance Underwriting Operations for the loss potential of an unusually severe loss year due to catastrophic flooding. NFIP premium revenues are recognized ratably over the life of the policies. Deferred revenue relates to unearned premiums reserved to provide for the remaining



period of insurance coverage. USCIS requires advance payments of the fees for adjudication of applications or petitions for immigration and naturalization benefits.

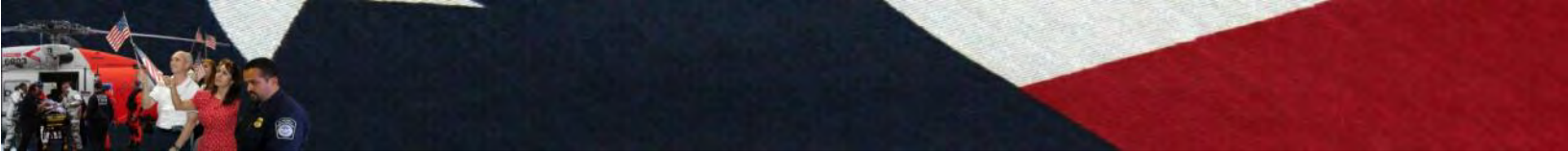
Effective October 1, 2010, the Department implemented a change in reporting the user fees collected by USCIS under the H-1B Nonimmigrant Petitioner Account and H-1B and L Fraud Prevention and Detection Account as exchange revenue reported on the Statement of Net Cost. These user fees were previously reported on the Statement of Custodial Activity. The basis for implementing the reporting change is to more fairly present the Department's results of operations and changes in net position.

Imputed Financing Sources. In certain instances, operating costs of DHS are paid out of funds appropriated to other federal agencies. For example, OPM, by law, pays certain costs of retirement programs, and certain legal judgments against DHS are paid from a judgment fund maintained by the Treasury. When costs that are identifiable to DHS and directly attributable to DHS operations are paid by other agencies, DHS recognizes these amounts as operating expenses. DHS also recognizes an imputed financing source on the Statements of Changes in Net Position to indicate the funding of DHS operations by other federal agencies.

Custodial Activity. Non-entity revenue, disbursements, and refunds are reported on the Statement of Custodial Activity using a modified cash basis. Non-entity revenue reported on the Department's Statement of Custodial Activity include duties, excise taxes, and various non-exchange fees collected by CBP that are subsequently remitted to the Treasury General Fund or to other federal agencies. Duties, user fees, fines, and penalties are assessed pursuant to the provisions of 19 U.S.C.; nonimmigrant petition fees and interest under 8 U.S.C.; and excise taxes are assessed under 26 U.S.C.

CBP assesses duties, taxes, and fees on goods and merchandise brought into the United States from foreign countries. The custodial revenue is recorded at the time of collection. These revenue collections primarily result from current fiscal year activities. CBP records an equal and offsetting liability due to the Treasury General Fund for amounts recognized as non-entity tax and trade receivables. Non-entity tax and trade accounts receivables are recognized when CBP is entitled to collect duties, user fees, fines and penalties, refunds and drawback overpayments, and interest associated with import/export activity on behalf of the Federal Government that have been established as a specifically identifiable, legally enforceable claim and remain uncollected as of year-end. CBP accrues an estimate of duties, taxes, and fees related to commerce released prior to year-end where receipt of payment is anticipated subsequent to year-end. The portions of the fees that are subsequently remitted to other federal agencies are recorded as custodial revenue at the time of collection.

Non-entity receivables are presented net of amounts deemed uncollectible. CBP tracks and enforces payment of estimated duties, taxes, and fees receivable by establishing a liquidated damage case that generally results in fines and penalties receivable. A fine or penalty, including interest on past-due balances, is established when a violation of import/export law is discovered. An allowance for doubtful collections is established for substantially all accrued fines and penalties and related interest. The amount is based on past experience in resolving disputed assessments, the debtor's payment record and willingness to pay, the probable recovery of amounts from secondary sources (such as sureties), and an analysis of aged receivable activity. CBP regulations allow importers to



dispute the assessment of duties, taxes, and fees. Receivables related to disputed assessments are not recorded until the protest period expires or a protest decision is rendered in CBP's favor.

Refunds and drawback of duties, taxes, and fees are recognized when payment is made. A permanent, indefinite appropriation is used to fund the disbursement of refunds and drawbacks. Disbursements are recorded as a decrease in the amount transferred to federal entities as reported on the Statements of Custodial Activity. The liability for refunds and drawbacks consists of amounts owed for refunds of duty and other trade related activity and drawback claims. CBP accrues a monthly liability for refunds and drawback claims approved at month-end, but paid subsequent to month-end.

An accrual adjustment is recorded on the Statements of Custodial Activity to adjust cash collections and refund disbursements with the net increase or decrease of accrued non-entity accounts receivables, net of uncollectible amounts, and refunds payable at year-end.

For additional information, see Note 7, Taxes, Duties, and Trade Receivables, Net, and Note 31, Custodial Revenues.

Y. Fiduciary Activities

Fiduciary activities are Federal Government activities that relate to the collection or receipt—and the subsequent management, protection, accounting, investment and disposition—of cash or other assets in which non-federal individuals or entities have an ownership. Federal accounting standards require the Department to distinguish the information relating to its fiduciary activities from all other activities. Fiduciary activities are not recognized on the accompanying financial statements. The Department's fiduciary activities are currently immaterial, and therefore, no additional disclosure is necessary.

Z. Taxes

The Department, as a federal agency, is not subject to federal, state, or local income taxes. Therefore, no provision for income taxes has been recorded in the accompanying financial statements.

AA. Reclassifications and Other Reporting Changes

The FY 2010 financial statements were reclassified to conform to FY 2011 Departmental presentation. For additional information, see Note 32, Reclassification and Other Reporting Changes.

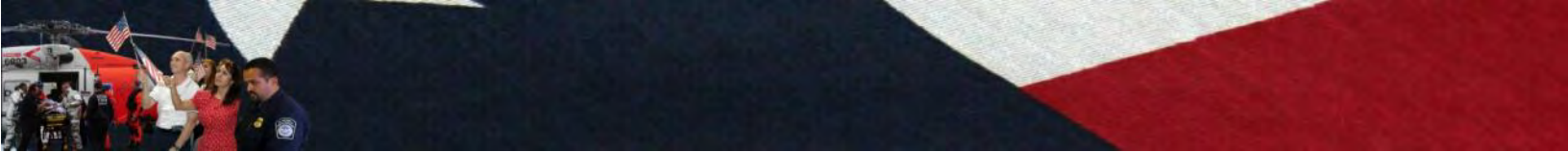


2. *Non-Entity Assets*

Non-entity assets at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Intragovernmental:		
Fund Balance with Treasury	\$1,430	\$1,327
Total Intragovernmental	<u>1,430</u>	<u>1,327</u>
Cash and Other Monetary Assets	32	8
Accounts Receivable, Net	35	23
Taxes, Duties, and Trade Receivables, Net	2,732	2,459
Total Public	<u>2,799</u>	<u>2,490</u>
Total Non-Entity Assets	4,229	3,817
Total Entity Assets	82,660	86,280
Total Assets	<u>\$86,889</u>	<u>\$90,097</u>

Non-entity Fund Balance with Treasury consists of certain special and deposit funds, permanent and indefinite appropriations, and miscellaneous receipts that are available to pay non-entity liabilities. Non-entity assets (also discussed in Notes 3, 4, 6, and 7) are offset by non-entity liabilities at September 30, 2011 and 2010. Taxes, duties and trade receivables from the public represent amounts due from importers for goods and merchandise imported to the United States.



3. Fund Balance with Treasury

A. Fund Balance with Treasury

Fund Balance with Treasury at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Appropriated Funds	\$48,733	\$54,407
Trust Funds	217	573
Revolving, Public Enterprise, and Working Capital Funds	1,284	851
Special Funds	4,817	4,264
Deposit Funds	909	727
Total Fund Balance with Treasury	\$55,960	\$60,822

Appropriated funds consist of amounts appropriated annually by Congress to fund the operations of the Department. Appropriated funds include clearing funds totaling \$20 million and \$151 million (unaudited) at September 30, 2011 and 2010, respectively, which represent reconciling differences with Treasury balances. As of September 30, 2011 and 2010, restricted non-entity fund balance with Treasury was \$1,430 million and \$1,327 million (unaudited), respectively.

Trust funds include both receipt accounts and expenditure accounts that are designated by law as a trust fund. Trust fund receipts are used for specific purposes, in general to offset the cost of expanding border and port enforcement activities and oil spill related claims and activities. For additional information, see Note 22, Earmarked Funds.

Revolving funds are used for continuing cycles of business-like activity, in which the fund charges for the sale of products or services and uses the proceeds to finance its spending, usually without requirement for annual appropriations. A public enterprise revolving fund is an account that is authorized by law to be credited with offsetting collections from the public and those monies are used to finance operations. The Working Capital Fund is a fee-for-service fund established to support operations of Department Components. Also included are the financing funds for credit reform and the National Flood Insurance Fund.

Special funds are funds designated for specific purposes including the disbursement of non-entity monies received in connection with antidumping and countervailing duty orders due to qualifying Injured Domestic Industries (IDI). The Department also has special funds for immigration and naturalization user fees and CBP user fees, as well as inspection fees, flood map modernization subsidy, and off-set and refund transfers. For additional information, see Note 22, Earmarked Funds.

Deposit funds represent amounts received as an advance that are not accompanied by an order and include non-entity collections that do not belong to the Federal Government.



B. Status of Fund Balance with Treasury

The status of Fund Balance with Treasury at September 30 consisted of the following (in millions):

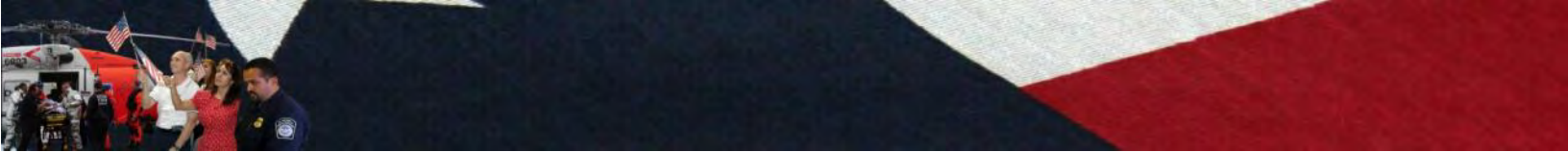
	2011	2010 (Unaudited)
Budgetary Status		
Unobligated Balances:		
Available	\$6,673	\$10,195
Unavailable	5,213	4,993
Obligated Balance Not Yet Disbursed	44,837	46,258
Total Budgetary Status	<u>56,723</u>	<u>61,446</u>
Reconciling Adjustments:		
Receipt, Clearing, and Deposit Funds	932	929
Borrowing Authority	(1,427)	(1,427)
Investments	(4,106)	(3,436)
Receivable Transfers and Imprest Fund	(356)	(317)
Receipts Unavailable for Obligation	2,652	2,117
Authority Temporarily Precluded from Obligation	50	46
SFRBTF; Oil Spill Liability Trust Fund	1,492	1,464
Total Fund Balance with Treasury	<u>\$55,960</u>	<u>\$60,822</u>

Portions of the Unobligated Balances Available, Unavailable, and Obligated Balance Not Yet Disbursed contain CBP's user fees of \$714 million and \$715 million (unaudited) at September 30, 2011 and 2010, respectively, which are restricted by law in its use to offset costs incurred by CBP.

Portions of the Unobligated Balance Unavailable include amounts appropriated in prior fiscal years that are not available to fund new obligations, including expired funds. However, the amounts can be used for upward and downward adjustments for existing obligations in future years. The Obligated Balance Not Yet Disbursed represents amounts designated for payment of goods and services ordered but not received or goods and services received but for which payment has not yet been made.

Since the following line items do not post to budgetary status accounts, certain adjustments are required to reconcile the budgetary status to nonbudgetary Fund Balance with Treasury as reported in the accompanying Balance Sheets:

- Receipt, clearing, and deposit funds represent amounts on deposit with Treasury that have no budget status at September 30, 2011 and 2010.



- Borrowing authority is in budgetary status for use by FEMA for NFIP purposes and community disaster loans, but transfers have not yet been made to the Fund Balance with Treasury account for these purposes.
- Budgetary resources have investments included; however, the money has been moved from the Fund Balance with Treasury asset account to Investments.
- Receivable transfers of currently invested balances increase the budget authority at the time the transfer is realized; however, obligations may be incurred before the actual transfer of funds.
- Imprest funds represent funds moved from Fund Balance with Treasury to Cash and Other Monetary Assets with no change in the budgetary status.
- For receipts unavailable for obligations, authorizing legislation may specify that obligations are not available until a specified time in the future or until specific legal requirements are met.
- Authority temporarily precluded from obligation is offsetting collections that become unavailable for obligation until specific legal requirements are met.
- Sport Fish Restoration Boating Trust Fund (SFRBTF) and Oil Spill Liability Trust Fund are Treasury-managed funds. These funds receive revenues transferred from custodial activities of the Treasury, which are deposited in a Treasury account (see Note 22).

4. Cash and Other Monetary Assets

Cash and Other Monetary Assets at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Cash	\$52	\$60
Seized Monetary Instruments	24	1
Total Cash and Other Monetary Assets	\$76	\$61

DHS cash includes cash held by others, imprest funds, undeposited collections, seized cash deposited, and the net balance maintained by insurance companies for flood insurance premiums received from policyholders. Seized Monetary Instruments are held until disposition. As of September 30, 2011 and 2010, restricted non-entity cash and other monetary assets were \$32 million and \$8 million (unaudited), respectively (see Note 2).



5. Investments, Net

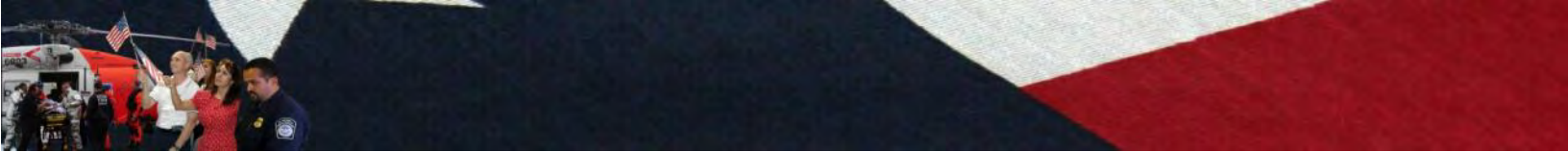
Investments at September 30, 2011, consisted of the following (in millions):

Type of Investment:	Amortization Method	Cost	Amortized (Premium) Discount	Interest Receivable	Investments, Net	Market Value Disclosure
Intragovernmental Securities:						
Oil Spill Liability Trust Fund	Effective interest method	\$2,225	\$30	\$8	\$2,263	N/A
SFRBTF	Effective interest method	1,882	10	3	1,895	N/A
General Gift Fund	Effective interest method	1	-	-	1	N/A
Total Nonmarketable		4,108	40	11	4,159	N/A
Total Investments, Net		\$4,108	\$40	\$11	\$4,159	N/A

Investments at September 30, 2010, consisted of the following (in millions) (unaudited):

Type of Investment:	Amortization Method	Cost	Amortized (Premium) Discount	Interest Receivable	Investments, Net	Market Value Disclosure
Intragovernmental Securities:						
Oil Spill Liability Trust Fund	Effective interest method	\$1,500	\$34	\$8	\$1,542	N/A
SFRBTF	Effective interest method	1,938	1	1	1,940	N/A
Total Nonmarketable		3,438	35	9	3,482	N/A
Total Investments, Net		\$3,438	\$35	\$9	\$3,482	N/A

The Federal Government does not set aside assets to pay future benefits or other expenditures associated with earmarked funds (Oil Spill Liability Trust Fund, SFRBTF, and General Gift Fund) for the U.S. Coast Guard. The cash receipts collected from the public for an earmarked fund are deposited in the Treasury, which uses the cash for general Federal Government purposes. Treasury securities are issued to the U.S. Coast Guard as evidence of its receipts. Treasury securities associated with earmarked funds are an asset to the U.S. Coast Guard and a liability to the Treasury.



Treasury securities provide the U.S. Coast Guard with authority to draw upon the Treasury to make future benefit payments or other expenditures. For additional information, see Note 22, Earmarked Funds.

6. Accounts Receivable, Net

Accounts Receivable, Net, at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Intragovernmental	<u>\$271</u>	<u>\$326</u>
With the Public:		
Accounts Receivable	819	682
Allowance for Doubtful Accounts	<u>(174)</u>	<u>(191)</u>
	<u>645</u>	<u>491</u>
Accounts Receivable, Net	<u>\$916</u>	<u>\$817</u>

Intragovernmental accounts receivable results from reimbursable work performed by the Department. Accounts receivable with the public consist of amounts due for reimbursable services, aviation security fees due to TSA, and other user fees. Intragovernmental and public accounts receivable includes reimbursements for costs associated with oil spills.



7. Taxes, Duties, and Trade Receivables, Net

Taxes, Duties, and Trade Receivables consisted of the following (in millions):

As of September 30, 2011:

Receivables Category	Gross Receivables	Allowance	Total Net Receivables
Duties	\$2,353	\$(148)	\$2,205
Excise Taxes	164	(8)	156
User Fees	148	(2)	146
Fines/Penalties	775	(652)	123
Antidumping and Countervailing Duties	1,001	(899)	102
Total Taxes, Duties, and Trade Receivables, Net	\$4,441	\$(1,709)	\$2,732

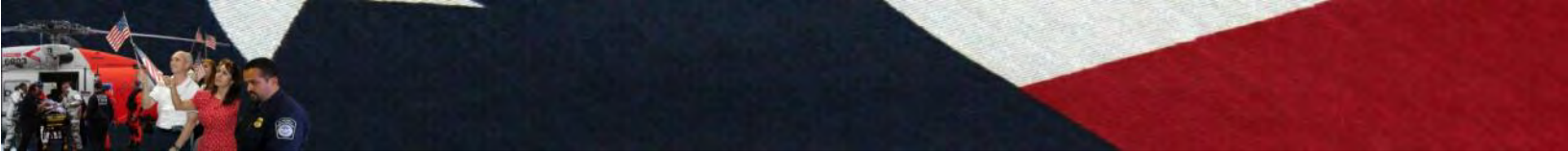
As of September 30, 2010 (Unaudited):

Receivables Category	Gross Receivables	Allowance	Total Net Receivables
Duties	\$2,162	\$(139)	\$2,023
Excise Taxes	121	(6)	115
User Fees	133	4	137
Fines/Penalties	716	(607)	109
Antidumping and Countervailing Duties	641	(566)	75
Total Taxes, Duties, and Trade Receivables, Net	\$3,773	\$(1,314)	\$2,459

When a violation of import/export law is discovered, a fine or penalty is established. CBP assesses a liquidated damage or penalty for these cases to the maximum extent of the law. After receiving the notice of assessment, the importer or surety has 60 days to either file a petition requesting a review of the assessment or pay the assessed amount. Once a petition is received, CBP investigates the circumstances as required by its mitigation guidelines and directives. Until this process has been completed, CBP records an allowance, net of interest, on fines and penalties of approximately 84 percent and 85 percent (unaudited) at September 30, 2011 and 2010, respectively of the total assessment based on historical experience of fines and penalties mitigation and collection. Duties and taxes receivables are non-entity assets for which there is an offsetting liability Due to the General Fund (see Note 18).

8. Direct Loans, Net

DHS's loan program consists of Community Disaster Loans (CDLs) administered by FEMA. CDLs may be authorized to local governments that have suffered a substantial loss of tax and other revenues as a result of a major disaster and have demonstrated a need for federal financial assistance in order to perform their municipal operating functions.



The CDLs are established at the current Treasury rate for a term of five years. A CDL has a maximum amount of \$5 million. The CDL amount cannot exceed 25 percent of the annual operating budget of the local government for the fiscal year in which the major disaster occurred, unless the loss of tax and other revenues for the local government is at least 75 percent of the annual operating budget. In this case, the CDL amount cannot exceed 50 percent of the annual operating budget. These CDLs can be cancelled.

The exception is the Special CDL (SCDL) for Hurricanes Katrina and Rita, where the interest rate on the loan is less than the Treasury rate, and the amount of the loan cannot exceed 50 percent of the annual operating budget of the local government for the fiscal year in which the major disaster occurred. In addition, SCDLs may exceed \$5 million and may be cancelled in accordance with the following *Stafford Act* amendments: the *Community Disaster Loan Act of 2005* (Pub. L. 109-88), the *U.S. Troop Readiness, Veteran's Care, Katrina Recovery, and Iraq Accountability Appropriations Act* (Pub. L. 110-28), the *Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Hurricane Recovery, 2006* (Pub. L. 109-234), and 44 CFR, *Emergency and Management Assistance*. Since the 2006 Cohort disbursed through FY 2011, the balance remains in the program account to cover costs of undisbursed loans. Disbursements are tracked by cohort as determined by the date of obligation rather than disbursement.

A. Summary of Direct Loans to Non-Federal Borrowers at September 30 (in millions):

	2011	2010 (Unaudited)
	Loans Receivable, Net	Loans Receivable, Net
Community Disaster Loans	\$10	\$85

An analysis of loans receivable and the nature and amounts of the subsidy and administrative costs associated with the direct loans is provided in the following sections.

B. Direct Loans Obligated After FY 1991 (in millions):

As of September 30, 2011:	Loans Receivable, Gross	Interest Receivable	Allowance for Subsidy Cost (Present Value)	Value of Assets Related to Direct Loans
Community Disaster Loans	\$423	\$54	\$(467)	\$10

As of September 30, 2010 (Unaudited):	Loans Receivable, Gross	Interest Receivable	Allowance for Subsidy Cost (Present Value)	Value of Assets Related to Direct Loans
Community Disaster Loans	\$1,074	\$113	\$(1,102)	\$85



C. Total Amount of Direct Loans Disbursed, Post-1991 (in millions):

	2011	2010 (Unaudited)
Community Disaster Loans	\$18	\$34

D. Subsidy Expense for Direct Loans by Program and Component (in millions):

Subsidy Expense for New Direct Loans Disbursed as of September 30 (in millions):

Community Disaster Loans	Interest Differential	Defaults and Other	Total
2011	\$4	\$14	\$18
2010 (Unaudited)	\$6	\$27	\$33

Total Direct Loan Subsidy Expense

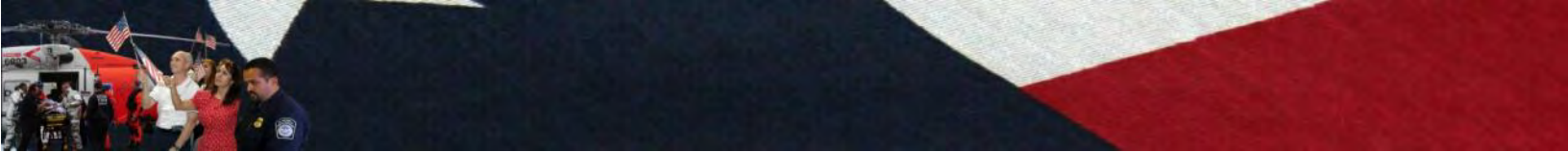
	2011	2010 (Unaudited)
Community Disaster Loans	\$18	\$33

E. Direct Loan Subsidy Rates at September 30 (in millions):

The direct loan subsidy rates, by program, are as follows:

	2011	2010 (Unaudited)
	Community Disaster Loans	Community Disaster Loans
Interest Subsidy Cost	3.47%	2.84%
Default Costs	- %	- %
Other	90.54%	90.98%

The Other line represents the subsidy rates for direct loans that are partially cancelled or cancelled in full if specified conditions are met. Historically, a high percentage of the borrowers have met the conditions for cancellation, thus resulting in a high percentage of direct loan subsidy rate.



F. Schedule for Reconciling Subsidy Cost Allowance Balances at September 30 (in millions):

	2011	2010 (Unaudited)
Beginning balance of the subsidy cost allowance	\$1,102	\$1,069
Add subsidy expense for direct loans disbursed during the reporting years by component:		
Interest rate differential costs	4	6
Other subsidy costs	14	27
Adjustments:		
Loans written off	(654)	-
Subsidy allowance amortization	18	-
Ending balance of the subsidy cost allowance before reestimates	484	1,102
Add subsidy reestimate by component		
Technical/default reestimate	(17)	-
Ending balance of the subsidy cost allowance	\$467	\$1,102

The amount of loans written off during FY 2011 is attributable to Katrina and Rita loans (2006 Cohort) being cancelled at the end of the fifth year.

G. Administrative Expenses at September 30 (in millions):

	2011	2010 (Unaudited)
Community Disaster Loans	\$1	\$0.7



9. Inventory and Related Property, Net

Inventory and Related Property, Net at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Operating Materials and Supplies (OM&S)		
Items Held for Use	\$330	\$315
Items Held for Future Use	33	31
Excess, Obsolete and Unserviceable Items	47	42
Less: Allowance for Losses	(19)	(18)
Total OM&S, Net	<u>391</u>	<u>370</u>
Inventory		
Inventory Purchased for Resale	64	71
Less: Allowance for Losses	(1)	(3)
Total Inventory, Net	<u>63</u>	<u>68</u>
Stockpile Materials Held in Reserve	<u>73</u>	<u>61</u>
Total Inventory and Related Property, Net	<u>\$527</u>	<u>\$499</u>

10. Seized and Forfeited Property

Prohibited seized property item counts as of September 30 and seizure and forfeiture activity for FY 2011 and 2010 are as follows:

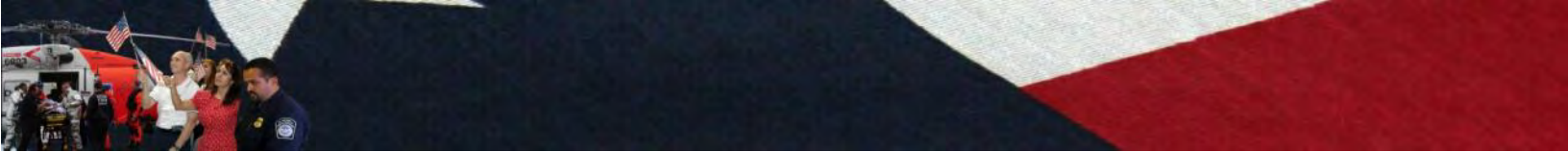
Seizure Activity						
Fiscal Year Ended September 30, 2011						
Seized Property Category:	Beginning Balance	New Seizures	Remissions	New Forfeitures	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	1,857	1,385,602	-	(1,387,482)	2,109	2,086
Cocaine	169	26,999	-	(27,020)	(74)	74
Heroin	8	1,892	-	(1,897)	-	3
Ecstasy	9	451	-	(451)	(8)	1
Steroids	578	312	-	(722)	(3)	165
Firearms and Explosives (in number of items)	1,482	4,446	(1,340)	(1,502)	(97)	2,989
Counterfeit Currency (US/Foreign, in number of items)	4,574,155	1,650,034	-	-	(1,174,081)	5,050,108
Forfeiture Activity						
Fiscal Year Ended September 30, 2011						
Forfeited Property Category:	Beginning Balance	New Forfeitures	Transfers	Destroyed	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	116,025	1,387,482	(711)	(537,859)	(844,470)	120,467
Cocaine	24,601	27,020	(881)	(22,579)	(4,230)	23,931
Heroin	6,085	1,897	(135)	(2,223)	(3,256)	2,368
Ecstasy	1,107	451	-	(481)	(19)	1,058
Steroids	17	722	-	(446)	-	293
Firearms and Explosives (in number of items)	647	1,502	(1,563)	(7)	432	1,011



Seizure Activity						
Fiscal Year Ended September 30, 2010 (Unaudited)						
Seized Property Category:	Beginning Balance	New Seizures	Remissions	New Forfeitures	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	1,163	1,203,104	-	(1,203,504)	1,094	1,857
Cocaine	174	23,955	-	(23,968)	8	169
Heroin	5	4,674	-	(4,673)	2	8
Ecstasy	34	787	-	(786)	(26)	9
Steroids	97	1,331	(812)	(280)	242	578
Firearms and Explosives (in number of items)	1,379	2,259	(1,267)	(763)	(126)	1,482
Counterfeit Currency (US/Foreign, in number of items)	4,198,926	1,631,500	-	-	(1,256,271)	4,574,155

Forfeiture Activity						
Fiscal Year Ended September 30, 2010 (Unaudited)						
Forfeited Property Category:	Beginning Balance	New Forfeitures	Transfers	Destroyed	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	126,052	1,203,504	(543)	(471,500)	(741,488)	116,025
Cocaine	19,037	23,968	(123)	(66,259)	47,978	24,601
Heroin	2,270	4,673	(36)	(1,118)	296	6,085
Ecstasy	1,417	786	(46)	(1,140)	90	1,107
Steroids	39	280	-	(300)	(2)	17
Firearms and Explosives (in number of items)	412	763	(576)	(1)	49	647

This schedule is presented only for material prohibited (nonvalued) seized and forfeited property. These items are retained and ultimately destroyed by CBP and USSS and are not transferred to the U.S. Departments of Treasury or Justice Asset Forfeiture Funds or other federal agencies. The ending balance for firearms includes only those seized items that can actually be used as firearms. Illegal drugs are presented in kilograms, and a portion of the weight includes packaging, which often cannot be reasonably separated from the weight of the drugs since the packaging must be



maintained for evidentiary purposes. The adjustments are caused by changes during the year to the beginning balances of cases. The total adjustments for counterfeit currency include items that were destroyed during the fiscal year. Also, a prior year case can change legal status or property type. For example, a case considered forfeited could be re-opened and changed to seized status or a drug property type may change on a case.

The U.S. Coast Guard and ICE also seize and take temporary possession of small boats, equipment, firearms, contraband, and illegal drugs. The U.S. Coast Guard and ICE usually dispose of these properties within three days by destroying it or by transfer to CBP (who transfers the proceeds from the sale of nonprohibited seized property to the Treasury Forfeiture Fund); the Drug Enforcement Administration; other federal, state and local law enforcement agencies; or foreign governments. Seized property in U.S. Coast Guard and ICE possession at year-end is not considered material and therefore is not itemized and is not reported in the financial statements of the Department.

11. General Property, Plant, and Equipment, Net

General Property, Plant, and Equipment (PP&E) consisted of the following (in millions):

As of September 30, 2011:	Service Life	Gross Cost	Accumulated Depreciation/Amortization	Total Net Book Value
Land and Land Rights	N/A	\$208	N/A	\$208
Improvements to Land	2-40 yrs	1,998	276	1,722
Construction in Progress	N/A	3,270	N/A	3,270
Buildings, Other Structures and Facilities	2-40 yrs	5,907	2,699	3,208
Equipment:				
Automated Data Processing Equipment	5 yrs	548	373	175
Aircraft	12-40 yrs	5,862	2,964	2,898
Vessels	5-74 yrs	6,572	3,106	3,466
Vehicles	4-8 yrs	880	620	260
Other Equipment	2-30 yrs	6,985	4,038	2,947
Assets Under Capital Lease	5-40 yrs	80	40	40
Leasehold Improvements	2-30 yrs	989	432	557
Internal Use Software	3-10 yrs	2,485	1,781	704
Internal Use Software - in Development	N/A	582	N/A	582
Total General Property, Plant, and Equipment, Net		\$36,366	\$16,329	\$20,037

The table above represents the general PP&E balances for all DHS Components as of September 30, 2011. The U.S. Coast Guard's general PP&E represents \$18,407 million (unaudited) of the total gross cost, \$8,542 million (unaudited) of the total accumulated depreciation/amortization, and \$9,865 million (unaudited) of the net book value as of September 30, 2011.



As of September 30, 2010 (Unaudited):	Service Life	Gross Cost	Accumulated Depreciation/ Amortization	Total Net Book Value
Land and Land Rights	N/A	\$191	N/A	\$191
Improvements to Land	2-40 yrs	1,800	177	1,623
Construction in Progress	N/A	4,782	N/A	4,782
Buildings, Other Structures and Facilities	6-40 yrs	5,279	2,499	2,780
Equipment:				
Automated Data Processing Equipment	5 yrs	453	322	131
Aircraft	12-40 yrs	5,373	2,697	2,676
Vessels	5-74 yrs	6,052	2,963	3,089
Vehicles	3-8 yrs	862	573	289
Other Equipment	2-30 yrs	5,688	3,627	2,061
Assets Under Capital Lease	2-40 yrs	69	26	43
Leasehold Improvements	2-40 yrs	761	297	464
Internal Use Software	2-7 yrs	2,077	1,606	471
Internal Use Software - in Development	N/A	474	N/A	474
Total General Property, Plant, and Equipment, Net		\$33,861	\$14,787	\$19,074

12. Stewardship Property, Plant, and Equipment

DHS's Stewardship PP&E is comprised of U.S. Coast Guard, CBP, USCIS, TSA, and FEMA heritage assets located in the United States, including the Commonwealth of Puerto Rico. Physical unit information related to heritage assets as of September 30 consisted of the following (in number of units):

2011	Beginning Balance	Additions	Withdrawals	Total
Collection-type Assets				
USCG (unaudited)	19,552	694	(205)	20,041
CBP	2	-	-	2
USCIS	5	-	-	5
TSA	3	4	-	7
Non-collection-type Assets				
USCG (unaudited)	60	-	-	60
Multi-use Heritage Assets				
USCG (unaudited)	764	-	(18)	746
CBP	4	-	-	4
FEMA	1	-	-	1
Total Stewardship Property, Plant and Equipment				
	20,391	698	(223)	20,866
<hr/>				
2010 (Unaudited)	Beginning Balance	Additions	Withdrawals	Total
Collection-type Assets				
USCG	19,768	207	(423)	19,552
CBP	2	-	-	2
USCIS	5	-	-	5
TSA	3	-	-	3
Non-collection-type Assets				
USCG	60	-	-	60
Multi-use Heritage Assets				
USCG	784	-	(20)	764
CBP	4	-	-	4
FEMA	1	-	-	1
Total Stewardship Property, Plant and Equipment				
	20,627	207	(443)	20,391



The Department's Stewardship PP&E primarily consists of U.S. Coast Guard's heritage assets, which are unique due to historical, cultural, artistic, or architectural significance. These assets are used to preserve and to provide education on U.S. Coast Guard history and tradition.

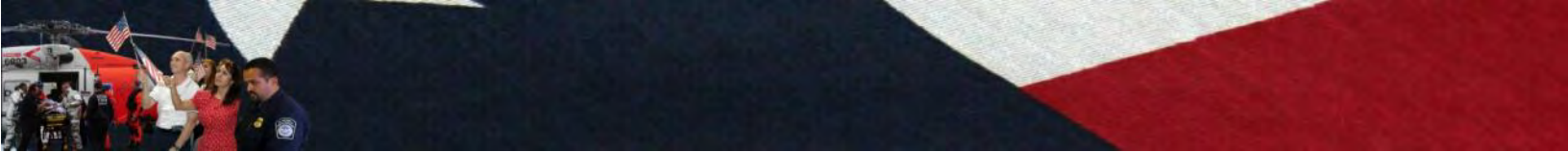
When heritage assets are functioning in operational status, the U.S. Coast Guard classifies these as multi-use heritage assets in accordance with SFFAS No. 6, *Accounting for Property, Plant and Equipment*. All multi-use heritage assets are reflected on the Balance Sheet as general PP&E and are depreciated over their useful life. U.S. Coast Guard's real property heritage assets are used in operations. Some examples are historic lighthouses and buildings still in use. Deferred maintenance and condition information for heritage assets and general PP&E are presented in the required supplementary information. When multi-use heritage assets are no longer needed for operational purposes, they are reclassified as heritage assets, where most are transferred to other Government agencies or public entities.

The U.S. Coast Guard possesses a wide range of heritage assets, such as ship's equipment, lighthouse and other aids-to-navigation/communication items, military uniforms, ordnance, artwork, and display models. Historical artifacts are also gifted to the U.S. Coast Guard. Withdrawals occur when items have deteriorated through damage due to moving and transportation, storage or display, or environmental degradation. Withdrawals are also made when the U.S. Coast Guard curatorial staff, in conjunction with the U.S. Coast Guard historian, determines that an artifact does not meet the needs of the collection. U.S. Coast Guard collectible heritage assets can be categorized as follows:

- Artifacts include ship's equipment (sextants, bells, binnacles, etc.); decommissioned aids-to-navigation and communication equipment (buoy bells, lighthouse lenses, lanterns, etc.); personal-use items (uniforms and related accessories); and ordnance (cannons, rifles, and Lyle guns).
- Artwork consists of the U.S. Coast Guard's collection of World War II combat art as well as modern art depicting both historical and modern U.S. Coast Guard activities.
- Display models are mostly of U.S. Coast Guard vessels and aircraft. These are often builders' models acquired by the U.S. Coast Guard as part of the contracts with the ship or aircraft builders.

U.S. Coast Guard non-collection type heritage assets include sunken vessels and aircraft, as stipulated in the property clause of the U.S. Constitution, Articles 95 and 96 of the *International Law of the Sea Convention*, *Sunken Military Craft Act*, and the sovereign immunity provisions of Admiralty law. Despite the passage of time or the physical condition of these assets, they remain Government-owned until the Congress of the United States formally declares them abandoned. The U.S. Coast Guard desires to retain custody of these assets to safeguard the remains of crew members lost at sea, to prevent the unauthorized handling of explosives or ordnance that may be aboard, and to preserve culturally valuable artifacts of the U.S. Coast Guard.

CBP possesses documents and artifacts that are unique due to historical, cultural, artistic, or architectural significance. CBP aggregates its personal property heritage assets as documents and artifacts and reflects its real property as a number of physical units. These assets are used to preserve and to educate about CBP's history and tradition. Documents consist of dated tariff



classifications, CBP regulations, ledgers of Collectors of Customs, and Customs pamphlets. Artifacts include antique scales, dated pictures of Customs inspectors, aged tools used to sample imported commodities such as wood bales and bulk grain, and dated Customs uniforms, badges, and stamps. In addition, CBP has four multi-use heritage assets located in Puerto Rico, which consist of customs houses that facilitate the collection of revenue for the Department.

USCIS stewardship assets consist of an archive of five different types of immigration and naturalization files that can be used to trace family lineages. USCIS has established a Genealogy Program to allow the public access to the records on a fee-for-service basis. Archived records available through the Genealogy Program include: naturalization certificate files, alien registration forms, visa files, registry files, alien files numbered below eight million, and documents dated prior to May 1951.

TSA possesses architectural or building artifacts that include concrete pieces that belonged to western wall of the Pentagon, subway rails from the Port Authority Trans-Hudson subway station located below the World Trade Center, and the steel facade from the exterior of one of the World Trade Center Towers that were destroyed by the terrorist attacks of September 11, 2001. TSA also possesses an explosives trace detection portal machine in order to preserve it an important example of new aviation security technology that was deployed to airports across the country after the September 11, 2001 terrorist attacks to keep the traveling public safe. As the lead agency protecting the Nation's transportation systems to ensure freedom of movement for people and commerce, TSA uses this property for the purpose of educating individuals about its history, mission, values, and culture.

FEMA has one multi-use heritage asset, the National Fire Academy, which is used by the U.S. Fire Administration for training in Emmitsburg, Maryland. The National Fire Academy develops, delivers, and manages educational and training programs to support the DHS and FEMA goals to help state and local response agencies prevent, mitigate, prepare for, and respond to local, regional, and national emergencies.



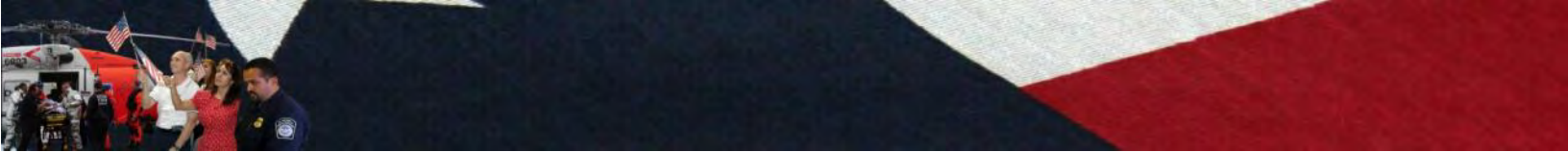
13. Other Assets

Other Assets at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Intragovernmental:		
Advances and Prepayments	\$1,832	\$2,225
Total Intragovernmental	1,832	2,225
Public:		
Advances and Prepayments	640	573
Total Public	640	573
Total Other Assets	\$2,472	\$2,798

Intragovernmental Advances and Prepayments primarily consist of FEMA's Disaster Relief Fund disaster assistance advances to other federal agencies (principally the U.S. Department of Transportation) responsible for restoration efforts of the New York City region transportation system.

The Department provides advance funds to public grant recipients to incur expenses related to the approved grant. Advances are made within the amount of the total grant obligation.



14. Liabilities Not Covered by Budgetary Resources

Liabilities Not Covered by Budgetary Resources at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Intragovernmental:		
Debt (Note 15)	\$17,526	\$18,276
Due to the General Fund (Note 18)	2,844	2,475
Accrued FECA Liability (Note 18)	374	374
Other	14	34
Total Intragovernmental	<u>20,758</u>	<u>21,159</u>
Public:		
Federal Employee and Veterans' Benefits:		
Actuarial FECA Liability (Note 16)	2,055	1,938
Military Service and Other Retirement Benefits (Note 16)	47,609	46,379
Environmental and Disposal Liabilities (Note 17)	1,044	1,018
Other:		
Accrued Payroll and Benefits (Note 18)	1,220	1,168
Insurance Liabilities (Note 20)	3,537	482
Contingent Legal Liabilities (Note 21)	601	540
Capital Lease Liability (Note 19)	48	51
Other	66	91
Total Public	<u>56,180</u>	<u>51,667</u>
Total Liabilities Not Covered by Budgetary Resources	76,938	72,826
Liabilities Covered by Budgetary Resources	11,009	10,770
Total Liabilities	<u>\$87,947</u>	<u>\$83,596</u>

The Department anticipates that the liabilities listed above will be funded from future budgetary resources when required, except for Due to the General Fund, which is funded by future custodial collections and insurance liabilities which are funded by cash on hand, future premiums, and/or borrowing authority.



15. Debt

Debt at September 30 consisted of the following (in millions):

As of September 30, 2011	Beginning Balance	Net Borrowing	Ending Balance
Debt to the Treasury General Fund:			
Debt for the NFIP	\$18,501	\$(751)	\$17,750
Debt for Credit Reform	4	-	4
Total Debt to the Treasury General Fund	\$18,505	\$(751)	\$17,754
Total Debt	\$18,505	\$(751)	\$17,754

As of September 30, 2010 (Unaudited)	Beginning Balance	Net Borrowing	Ending Balance
Debt to the Treasury General Fund:			
Debt for the NFIP	\$19,000	\$(499)	\$18,501
Debt for Credit Reform	4	-	4
Total Debt to the Treasury General Fund	\$19,004	\$(499)	\$18,505
Total Debt	\$19,004	\$(499)	\$18,505

DHS's intragovernmental debt is owed to Treasury's Bureau of Public Debt (BPD) and consists of borrowings to finance claims under NFIP and borrowings to finance FEMA's credit reform programs (Disaster Assistance Direct Loan Program). Total debt decreased due to FEMA repayments of their NFIP loan during FY 2011.

NFIP loans from Treasury are typically for a three-year term. Interest rates are obtained from the BPD and range by cohort year from 0.25 percent to 2.00 percent as of September 30, 2011, and from 0.38 percent to 4.75 percent (unaudited) as of September 30, 2010. Interest is paid semi-annually on March 31 and September 30. The total interest paid was \$61 million and \$115 million (unaudited) as of September 30, 2011 and 2010, respectively. Interest is accrued based on the loan balances reported by BPD. Principal repayments are required only at maturity but are permitted any time during the term of the loan. The loan and interest payments are financed by the flood premiums from policy holders and map collection fees. Given the current rate structure, FEMA will be unable to pay its debt when payment is due. Due to the size of the debt incurred for damages sustained for Hurricanes Katrina and Rita, legislation will need to be enacted to provide funding to repay the Bureau of Public Debt or to forgive the debt.

Under Credit Reform, the unsubsidized portion of direct loans is borrowed from the Treasury. The repayment terms of FEMA's borrowing from Treasury are based on the life of each cohort of direct loans. Proceeds from collections of principal and interest from the borrowers are used to repay the Treasury. In addition, an annual reestimate is performed to determine any change from the original subsidy rate. If an upward reestimate is determined to be necessary, these funds are available through permanent indefinite authority, which is to be approved by OMB. Once these funds are

appropriated, the original borrowings are repaid to Treasury. The weighted average interest rates for FY 2011 and FY 2010 were 3.69 percent and 2.76 percent (unaudited), respectively.

16. Federal Employee and Veterans' Benefits

Accrued liability for military service and other retirement and employment benefits at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
U.S. Coast Guard Military Retirement and Healthcare Benefits	\$43,777	\$42,476
USSS DC Pension Plan Benefits	3,833	3,833
U.S. Coast Guard Post-Employment Military Travel Benefits and Other	(1)	70
Actuarial FECA Liability	2,055	1,938
Total Federal Employee and Veterans' Benefits	\$49,664	\$48,317

A. Reconciliation of Beginning and Ending Liability Balances for Pensions, ORB, and OPEB

The reconciliation of beginning and ending liability balances for pensions, ORB, and OPEB at September 30 consisted of the following (in millions):

	USCG Defined Benefit Plan	USCG Post- Retirement Healthcare	USSS Defined Benefit Plan	Total
As of September 30, 2011				
Beginning Liability Balance:	\$33,761	\$8,715	\$3,833	\$46,309
Expenses:				
Normal Cost	1,240	450	246	1,936
Interest on the Liability Balance	1,583	339	-	1,922
Actuarial Losses/(Gains):				
From Experience	(907)	(495)	-	(1,402)
From Assumption Changes	1,478	(1,078)	-	400
Other	-	19	(1)	18
Total Expense	3,394	(765)	245	2,874
Less Amounts Paid	1,119	209	245	1,573
Ending Liability Balance	\$36,036	\$7,741	\$3,833	\$47,610

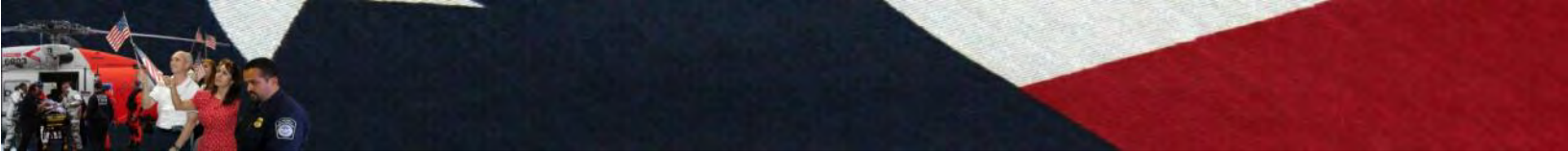


As of September 30, 2010 (Unaudited)	USCG Defined Benefit Plan	USCG Post- Retirement Healthcare	USSS Defined Benefit Plan	Total
Beginning Liability Balance:	\$26,801	\$6,960	\$3,770	\$37,531
Expenses:				
Normal Cost	1,189	528	244	1,961
Interest on the Liability Balance	1,555	392	-	1,947
Actuarial Losses/(Gains):				
From Experience	626	(80)	63	221
From Assumption Changes	4,557	1,118	-	6,063
Other	113	-	(1)	112
Total Expense	8,040	1,958	306	10,304
Less Amounts Paid	1,080	203	243	1,526
Ending Liability Balance	\$33,761	\$8,715	\$3,833	\$46,309

U.S. Coast Guard. The U.S. Coast Guard’s military service members (both current active component and reserve component) participate in the MRS. The U.S. Coast Guard receives an annual “Retired Pay” appropriation to fund MRS benefits. The retirement system allows voluntary retirement with retired pay and benefits for active component members upon credit of at least 20 years of active service at any age. Reserve component members may retire after 20 years of creditable service with retired pay and health benefits beginning at age 60. Reserve component members may qualify for retired pay at an earlier age (but not earlier than age 50) if they perform certain active service after January 28, 2008, but in such cases Military Health System (MHS) benefits for themselves and their dependents do not begin until the member attains age 60.

The U.S. Coast Guard’s MHS is a post-retirement medical benefit plan that covers all active component and reserve component members of the U.S. Coast Guard. The accrued MHS liability is for the health care of non-Medicare eligible retirees and beneficiaries. Effective October 1, 2002, the U.S. Coast Guard transferred its liability for the health care of Medicare eligible retirees/beneficiaries to the DOD MERHCF, which was established to finance the health care benefits for the Medicare-eligible beneficiaries of all DOD and non-DOD uniformed services.

The unfunded accrued liability, presented as a component of the liability for military service and other retirement benefits in the accompanying Balance Sheet, represents both retired pay for retirees and health care benefits for non-Medicare eligible retirees/survivors. The present value of future benefits is the actuarial present value of the future payments that are expected to be paid under the retirement plan’s provisions. Credited service is the years of service from active duty base date (or constructive date in the case of active duty reservists) to date of retirement measured in years and completed months. The present value of future benefits is then converted to an accrued liability by subtracting the present value of future employer/employee normal contributions. U.S. Coast Guard plan participants may retire after 20 years of active service at any age with annual benefits equal to 2.5 percent of retired base pay for each year of creditable active service. The retired pay base depends upon the date of initial entry into military service (DIEMS). For DIEMS of



September 8, 1980, or later, the retired pay base would be the mean of the highest 36 months of basic pay earned (or would have earned if on active duty). For DIEMS of September 7, 1980, or earlier, the retired pay base would be the basic pay rate in effect on the first day of retirement (if a commissioned officer or an enlisted member) or the basic pay rate in effect on the last day of active duty before retirement (if a warrant officer). Personnel who became members after August 1, 1986, may elect to receive a \$30,000 Career Status Bonus after 15 years of service in return for reductions in retired pay.

If a U.S. Coast Guard member is disabled, the member is entitled to disability benefits, assuming (1) the disability is at least 30 percent under a Department of Veterans Affairs (VA) Schedule of Rating Disability and (2) the disability results from injuries or illnesses incurred in the line of duty. Disability retired pay is equal to the basic pay (as of the separation date) multiplied by the larger of the VA disability rating or 2.5 percent times the years of creditable service.

The significant actuarial assumptions used to compute the accrued pension and healthcare liability are as follows:

- DOD decrement tables are only used for mortality. Disability, withdrawal, and retirement tables reflecting actual U. S. Coast Guard experience were developed based on an U.S. Coast Guard experience study dated September 30, 2009;
- Cost of living increases are three percent annually (only for the retirement plan);
- Healthcare cost increase assumptions are based on the annual liability report provided by DOD and vary, depending on the year and type of care;
- The discount rate of 4.52 percent is determined in accordance with SFFAS No. 33 and is calculated independently for pensions and healthcare; however, for this year the rate is the same.

U.S. Secret Service. Special agents and other USSS personnel in certain job series hired as civilians before January 1, 1984, are eligible to transfer to the District of Columbia Police and Fireman's Retirement System (DC Pension Plan) after completion of ten years of Secret Service employment and ten years of protection-related experience. All uniformed USSS officers who were hired before January 1, 1984, are automatically covered under this retirement system. Participants in the DC Pension Plan make contributions of seven percent of base pay with no matching contribution made by USSS. Annuitants of this plan receive benefit payments directly from the DC Pension Plan. USSS reimburses the District of Columbia for the difference between benefits provided to the annuitants and payroll contributions received from current employees. This liability is presented as a component of the liability for military service and other retirement benefits in the accompanying Balance Sheet. SFFAS No. 5 requires the administrative entity (administrator) to report the actuarial liability. However, USSS records a liability because the administrator (the DC Pension Plan) is not a federal entity and as such the liability for future funding would not otherwise be recorded in the Government-wide consolidated financial statements.

The primary actuarial assumptions used to determine the liability at September 30, 2011, are:

- Life expectancy is based upon the RP 2000 Combined Healthy Mortality Table;
- Cost of living increases are 3.5 percent annually;
- Rates of salary increases are 3.5 percent annually;
- Annual rate of investment return is 7.25 percent; and
- Rates of withdrawal for active service by gender and age.



B. Actuarial FECA Liability

The actuarial FECA liability represents the estimated liability for future workers' compensation and includes the expected liability for death, disability, medical, and miscellaneous costs for approved cases. Future workers' compensation estimates for the future cost of approved compensation cases, which are generated from an application of actuarial procedures developed by DOL, were approximately \$2,055 million and \$1,938 million (unaudited) at September 30, 2011 and 2010, respectively.

17. Environmental and Disposal Liabilities

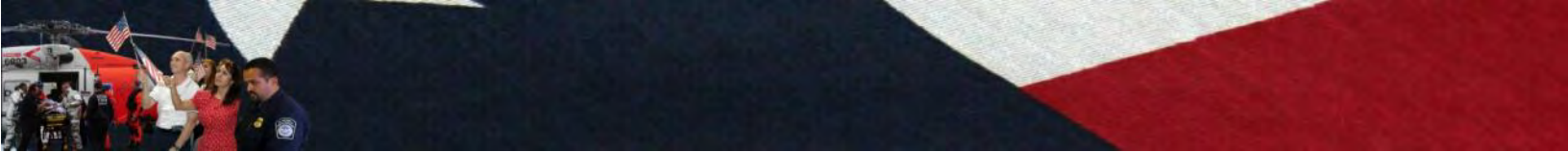
Environmental and disposal liabilities at September 30, 2011 and 2010, are \$1,047 million (unaudited) and \$1,061 million (unaudited), respectively. The Department is responsible for remediating its sites with environmental contamination and is party to various administrative proceedings, legal actions, and tort claims that may result in settlements or decisions adverse to the Federal Government. The source of remediation requirements to determine the environmental liability is based on compliance with federal, state, or local environmental laws and regulations. The major federal laws covering environmental response, cleanup, and monitoring are the *Comprehensive Environmental Response, Compensation and Liability Act* (Pub. L. 96-510) and the *Resource Conservation and Recovery Act* (Pub. L. 94-580).

The U.S. Coast Guard completed a study of its lighthouses in FY 2009, identifying from various historical lists of lighthouses with potential liability. Based on this study, the U.S. Coast Guard created a cost methodology for estimating cleanup cost for various categories of lighthouse environmental liability. As of September 30, 2011, \$797 million was recognized for 1,544 lighthouses confirmed and recorded as a probable environmental and disposal liability.

In accordance with the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009* (Pub. L. 110-329), the Secretary of Homeland Security has directed the administrator of GSA to sell through public sale all real and related personal property and transportation assets that support the Plum Island Animal Disease Center operations. The probable environmental remediation cost of the center is recognized as \$9 million for S&T.

The Department's remaining environmental liabilities are due to light stations, fuel storage tanks, underground storage tanks, buildings containing asbestos and/or lead-based paint, firing ranges, fuels, solvents, industrial chemicals, and other environmental cleanup associated with normal operations of CBP, FLETC, TSA, the U.S. Coast Guard, FEMA, S&T, and USSS.

Cost estimates for environmental and disposal liabilities are subject to revision as a result of changes in inflation, technology, environmental laws and regulations, and plans for disposal.



18. Other Liabilities

Other Liabilities at September 30 consisted of the following (in millions):

As of September 30, 2011	Current	Non-Current	Total
Intragovernmental:			
Due to the General Fund	\$2,844	\$ -	\$2,844
Accrued FECA Liability	160	214	374
Advances from Others	228	-	228
Employer Benefits Contributions and Payroll Taxes	280	-	280
Other Intragovernmental Liabilities	21	3	24
Total Intragovernmental Other Liabilities	\$3,533	\$217	\$3,750
Public:			
Accrued Payroll and Benefits (See B. below)	\$2,136	\$62	\$2,198
Deferred Revenue and Advances from Others (See B. below)	2,005	711	2,716
Insurance Liabilities (Note 20)	3,422	115	3,537
Refunds and Drawbacks	131	-	131
Contingent Legal Liabilities (Note 21)	233	376	609
Capital Lease Liability (Note 19)	6	42	48
Other	1,484	2	1,486
Total Other Liabilities with the Public	\$9,417	\$1,308	\$10,725
Total Other Liabilities	\$12,950	\$1,525	\$14,475
As of September 30, 2010 (Unaudited)	Current	Non-Current	Total
Intragovernmental:			
Due to the General Fund	\$2,475	\$ -	\$2,475
Accrued FECA Liability	165	209	374
Advances from Others	216	-	216
Employer Benefits Contributions and Payroll Taxes	237	-	237
Other Intragovernmental Liabilities	46	2	48
Total Intragovernmental Other Liabilities	\$3,139	\$211	\$3,350



Public:

Accrued Payroll and Benefits (See B. below)	\$2,217	\$ -	\$2,217
Deferred Revenue and Advances from Others (See B. below)	1,941	709	2,650
Insurance Liabilities (Note 20)	401	81	482
Refunds and Drawbacks	129	-	129
Contingent Legal Liabilities (Note 21)	693	34	727
Capital Lease Liability (Note 19)	6	45	51
Other	1,352	10	1,362
Total Other Liabilities with the Public	\$6,739	\$879	\$7,618
Total Other Liabilities	\$9,878	\$1,090	\$10,968

A. Intragovernmental Other Liabilities

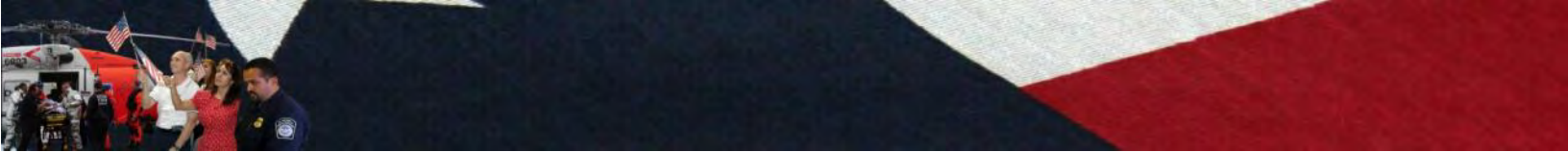
Due to the General Fund. Amounts due to the Treasury General Fund represent duty, tax, and fees collected by CBP to be remitted to various General Fund accounts maintained by Treasury.

Workers' Compensation. Claims incurred for the benefit of Department employees under FECA are administered by DOL and are ultimately paid by the Department. The accrued FECA liability represents money owed for current claims. Reimbursement to DOL for payments made occurs approximately two years subsequent to the actual disbursement. Budgetary resources for this intragovernmental liability are made available to the Department as part of its annual appropriation from Congress in the year in which the reimbursement takes place. Workers' compensation expense was \$165 million and \$165 million (unaudited), respectively, for the fiscal years ended September 30, 2011 and 2010.

B. Other Liabilities with the Public

Accrued Payroll and Benefits. Accrued Payroll and Benefits at September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Accrued Funded Payroll and Benefits	\$905	\$967
Accrued Unfunded Leave	1,211	1,155
Unfunded Employment Related Liabilities	9	13
Other	73	82
Total Accrued Payroll and Benefits	\$2,198	\$2,217



Deferred Revenue and Advances from Others. Deferred Revenue and Advances from Others for the years ended September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
USCIS Application Fees	\$712	\$711
FEMA Unearned NFIP Premium	1,981	1,911
Advances from Others	23	28
Total Deferred Revenue	\$2,716	\$2,650

USCIS requires payments of fees for applications or petitions for immigration and naturalization benefits at the time of filing. FEMA’s deferred revenue relates to unearned NFIP premiums recognized over the term of the period of insurance coverage.

Other Liabilities. Other public liabilities consist primarily of deposit and suspense fund liability.

19. Leases

A. Operating Leases

The Department leases various facilities and equipment under leases accounted for as operating leases. Leased items consist of offices, warehouses, vehicles, and other equipment. The majority of office space occupied by the Department is either owned by the Federal Government or is leased by GSA from commercial sources. The Department is not committed to continue paying rent to GSA beyond the period occupied, providing that proper advance notice to GSA is made and unless the space occupied is designated as unique to Department operations. However, it is expected the Department will continue to occupy and lease office space from GSA in future years, and lease charges will be adjusted annually to reflect operating costs incurred by GSA.

As of September 30, 2011, estimated future minimum lease commitments under operating leases, which are non-cancelable, for equipment and GSA-controlled leases were as follows (in millions):

	Land and Buildings	Vehicles and Equipment	Total
FY 2012	\$462	\$7	\$469
FY 2013	442	7	449
FY 2014	417	7	424
FY 2015	394	7	401
FY 2016	389	7	396
After FY 2016	1,444	8	1,452
Total Future Minimum Lease Payments	\$3,548	\$43	\$3,591



The estimated future lease payments for operating leases are based on lease contract terms considering payments made during the year ended September 30, 2011.

B. Capital Leases

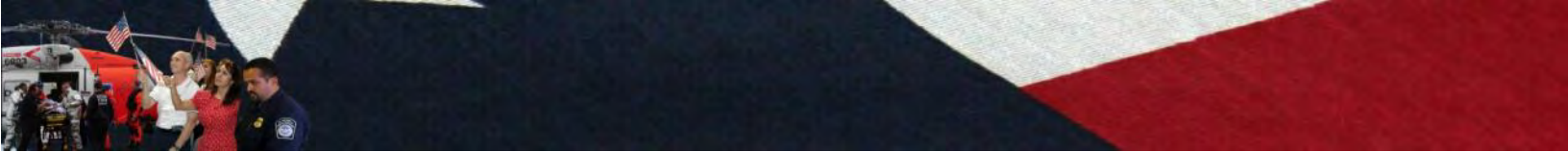
The Department maintains capital leases for buildings and commercial software license agreements. The liabilities associated with capital leases and software license agreements are presented as other liabilities in the accompanying financial statements based upon the present value of the future minimum lease payments.

Certain license agreements are cancelable depending on future funding. Substantially all of the net present value of capital lease obligations and software license agreements will be funded from future sources. As of September 30, the summary of assets under capital lease was as follows (in millions):

	2011	2010 (Unaudited)
Land and Buildings	\$69	\$69
Software	11	116
Accumulated Amortization	(40)	(142)
Assets under Capital Lease, Net	\$40	\$43

As of September 30, 2011, estimated future minimum lease payments under capital leases, which were all non-GSA, were as follows (in millions):

	Land and Buildings
FY 2012	\$6
FY 2013	6
FY 2014	6
FY 2015	6
FY 2016	6
After FY 2016	39
Total Future Minimum Lease Payments	69
Less: Imputed Interest and Executory Costs	(21)
Total Capital Lease Liability	\$48



20. Insurance Liabilities

Insurance liabilities for the periods ended September 30, 2011 and 2010, were \$3,537 million and \$482 million (unaudited), respectively, and consist primarily of NFIP insurance liabilities.

The insurance liability for unpaid losses and related loss adjustment expenses and amounts paid for the year ended September 30 consisted of the following (in millions):

	2011	2010 (Unaudited)
Beginning Balance	\$482	\$508
Change in Incurred Losses	3,943	1,132
Less: Amounts Paid During Current Period	(888)	(1,158)
Total Insurance Liability	\$3,537	\$482

The NFIP insurance liability, the majority of the insurance liability reported, represents an estimate of NFIP based on the loss and loss adjustment expense factors inherent in the NFIP insurance underwriting operations experience and expectations. Estimation factors used by the insurance underwriting operations reflect current case basis estimates and give effect to estimates of trends in claim severity and frequency. These estimates are periodically reviewed, and adjustments, reflected in current operations, are made as deemed necessary. The increase in the actuarial liability for future estimated losses in FY 2011 is an unfunded commitment relating primarily to the flood activity from Hurricanes Irene and Lee. For additional information, see Notes 14 and 15, Liabilities Not Covered by Budgetary Resources and Debt.

21. Commitments and Contingent Liabilities

A. Legal Contingent Liabilities

The Department is a party in various administrative proceedings, legal actions, and tort claims that may ultimately result in settlements or decisions adverse to the Federal Government. These contingent liabilities arise in the normal course of operations, and their ultimate disposition is unknown.

In the opinion of the Department's management and legal counsel, based on information currently available, the expected outcome of legal actions, individually or in the aggregate, will not have a materially adverse effect on the Department's financial statements, except for the legal actions described below (in millions).

	<u>Accrued Liabilities</u>	Estimated Range of Loss	
		<u>Lower End</u>	<u>Upper End</u>
FY 2011			
Probable	\$609	\$609	\$1,154
Reasonably Possible		\$670	\$975



The claims above generally relate to the *Federal Tort Claims Act* (Pub. L. 79-601), Oil Spill Liability Trust Fund, and various customs laws and regulations. The estimated contingent liability recorded in the accompanying financial statements included with other liabilities for all probable and reasonably estimable litigation-related claims at September 30, 2011, was \$609 million, of which \$8 million was funded.

Asserted and pending legal claims for which loss was reasonably possible is estimated to range from \$670 million to \$975 million at September 30, 2011.

As of September 30, 2011, legal claims exist for which the potential range of loss could not be determined; however, the total amount claimed is not material to the financial statements. In addition, other claims exist for which the amount claimed and the potential range of loss could not be determined.

B. Duty and Trade Refunds

There are various trade-related matters that fall under the jurisdiction of other federal agencies, such as the Department of Commerce, which may result in refunds of duties, taxes, and fees collected by CBP. Until a decision is reached by the other federal agencies, CBP does not have sufficient information to estimate a contingent liability amount, if any, for trade-related refunds under jurisdiction of other federal agencies in addition to the amount accrued on the accompanying financial statements. All known duty and trade refunds as of September 30, 2011 and 2010, have been recorded.

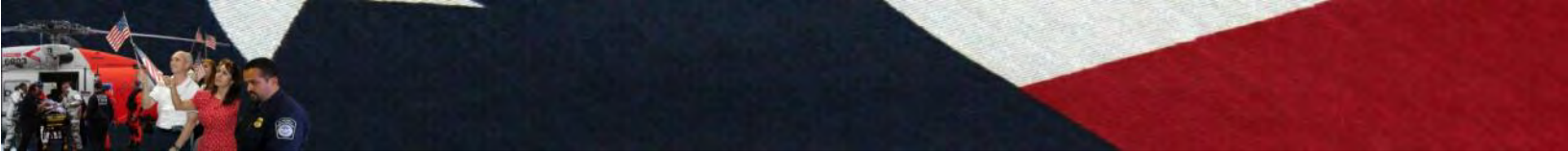
C. Loaned Aircraft and Equipment

The Department is generally liable to DOD for damage or loss to aircraft on loan to CBP and vessels on loan to the U.S. Coast Guard. As of September 30, 2011 and 2010, CBP had 16 aircraft and 17 aircraft, respectively, loaned from DOD with a replacement value of up to \$23 million per aircraft. As of September 30, 2011, the U.S. Coast Guard had seven vessels on loan from DOD with a total replacement value of \$84 million.

D. Other Contractual Arrangements

In addition to future lease commitments disclosed in Note 19, the Department is committed under contractual agreements for goods and services that have been ordered but not yet received (undelivered orders) at fiscal year-end. Aggregate undelivered orders for all Department activities are disclosed in Note 30. In accordance with the *National Defense Authorization Act for Fiscal Year 1991* (Pub. L. 101-510), the Department is required to automatically cancel obligated and unobligated balances of appropriated funds five years after a fund expires. Obligations that have not been paid at the time an appropriation is cancelled may be paid from an unexpired appropriation that is available for the same general purpose. As of September 30, 2011, DHS estimates total payments related to cancelled appropriations to be \$242 million, of which \$111 million for contractual arrangements may require future funding.

TSA entered into a number of Letters of Intent for Modifications to Airport Facilities with 11 major airports in which TSA may reimburse the airports up to 90 percent (estimated total of \$1.5 billion) of the costs to modify the facilities for security purposes. These letters of intent (LOI) would not



obligate TSA until funds have been appropriated and obligated. An LOI, though not a binding commitment of federal funding, represents TSA's intent to provide the agreed-upon funds in future years if the agency receives sufficient appropriations to cover the agreement. TSA received \$200 million in both FY 2011 and FY 2010 (unaudited) to fund LOIs. These funds are available for payment to the airports upon approval by TSA of an invoice for the modification costs incurred. As of September 30, 2011, TSA has received invoices or documentation for costs incurred totaling \$4 million for the invoices that have not yet been paid.

22. Earmarked Funds

Earmarked funds are financed by specifically identified revenues, often supplemented by other financing sources that remain available over time. These specifically identified revenues and other financing sources are required by statute to be used for designated activities or purposes. SFFAS No. 27, *Identifying and Reporting Earmarked Funds*, defines the following three criteria for determining an earmarked fund: 1) a statute committing the Federal Government to use specifically identified revenues and other financing sources only for designated activities, benefits, or purposes; 2) explicit authority for the earmarked fund to retain revenues and other financing sources not used in the current period for future use to finance the designated activities, benefits, or purposes; and 3) a requirement to account for and report on the receipt, use, and retention of the revenues and other financing sources that distinguished the earmarked fund from the Federal Government's general revenues.

There are no transactions between earmarked funds that require elimination in consolidation. Earmarked funds consisted of the following (in millions):

	Customs User Fees	Sport Fish Restoration Boating Trust Fund	Immigration Examination Fees	National Flood Insurance Program	Oil Spill Liability Trust Fund	All Other Earmarked Funds	Total Earmarked Funds
Balance Sheet as of September 30, 2011							
ASSETS							
Fund Balance with							
Treasury	\$717	\$9	\$1,743	\$1,211	\$200	\$1,862	\$5,742
Investments, Net	-	1,895	-	-	2,263	1	4,159
Accounts Receivable	98	132	7	2	309	42	590
Taxes Receivable	86	-	-	-	-	-	86
Other	-	-	187	567	-	8	762
Total Assets	\$901	\$2,036	\$1,937	\$1,780	\$2,772	\$1,913	\$11,339
LIABILITIES							
Other Liabilities	\$105	\$1,263	\$1,089	\$23,348	\$303	\$71	\$26,179
Total Liabilities	\$105	\$1,263	\$1,089	\$23,348	\$303	\$71	\$26,179



	Customs User Fees	Sport Fish Restoration Boating Trust Fund	Immigration Examination Fees	National Flood Insurance Program	Oil Spill Liability Trust Fund	All Other Earmarked Funds	Total Earmarked Funds
NET POSITION							
Cumulative Results of Operations	\$796	\$773	\$848	\$(21,568)	\$2,469	\$1,842	\$(14,840)
Total Liabilities and Net Position	\$901	\$2,036	\$1,937	\$1,780	\$2,772	\$1,913	\$11,339

Statement of Net Cost for the Year Ended September 30, 2011 (unaudited)

Gross Program Costs	\$407	\$126	\$2,433	\$5,312	\$319	\$897	\$9,494
Less: Earned Revenues	-	-	(2,578)	(3,313)	(330)	(808)	(7,029)
Net Cost of Operations	\$407	\$126	\$(145)	\$1,999	\$(11)	\$89	\$2,465

Statement of Changes in Net Position for the Year Ended September 30, 2011 (unaudited)

Net Position Beginning of Period	\$789	\$794	\$640	\$(19,563)	\$2,005	\$1,519	\$(13,816)
Net Cost of Operations	(407)	(126)	145	(1,999)	11	(89)	(2,465)
Non-exchange Revenue	406	638	-	1	547	143	1,735
Other	8	(533)	63	(7)	(94)	269	(294)
Change in Net Position	7	(21)	208	(2,005)	464	323	(1,024)
Net Position, End of Period	\$796	\$773	\$848	\$(21,568)	\$2,469	\$1,842	\$(14,840)

	Customs User Fees	Sport Fish Restoration Boating Trust Fund	Immigration Examination Fees	National Flood Insurance Program	Oil Spill Liability Trust Fund	All Other Earmarked Funds	Total Earmarked Funds
--	----------------------	--	------------------------------------	---	---	---------------------------------	-----------------------------

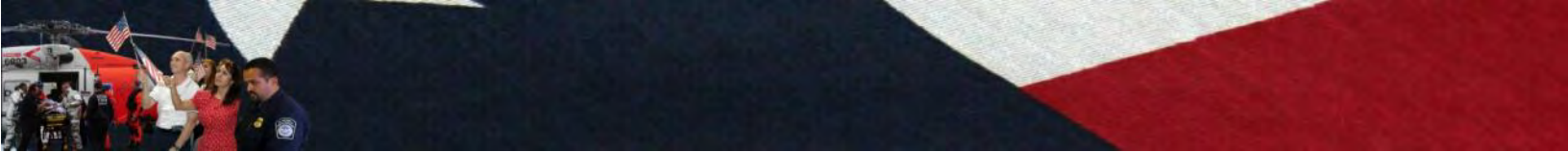
Balance Sheet as of September 30, 2010 (unaudited)

ASSETS

Fund Balance with Treasury	\$715	\$(3)	\$1,533	\$714	\$566	\$1,536	\$5,061
Investments, Net	-	1,940	-	-	1,542	-	3,482
Accounts Receivable	93	140	4	4	195	60	496
Taxes Receivables	81	-	-	-	-	1	82
Other	-	-	139	559	7	74	779
Total Assets	\$889	\$2,077	\$1,676	\$1,277	\$2,310	\$1,671	\$9,900

LIABILITIES

Other Liabilities	\$100	\$1,283	\$1,036	\$20,840	\$305	\$152	\$23,716
Total Liabilities	\$100	\$1,283	\$1,036	\$20,840	\$305	\$152	\$23,716



	Customs User Fees	Sport Fish Restoration Boating Trust Fund	Immigration Examination Fees	National Flood Insurance Program	Oil Spill Liability Trust Fund	All Other Earmarked Funds	Total Earmarked Funds
NET POSITION							
Cumulative Results of Operations	\$789	\$794	\$640	\$(19,563)	\$2,005	\$1,519	\$(13,816)
Total Liabilities and Net Position	\$889	\$2,077	\$1,676	\$1,277	\$2,310	\$1,671	\$9,900

Statement of Net Cost for the Year Ended September 30, 2010 (unaudited)

Gross Program Costs	\$398	\$133	\$2,368	\$2,457	\$405	\$1,035	\$6,796
Less: Earned Revenues	-	-	(2,433)	(3,285)	(516)	(449)	(6,683)
Net Cost of Operations	\$398	\$133	\$(65)	\$(828)	\$(111)	\$586	\$113

Statement of Changes in Net Position for the Year Ended September 30, 2010 (unaudited)

Net Position Beginning of Period	\$811	\$850	\$506	\$(20,388)	\$1,441	\$1,370	\$(15,410)
Net Cost of Operations	(398)	(133)	65	828	111	(586)	(113)
Non-exchange Revenue	382	638	-	-	550	37	1,607
Other	(6)	(561)	69	(3)	(97)	698	100
Change in Net Position	(22)	(56)	134	825	564	149	1,594
Net Position, End of Period	\$789	\$794	\$640	\$(19,563)	\$2,005	\$1,519	\$(13,816)

Customs User Fees

When signed in April 1986, COBRA (Pub. L. 99-272) authorized CBP to collect user fees for certain services. The law initially established processing fees for air and sea passengers, commercial trucks, rail cars, private vessels and aircraft, commercial vessels, dutiable mail packages, and CBP broker permits. An additional fee category, contained in tax reform legislation, for processing barges and bulk carriers for Canada and Mexico, was added later that year.

In addition to the collection of user fees, other changes in CBP procedures were enacted due to the COBRA statute. Most importantly, provisions were included for providing non-reimbursable inspectional overtime services and paying for excess pre-clearance costs from COBRA user fee collections.

The *Customs and Trade Act of 1990* amended the COBRA legislation to provide for the hiring of inspectional personnel, the purchasing of equipment, and the covering of related expenses with any surplus monies available after overtime and excess pre-clearance costs are satisfied. Expenditures from the surplus can only be used to enhance the service provided to those functions for which fees are collected. The fees for certain customs services are provided by 19 U.S.C. § 58c. The authority to use these funds is contained in the annual DHS Appropriations Act.



Sport Fish Restoration and Boating Trust Fund (SFRBTF)

The SFRBTF, previously known as the Aquatic Resources Trust Fund, was created by Section 1016 of the *Deficit Reduction Act of 1984* (Pub. L. 98-369). Two funds were created under this act, the Boating Safety Account and the Sport Fish Restoration Account. The SFRBTF has been the source of budget authority for the boat safety program for many years through the transfer of appropriated funds. The SFRBTF is a Treasury-managed fund and provides funding to states and other entities to promote boating safety and conservation of U.S. recreational waters.

This fund receives revenues transferred from custodial activities of the Treasury, which are deposited in a Treasury account. The revenues are derived from a number of sources, including motor boat fuel tax, excise taxes on sport fishing equipment, and import duties on fishing tackle and yachts. Three agencies share in the available portion of the revenue: Fish and Wildlife Service in the U.S. Department of Interior (Treasury Account Fund Symbol (TAFS) 14X8151); the U.S. Army Corps of Engineers (TAFS 96X8333); and the U.S. Coast Guard (TAFS 70X8149 and TAFS 70X8147).

The most recent reauthorization of SFRBTF and expenditure of Boating Safety funds for the National Recreational Boating Safety Program was enacted in 2005 in the *Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users* (Pub. L. 109-59) and the *Sportfishing and Recreational Boating Safety Amendments Act of 2005* (Pub. L. 109-74).

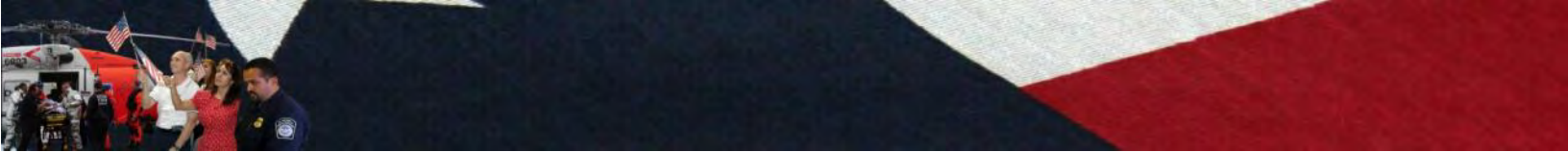
Immigration Examination Fees

In 1988, Congress established the Immigration Examination Fee Account (IEFA), and the fees deposited into the IEFA have been the primary source of funding for providing immigration and naturalization benefits and other benefits as directed by Congress. The *Immigration and Nationality Act* (INA) (Pub. L. 82-414, Section 286(m)) provides for the collection of fees at a level that will ensure recovery of the costs of providing adjudication and naturalization services, including the costs of providing similar services without charge to asylum applicants and other immigrants. The INA also states that the fees may recover administrative costs. This revenue remains available to provide immigration and naturalization benefits and allows the collection, safeguarding, and accounting for fees.

The primary sources of revenue are the application and petition fees that are collected during the course of the fiscal year and deposited into the Immigration Examinations Fee Account (TAFS 70X5088). In addition, USCIS provides specific services to other federal agencies, such as production of border crossing cards for the U.S. Department of State, that result in the collection of other revenues arising from intragovernmental activities.

National Flood Insurance Program

The NFIP was established by the *National Flood Insurance Act of 1968* (Pub. L. 90-448). The purpose of NFIP is to better indemnify individuals for flood losses through insurance, reduce future flood damages through state and community floodplain management regulations, and reduce federal expenditures for disaster assistance and flood control.



The *Flood Disaster Protection Act of 1973* (Pub. L. 93-234) expanded the authority of FEMA and its use of the NFIP to grant premium subsidies as an additional incentive to encourage widespread state, community, and property owner acceptance of the program requirements.

The *National Flood Insurance Reform Act of 1994* (Pub. L. 103-325) reinforced the objective of using insurance as the preferred mechanism for disaster assistance by expanding mandatory flood insurance purchase requirements and by effecting a prohibition on further flood disaster assistance for any property where flood insurance, after having been mandated as a condition for receiving disaster assistance, is not in force.

The *Bunning-Bereuter-Blumenauer Flood Insurance Reform Act of 2004* (Pub. L. 108-264) provides additional tools for addressing the impact of repetitive loss properties on the National Flood Insurance Fund.

The NFIP requires all partners (Write Your Own (WYO) companies) in the program to submit financial statements and statistical data to the NFIP Legacy Systems Services on a monthly basis. This information is reconciled, and the WYO companies are required to correct any variances.

The NFIP is an insurance program for which the Department pays claims to policyholders that experience flood damage due to flooding within the rules and regulations. The WYO companies that participate in the program have authority to use Departmental funds (revenue and other financing sources) to respond to the obligations of the policyholders. Congress has mandated that the NFIP funds are used only to pay claims and claims-related loss adjustment expenses caused by flooding.

The NFIP sources of revenue and other financing comes from premiums collected to insure policyholders' homes and the borrowing authority provided to the program from Congress. The resources are inflows to the Government and are not the result of intragovernmental flows.

Oil Spill Liability Trust Fund

The Oil Spill Liability Trust Fund (OSLTF) was originally established under § 9509 of the *Internal Revenue Code of 1986*. The *Oil Pollution Act of 1990* (OPA) (Pub. L. 101-380) authorized the use of the money or the collection of revenue necessary for its maintenance.

Fund uses defined by the OPA include removal costs incurred by the U.S. Coast Guard and the Environmental Protection Agency; state access for removal activities; payments to federal, state, and Indian tribe trustees to conduct natural resource damage assessments and restorations; payment of claims for uncompensated removal costs and damages; costs and expenses reasonably necessary for the implementation of OPA (subject to congressional appropriations); and other specific appropriations by the Congress.

The OSLTF has four major funds: the Principal Fund (TAFS 70X8185), Emergency Fund (TAFS 70X8349), Claims Fund (TAFS 70X8312) and Trust Fund Share of Expenses (TAFS 70 8314) appropriated annually to the U.S. Coast Guard. All revenue is deposited directly into the Principal Fund. The recurring and nonrecurring revenue are derived from a number of sources, including barrel tax, interest from U.S. Treasury investments, cost recoveries, and fines and penalties. The Emergency Fund is available for federal on-scene coordinators (FOSCs) to respond to discharges



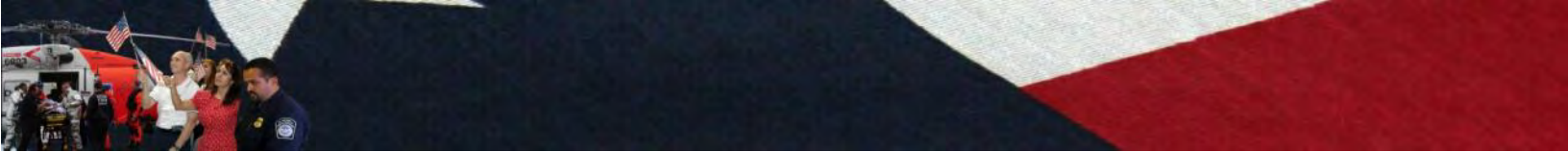
and for federal trustees to initiate natural resource damage assessments. The Emergency Fund is a recurring \$50 million appropriation available to the President annually. The fund remains available until expended. Claimants may file oil spill related claims against the Claims Fund if the responsible party is not identified or denies the claims. The maximum amount that can be paid from the OSLTF with respect to any single incident shall not exceed \$1 billion. Once the maximum payout has been reached for the incident, no additional funds can be disbursed from the OSLTF for that specific incident. Trust Fund Share of Expenses is funded by annual Congressional appropriations from the OSLTF that are then distributed to the U.S. Coast Guard Operating Expenses; Acquisition, Construction and Improvements; and Research, Development, Test and Evaluation appropriations.

Deepwater Horizon Oil Spill. On April 20, 2010, the offshore drilling platform, Deepwater Horizon, exploded and sank 52 miles southeast of Venice, Louisiana. An estimated 4.9 million barrels of oil leaked from the sunken platform's undersea ruptured pipe. The states of Louisiana, Mississippi, Alabama, Florida, and Texas were affected by the spill. The cost of clean-up and damages is unprecedented.

There are currently five identified responsible parties and two guarantors for the Deepwater Horizon oil spill. Liability is joint and severable under the OPA (33 U.S.C. 2701 et seq). The OPA and the *Clean Water Act* (33 U.S.C. 1321 et seq) direct the responsible parties to conduct clean up operations, and to advertise and pay claims for damages specified by the OPA. Under the OPA, the responsible party is liable for costs associated with the containment or clean up of the spill, property damage, loss of government revenue, loss of profits or earning capacity, loss of subsistence use of natural resources, increased state and local public service costs, and damages to natural resources resulting from the spill. In addition, the OPA and applicable federal legislation and regulations provide the U.S. Coast Guard with broad responsibilities and authorities regarding oil spill response oversight on the navigable waters of the United States. The U.S. Coast Guard has been designated as the FOSC to respond to this disaster. As FOSC, the U.S. Coast Guard directs and coordinates the response activities of all federal agencies. The U.S. Coast Guard has entered into various reimbursable agreements with other federal agencies.

In responding to the Deepwater Horizon oil spill, British Petroleum (BP), a responsible party, established a process designed to pay individual, business, and governmental claims for compensable costs under OPA. BP transferred responsibility for administration and payment of individual and business claims to the Gulf Coast Claims Facility (GCCF) in August 2010. BP established a \$20 billion escrow account, funded over the next three years, to pay spill-related costs, including claims paid by the GCCF. Establishment of this account does not represent a cap or floor on any amount that may ultimately be paid by BP.

The OSLTF provides emergency funding resources to the FOSC for oil removal, and to federal trustees for initial natural resource damage assessment activities, up to amounts specified under OPA Section 6002(b) (33 U.S.C. 2752(b)). In June 2010, the President of the United States signed into law an amendment to Section 6002(b) allowing multiple budgetary authority advances from the OSLTF for the Deepwater Horizon oil spill response and federal natural resource damage assessment activities limited only by the statutory per-incident cap at 26 U.S.C. 9509(c)(2). The status of OSLTF available funds, costs incurred by the Federal Government, and billings to the responsible parties as of September 30, 2011, is described below.



Status of OSLTF Funds and Costs Incurred and Billed. Through September 30, 2011, the Total Incident Cost of the Deepwater Horizon oil spill response was \$847 million. The Total Incident Cost includes both the cost of U.S. Coast Guard assets employed, which are funded from U.S. Coast Guard annual appropriations, and other removal costs, which are funded from the OSLTF. The total U.S. Coast Guard asset costs accumulated through September 30, 2011 are \$322 million. The OSLTF has advanced \$596.3 million to the FOSC to fund Deepwater Horizon oil spill removal activities. Of the amount advanced, FOSC has obligated \$573.6 million. In addition, the U.S. Coast Guard has obligated \$47.8 million out of the OSLTF advance amounts to the Federal Lead Administrative Trustee to initiate the assessment of natural resource damages, as provided by OPA section 6002(b). Amounts expended from the OSLTF through September 30, 2011 are \$363.2 million.

U.S. Coast Guard has billed the responsible parties for \$716.7 million. The billed amounts include \$317.3 million in costs for all U.S. Coast Guard personnel, ships, aircraft, and cutters directly supporting the FOSC; and \$399.4 million in OSLTF funds obligated by the FOSC to other federal, state, and local government agencies for their role in the response. Funds are obligated by the FOSC to other federal, state, and local government agencies via FOSC-approved pollution removal funding authorizations or military interdepartmental purchase requests that provide reimbursable funding authority.

Contingent Liabilities. The OSLTF, which is administered by the U.S. Coast Guard National Pollution Funds Center (NPFC), may be available to pay claims for OPA specified costs and damages, not paid by BP, or another responsible party. Under OPA, claimants are required to present their claims first to the responsible parties (or the GCCF for Deepwater Horizon costs); if not compensated, they may then file an action in court or file a claim against the OSLTF through the NPFC.

All Other Earmarked Funds

The balances and activity reported for all other earmarked funds result from the funds listed below. Information related to these earmarked funds can be located in the Department's appropriations legislation or the statutes referenced.

- 70X0715: Radiological Emergency Preparedness Program, Federal Emergency Management Agency, Department of Homeland Security
- 70X5089: U.S. Customs and Border Protection, Land Border Inspection Fees, Border and Transportation Security, Department of Homeland Security; 116 Stat. 2135
- 70_5087: U.S. Customs and Border Protection, Immigration User Fees, Border and Transportation Security, Department of Homeland Security; 116 Stat. 2135
- 70X5126: Breach Bond/Detention Fund, Border and Transportation Security, Department of Homeland Security; 116 Stat. 2135
- 70X5378: Student and Exchange Visitor Program, Border and Transportation Security, Department of Homeland Security; 110 Stat. 3009-706, Sec. (e)(4)(B)
- 70X5382: Immigration User Fee Account, BICE, Department of Homeland Security; 116 Stat. 2135
- 70X5385: Aviation Security Capital Fund, Transportation Security Administration, Department of Homeland Security; 117 Stat. 2567(h)(1)



- 70_5389: H-1B and L Fraud Prevention and Detection Account, U.S. Citizenship and Immigration Service, Department of Homeland Security; 8 U.S.C. § 1356(s)
- 70X5390: Unclaimed Checkpoint Money, Transportation Security Administration, Department of Homeland Security; 118 Stat. 1317-1318, Sec.515(a)
- 70X5398: H-1B and L Fraud Prevention and Detection, U.S. Immigration and Customs Enforcement, Department of Homeland Security; Pub. L. 108-447, 118 Stat. 3357, Sec. 426(b)(1)
- 70X5451: Immigration Enforcement Account, Border and Transportation Security, Department of Homeland Security; 116 Stat. 2135
- 70X5542: Detention and Removal Operations, U.S. Immigration and Customs Enforcement, Department of Homeland Security; 8 USC 1356(m)-(n); Pub. L. 107-296, Sec. 476c
- 70X5545: Airport Checkpoint Screening Fund, Transportation Security Administration, Department of Homeland Security; Pub. L. 110-161
- 70X5595: Electronic System for Travel Authorization (ESTA) Fees, U.S. Customs and Border Protection, Department of Homeland Security; Pub. L. 110-53, 121 Stat. 344; Pub. L. 111-145, 124 Stat. 56
- 70_5694: User Fees, Small Airports, U.S. Customs Service, Department of Homeland Security; 116 Stat. 2135
- 70X8244: Gifts and Donations, Department Management, Department of Homeland Security; 116 Stat. 2135
- 70X8533: General Gift Fund, U.S. Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70X8870: Harbor Maintenance Fee Collection, U.S. Customs Service, Department of Homeland Security; 116 Stat. 2135
- 70_5106: H-1 B Nonimmigrant Petitioner Account, U.S. Citizenship and Immigration Service, Department of Homeland Security; 116 Stat. 2135
- 70X8360: Gifts and Bequests, Federal Law Enforcement Training Center, Department of Homeland Security; 116 Stat. 2135
- 70X8420: Surcharge Collections, Sales of Commissary Stores, U.S. Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70X8428: Coast Guard Cadet Fund, U.S. Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70X5543: International Registered Traveler Program Fund, U.S. Customs and Border Protection, Department of Homeland Security; 121 Stat. 2091-2092

23. Intragovernmental Costs and Exchange Revenue

For the year ended September 30, 2011 (in millions) (Unaudited)

Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
<i>U.S. Customs and Border Protection</i>			
Gross Cost	\$3,548	\$8,494	\$12,042
Less Earned Revenue	(48)	(130)	(178)
Net Cost	3,500	8,364	11,864
<i>U.S. Coast Guard</i>			
Gross Cost	842	10,847	11,689
Less Earned Revenue	(197)	(471)	(668)
Net Cost	645	10,376	11,021
<i>U.S. Citizenship and Immigration Services</i>			
Gross Cost	735	1,778	2,513
Less Earned Revenue	(3)	(3,043)	(3,046)
Net Cost	732	(1,265)	(533)
<i>Federal Emergency Management Agency</i>			
Gross Cost	1,429	15,729	17,158
Less Earned Revenue	(351)	(3,354)	(3,705)
Net Cost	1,078	12,375	13,453
<i>Federal Law Enforcement Training Center</i>			
Gross Cost	59	382	441
Less Earned Revenue	(35)	(2)	(37)
Net Cost	24	380	404
<i>National Protection and Programs Directorate</i>			
Gross Cost	490	1,927	2,417
Less Earned Revenue	(914)	-	(914)
Net Cost	(424)	1,927	1,503
<i>U.S. Immigration and Customs Enforcement</i>			
Gross Cost	1,427	4,336	5,763
Less Earned Revenue	(25)	(124)	(149)
Net Cost	1,402	4,212	5,614
<i>Office of Health Affairs</i>			
Gross Cost	206	84	290
Less Earned Revenue	-	-	-
Net Cost	206	84	290



Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
<i>Departmental Operations and Other</i>			
Gross Cost	\$650	\$1,274	\$1,924
Less Earned Revenue	(8)	-	(8)
Net Cost	642	1,274	1,916
<i>U.S. Secret Service</i>			
Gross Cost	493	1,355	1,848
Less Earned Revenue	(14)	-	(14)
Net Cost	479	1,355	1,834
<i>Science and Technology Directorate</i>			
Gross Cost	355	533	888
Less Earned Revenue	(9)	(9)	(18)
Net Cost	346	524	870
<i>Transportation Security Administration</i>			
Gross Cost	1,789	5,680	7,469
Less Earned Revenue	(1)	(2,278)	(2,279)
Net Cost	1,788	3,402	5,190
Total Department of Homeland Security			
Gross Cost	12,023	52,419	64,442
Less Earned Revenue	(1,605)	(9,411)	(11,016)
Net Cost Before Loss on Pension, ORB, or OPEB Assumption Changes	10,418	43,008	53,426
Loss on Pension, ORB, or OPEB Assumption Changes	-	400	400
Net Cost	\$10,418	\$43,408	\$53,826

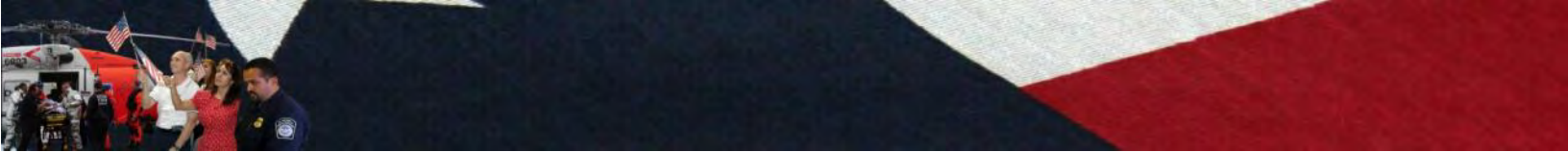
For the year ended September 30, 2010 (in millions) (Unaudited)

Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
<i>U.S. Customs and Border Protection</i>			
Gross Cost	\$3,247	\$8,528	\$11,775
Less Earned Revenue	(40)	(112)	(152)
Net Cost	3,207	8,416	11,623
<i>U.S. Coast Guard</i>			
Gross Cost	1,150	11,825	12,975
Less Earned Revenue	(137)	(760)	(897)
Net Cost	1,013	11,065	12,078
<i>U.S. Citizenship and Immigration Services</i>			
Gross Cost	722	1,809	2,531
Less Earned Revenue	(3)	(2,415)	(2,418)
Net Cost	719	(606)	113
<i>Federal Emergency Management Agency</i>			
Gross Cost	1,207	13,000	14,207
Less Earned Revenue	(364)	(3,317)	(3,681)
Net Cost	843	9,683	10,526
<i>Federal Law Enforcement Training Center</i>			
Gross Cost	61	349	410
Less Earned Revenue	(34)	(2)	(36)
Net Cost	27	347	374
<i>National Protection and Programs Directorate</i>			
Gross Cost	414	1,647	2,061
Less Earned Revenue	(828)	-	(828)
Net Cost	(414)	1,647	1,233
<i>U.S. Immigration and Customs Enforcement</i>			
Gross Cost	1,477	4,273	5,750
Less Earned Revenue	(73)	(156)	(229)
Net Cost	1,404	4,117	5,521
<i>Office of Health Affairs</i>			
Gross Cost	150	81	231
Less Earned Revenue	-	-	-
Net Cost	150	81	231



Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
<i>Departmental Operations and Other</i>			
Gross Cost	\$680	\$1,200	\$1,880
Less Earned Revenue	(6)	-	(6)
Net Cost	674	1,200	1,874
<i>U.S. Secret Service</i>			
Gross Cost	442	1,340	1,782
Less Earned Revenue	(15)	-	(15)
Net Cost	427	1,340	1,767
<i>Science and Technology Directorate</i>			
Gross Cost	408	479	887
Less Earned Revenue	(3)	(2)	(5)
Net Cost	405	477	882
<i>Transportation Security Administration</i>			
Gross Cost	1,386	5,245	6,631
Less Earned Revenue	-	(2,145)	(2,145)
Net Cost	1,386	3,100	4,486
Total Department of Homeland Security			
Gross Cost	11,344	49,776	61,120
Less Earned Revenue	(1,503)	(8,909)	(10,412)
Net Cost Before Loss on Pension, ORB, or OPEB			
Assumption Changes	9,841	40,867	50,708
Loss on Pension, ORB, or OPEB Assumption			
Changes	-	5,675	5,675
Net Cost	\$9,841	\$46,542	\$56,383

Intragovernmental costs represent exchange transactions made between two reporting entities within the Federal Government and are presented separately from costs with the public (exchange transactions made between the reporting entity and a non-federal entity). Intragovernmental exchange revenue is disclosed separately from exchange revenue with the public. The criteria used for this classification requires that the intragovernmental expenses relate to the source of goods and services purchased by the reporting entity and not to the classification of related revenue. For example, with “exchange revenue with the public,” the buyer of the goods or services is a non-federal entity. With “intragovernmental costs,” the buyer and seller are both federal entities. If a federal entity purchases goods or services from another federal entity and sells them to the public, the exchange revenue would be classified as “with the public,” but the related costs would be classified as “intragovernmental.” The purpose of this classification is to enable the Federal Government to provide consolidated financial statements, and not to match public and intragovernmental revenue with costs that are incurred to produce public and intragovernmental revenue.



24. Suborganization Costs by DHS Missions and Goals

Operating costs are summarized in the Statement of Net Cost by responsibility segment, as applicable to the reporting period. A responsibility segment is the Component that carries out a mission or major line of activity, and whose managers report directly to Departmental management.

Net cost of operations is the gross (i.e., total) cost incurred by the Department, excluding any gains and losses from changes in long-term assumptions used to measure federal civilian and military employee pensions, other retirement benefits (ORB), and other postemployment benefits (OPEB), including veterans' compensation, less any exchange (i.e., earned) revenue. Gains and losses from changes in long-term assumptions used to measure federal civilian and military employee pensions, ORB, and OPEB are reported on a separate line item in accordance with SFFAS No. 33, *Pensions, Other Retirement Benefits, and Other Postemployment Benefits: Reporting the Gains and Losses from Changes in Assumptions and Selecting Discount Rates and Valuation Dates*.

In FY 2010, the Department completed the Quadrennial Homeland Security Review (QHSR), which established a unified, strategic framework for homeland security missions and goals, and also conducted a Bottom-Up Review (BUR) to align programmatic activities and organizational structure to those missions and goals. Since the QHSR and the BUR reflect the most comprehensive assessment and analysis of Homeland Security to date, the Department has elected to use them as basis for integrating net cost to performance information. The Department is implementing and refining an appropriate cost methodology within the QHSR framework that will be used to present DHS suborganization costs by mission and goals in future disclosures.



25. Apportionment Categories of Obligations Incurred: Direct versus Reimbursable Obligations

Apportionment categories are determined in accordance with the guidance provided in OMB Circular No. A-11, *Preparation, Submission and Execution of the Budget*. Category A represents resources apportioned for calendar quarters. Category B represents resources apportioned for other time periods; for activities, projects, or objectives; or for any combination thereof (in millions).

Year Ended September 30, 2011 (Unaudited):	Apportionment Category A	Apportionment Category B	Exempt from Apportionment	Total
Obligations Incurred – Direct	\$36,638	\$23,801	\$1,229	\$61,668
Obligations Incurred – Reimbursable	4,008	850	12	4,870
Total Obligations Incurred	\$40,646	\$24,651	\$1,241	\$66,538

Year Ended September 30, 2010 (Unaudited):	Apportionment Category A	Apportionment Category B	Exempt from Apportionment	Total
Obligations Incurred – Direct	\$34,501	\$27,823	\$1,020	\$63,344
Obligations Incurred – Reimbursable	4,003	654	11	4,668
Total Obligations Incurred	\$38,504	\$28,477	\$1,031	\$68,012

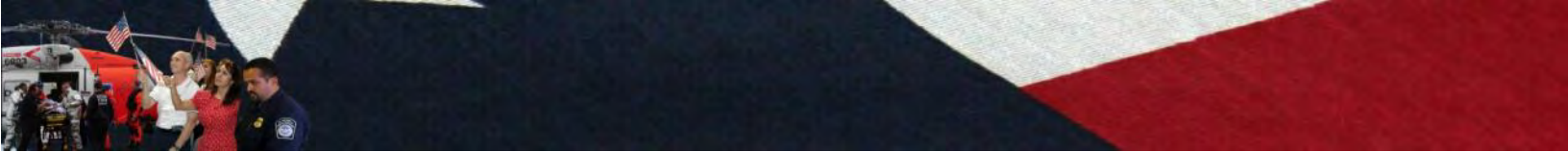
26. Available Borrowing Authority

At the beginning of FY 2011, the Department, through FEMA's NFIP, had available borrowing authority of \$1,427 million (unaudited). During FY 2011, FEMA did not receive any new borrowing authority and did not use any borrowing authority, which leaves a balance of \$1,427 million (unaudited). For FY 2010, FEMA had a beginning balance of \$1,427 million (unaudited) in borrowing authority. During FY 2010, FEMA did not receive new borrowing authority and did not use any borrowing authority, which left a balance of \$1,427 million (unaudited). FEMA annually requests borrowing authority to cover the principal amount of direct loans not to exceed \$25 million less the subsidy due from the program account.

27. Permanent Indefinite Appropriations

Permanent indefinite appropriations are appropriations that result from permanent public laws, which authorize the Department to retain certain receipts. The amount appropriated depends upon the amount of the receipts rather than on a specific amount. The Department has three permanent indefinite appropriations, which are not subject to budgetary ceilings established by Congress:

- CBP has a permanent and indefinite appropriation that is used to disburse tax and duty refunds and duty drawbacks. Although funded through appropriations, refund and drawback activity is, in most instances, reported as custodial activity of the Department. Refunds are custodial revenue-related activity in that refunds are a direct result of overpayments of taxes, duties, and fees. CBP's refunds payable at year-end are not subject to funding restrictions.



Federal tax revenue received from taxpayers is not available for use in the operation of the Department and is not reported on the Statement of Net Cost. Likewise, the refunds of overpayments are not available for use by the Department in its operations.

- USSS has a permanent and indefinite appropriation that is used to reimburse the DC Pension Plan for the difference between benefits to participants in the DC Pension Plan (see Note 16) and payroll contributions received from current employees.
- USCIS has permanent authority to use immigration and naturalization application fees to pay costs of providing adjudication and naturalization services, including the costs of providing services without charge to asylum applicants and other immigrants and costs associated with the collection, safeguarding, and accounting for fees. USCIS also has the authority to transfer certain fees to other federal agencies, including the Department of Labor, the Department of State, and the National Science Foundation. The transferred funds are earmarked for immigration fraud prevention and domestic training programs intended to reduce the need for foreign workers under the H-1B visa program.

28. Legal Arrangements Affecting the Use of Unobligated Balances

Unobligated balances whose period of availability has expired are not available to fund new obligations. Expired unobligated balances are available to pay for current period adjustments to obligations incurred prior to expiration. For a fixed appropriation account, the balance can be carried forward for five fiscal years after the period of availability ends. At the end of the fifth fiscal year, the account is closed and any remaining balance is canceled and returned to Treasury. For a no-year account, the unobligated balance is carried forward indefinitely until specifically rescinded by law or the head of the agency concerned or the President determines that the purposes for which the appropriation was made have been carried out and disbursements have not been made against the appropriation for two consecutive years.

Included in the cumulative results of operations for special funds is \$1 billion and \$924 million (unaudited) at September 30, 2011, and September 30, 2010, respectively, that represents the Department's authority to assess and collect user fees relating to merchandise and passenger processing; to assess and collect fees associated with services performed at certain small airports or other facilities; to retain amounts needed to offset costs associated with collecting duties; and taxes and fees for the Government of Puerto Rico. These special fund balances are restricted by law in their use to offset specific costs incurred by the Department. Part of the passenger fees in the User Fees Account, totaling approximately \$729 million and \$743 million (unaudited) at September 30, 2011 and 2010, respectively, is restricted by law in its use to offset specific costs incurred by the Department and are available to the extent provided in Department appropriation acts.

The entity trust fund balances result from the Department's authority to use the proceeds from general order items sold at auction to offset specific costs incurred by the Department relating to their sale, to use available funds in the Salaries and Expense Trust Fund to offset specific costs for expanding border and port enforcement activities, and to use available funds from the Harbor

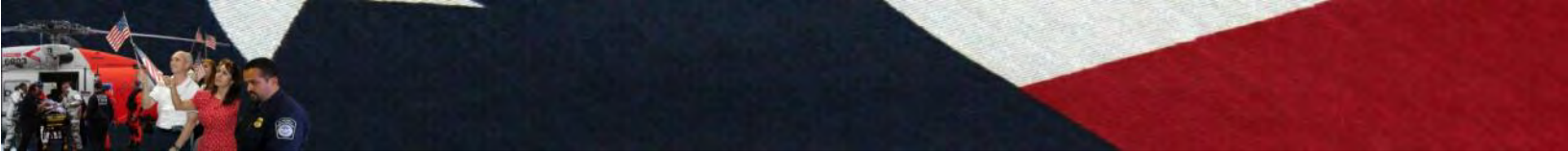


Maintenance Fee Trust Fund to offset administrative expenses related to the collection of the Harbor Maintenance Fee.

29. Explanation of Differences between the Statement of Budgetary Resources and the Budget of the U.S. Government

The table below documents the material differences between the FY 2010 Statement of Budgetary Resources (SBR) and the actual amounts reported for FY 2010 in the Budget of the U.S. Government. Since the FY 2011 financial statements will be reported prior to the release of the Budget of the U.S. Government, DHS is reporting for FY 2010 only. Typically, the Budget of the U.S. Government with the FY 2011 actual data is published in February of the subsequent year. Once published, the FY 2011 actual data will be available on the OMB website at: www.whitehouse.gov/omb.

	Budgetary Resources	Obligations Incurred	Distributed Offsetting Receipts	Net Outlays
FY 2010 Actual Balances per the FY 2011 Budget of the U.S. Government (in millions) (Unaudited)	\$79,690	\$66,477	\$6,328	\$50,785
Reconciling Items:				
Accounts that are expired that are not included in Budget of the United States	1,741	315	-	-
Distributed Offsetting Receipts not included in the Budget of the United States	-	-	-	(6,328)
Refunds and drawbacks not included in the Budget of the United States	806	259	-	259
Byrd Program (Continued Dumping and Subsidy Offset) not included in the Budget of the United States	972	972	-	969
Biodefense Countermeasure Program included in the Budget of the United States	-	-	-	(96)
Miscellaneous Differences	(9)	(11)	-	(1)
Per the 2010 SBR (Unaudited)	\$83,200	\$68,012	\$6,328	\$45,588



30. Undelivered Orders, Unpaid, End of Period

An unpaid undelivered order exists when a valid obligation has occurred and funds have been reserved but the goods or services have not been delivered. Undelivered orders for the periods ended September 30, 2011 and 2010, were \$42,011 million (unaudited) and \$43,445 million (unaudited), respectively.

31. Custodial Revenues

The Department collects revenue from a variety of duties, excise taxes, and various other fees. Collection activity primarily relates to current-year activity. Non-entity revenue reported on the Department's Statement of Custodial Activity include duties, excise taxes, and various non-exchange fees collected by CBP. CBP assesses duties, taxes, and fees on goods and merchandise brought into the United States from foreign countries. For FY 2010, non-entity revenue also includes user fees collected by USCIS that were subsequently remitted to the Treasury General Fund or to other federal agencies. In FY 2011, these user fees are reported as exchange revenue on the Statement of Net Cost to more fairly present the Department's results of operations and changes in net position. For additional information, see Note 1.X., Exchange and Non-exchange Revenue.

The significant types of non-entity accounts receivable (custodial revenues as presented in the Statement of Custodial Activity) are described below.

- **Duties:** amounts collected on imported goods collected on behalf of the Federal Government.
- **User fees:** amounts designed to maintain U.S. harbors and to defray the cost of other miscellaneous service programs.
- **Excise taxes:** amounts collected on imported distilled spirits, wines, tobacco products, and other miscellaneous taxes collected on the behalf of the Federal Government.
- **Fines and penalties:** amounts collected for violations of laws and regulations.

Refunds are amounts due to the importer/exports as a result of overpayments of duties, taxes, fees, and interest. Refunds include drawback remittance paid when imported merchandise, for which duty was previously paid, is exported from the United States.

Tax disbursements from the refunds and drawbacks account, broken out by revenue type and by tax year, were as follows for the fiscal years ended September 30, 2011 and 2010 (in millions):



	2011 Tax Disbursements			
	Tax Year			
	2011	2010	2009	Prior Years
Customs duties	\$720	\$271	\$90	\$267
Total non-exchange revenue refunded	720	271	90	267
Exchange revenue refunded	-	-	-	-
Total tax refunds and drawbacks disbursed	\$720	\$271	\$90	\$267

	2010 Tax Disbursements (Unaudited)			
	Tax Year			
	2010	2009	2008	Prior Years
Customs duties	\$767	\$154	\$74	\$284
Total non-exchange revenue refunded	767	154	74	284
Exchange revenue refunded	-	-	-	-
Total tax refunds and drawbacks disbursed	\$767	\$154	\$74	\$284

The disbursements include interest payments of \$42 million and \$35 million (unaudited) for the fiscal years ended September 30, 2011 and 2010, respectively.

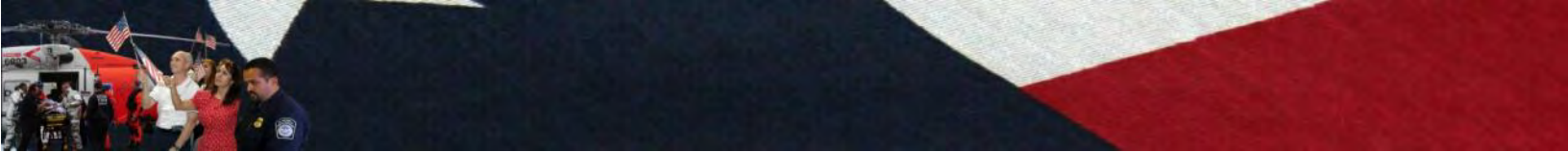
The disbursement totals for refunds include antidumping and countervailing duties collected that are refunded pursuant to rulings by DOC. These duties are refunded when the DOC issues a decision in favor of the foreign industry. See Note 18, Other Liabilities, for more information.

32. Reclassifications and Other Reporting Changes

Reclassifications

During FY 2011, the Department added a budgetary impact indicator to its chart of accounts because of updates to the U.S. Standard General Ledger crosswalk provided by the U.S. Treasury. Based on the attribute additions, DHS determined non-exchange revenue for CBP reported on the Statement of Changes of Net Position should be reclassified in FY 2010 from a Budgetary Financing Source to an Other Financing Source for comparative purposes. This resulted in a \$2 billion reclassification adjustment to the Statement of Changes in Net Position and related footnotes. The reclassification did not affect the total Cumulative Results of Operations for FY 2010.

In FY 2011, a reclassification was made to the FY 2010 Balance Sheet and related footnotes to combine the liabilities from the Unliquidated Antidumping and Countervailing Duties line into the



Other line. Therefore, the Department is not presenting liabilities from Unliquidated Antidumping and Countervailing Duties as a separate line of the Balance Sheet.

Other Reporting Changes

Effective October 1, 2010, the Department implemented a change in reporting the user fees collected by USCIS under the H-1B Nonimmigrant Petitioner Account and H-1 B and L Fraud Prevention and Detection Account as exchange revenue reported on the Statement of Net Cost. These user fees were previously reported on the Statement of Custodial Activity. The basis for implementing the reporting change is to more fairly present the Department's results of operations and changes in net position, and therefore no adjustment to the beginning balance is necessary.

Beginning October 1, 2010, the U.S. Coast Guard no longer recognizes an actuarial unfunded liability for PCS transfer benefits. Instead, the U.S. Coast Guard records obligations for separation PCS orders in the fiscal year in which they are issued.



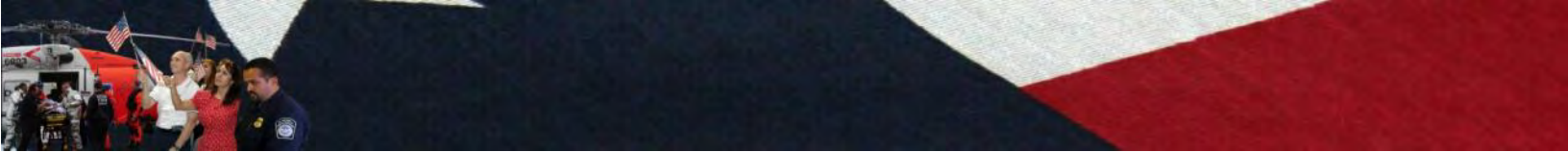
33. Reconciliation of Net Cost of Operations (Proprietary) to Budget

The Reconciliation of Net Cost of Operations to Budget reconciles the Department's Resources Used to Finance Activities (first section), which consists of the budgetary basis of accounting Net Obligations plus the proprietary basis of accounting Other Resources, to the proprietary basis of accounting Net Cost of Operations. The second section, Resources Used to Finance Items Not Part of the Net Cost of Operations, reverses out items included in the first section that are not included in Net Cost of Operations. The third section, Components of Net Cost of Operations that Will Not Require or Generate Resources in the Current Period, adds items included in the Net Cost of Operations that are not included in the first section.

The third section's subsection, Components Requiring or Generating Resources in Future Periods, includes costs reported in the current period that are included in the Liabilities Not Covered by Budgetary Resources reported in Note 14. This subsection does not include costs reported in prior fiscal years that are also included in Liabilities Not Covered by Budgetary Resources.

The reconciliations of net cost of operations to budget for FY 2011 and FY 2010 are as follows:

	2011 <u>(Unaudited)</u>	2010 <u>(Unaudited)</u>
Resources Used to Finance Activities		
Budgetary Resources Obligated		
Obligations Incurred (Note 25)	\$66,538	\$68,012
Less: Spending Authority from Offsetting Collections and Recoveries	<u>(14,731)</u>	<u>(14,533)</u>
Obligations Net of Offsetting Collections and Recoveries	51,807	53,479
Less: Offsetting Receipts	<u>(6,246)</u>	<u>(6,328)</u>
Net Obligations	<u>45,561</u>	<u>47,151</u>
Other Resources		
Donations and Forfeiture of Property	-	3
Transfers In (Out) Without Reimbursement	114	120
Imputed Financing from Costs Absorbed by Others	1,522	1,064
Other	2,020	1,926
Net Other Resources Used to Finance Activities	<u>3,656</u>	<u>3,113</u>
Total Resources Used to Finance Activities	<u>\$49,217</u>	<u>\$50,264</u>



Resources Used to Finance Items Not Part of the Net Cost of Operations

Change in Budgetary Resources Obligated for Goods, Services and Benefits Ordered but Not Yet Provided	\$(1,742)	\$1,192
Resources that Fund Expenses Recognized in Prior Periods	1,099	27
Budgetary Offsetting Collections and Receipts that Do Not Affect Net Cost of Operations:		
Credit Program Collections that Increase Liabilities for Loan Guarantees or Allowances for Subsidy	37	33
Other	(729)	(3,504)
Resources that Finance the Acquisition of Assets	3,425	3,664
Other Resources or Adjustments to Net Obligated Resources that Do Not Affect Net Cost of Operations	1,344	3,233
Total Resources Used to Finance Items Not Part of the Net Cost of Operations	<u>3,434</u>	<u>4,645</u>
TOTAL RESOURCES USED TO FINANCE THE NET COST OF OPERATIONS	<u>\$45,783</u>	<u>\$45,619</u>

Components of the Net Cost of Operations that Will Not Require or Generate Resources in the Current Period:

Components Requiring or Generating Resources in Future Periods

Increase in Annual Leave Liability	\$60	\$109
Increase in Environmental and Disposal Liability	5	49
Increase in Exchange Revenue Receivable from the Public	-	(7)
Upward/Downward Reestimates of Credit Subsidy Expense	(2)	-
Other		
Increase in Insurance Liabilities	3,740	-
Increase in Actuarial Pension Liability	2,274	7,024
Increase in Actuarial Health Insurance Liability	-	1,754
Increase in USCG Military Post-Employment Benefits and Other	-	1
Other	-	377
Total Components of Net Cost of Operations that Will Require or Generate Resources in Future Periods	6,077	9,307
Components not Requiring or Generating Resources		
Depreciation and Amortization	2,271	1,560
Revaluation of Assets or Liabilities	566	48
Other	(871)	(151)
Total Components of Net Cost of Operations that Will Not Require or Generate Resources	1,966	1,457
Total Components of Net Cost of Operations That Will Not Require or Generate Resources in the Current Period	<u>8,043</u>	<u>10,764</u>
NET COST OF OPERATIONS	<u><u>\$53,826</u></u>	<u><u>\$56,383</u></u>



Required Supplementary Stewardship Information

Unaudited, see accompanying Auditors' Report

Stewardship Investments

Stewardship investments are substantial investments made by the Federal Government for the benefit of the Nation. When incurred, stewardship investments are treated as expenses in calculating net cost, but they are separately reported as Required Supplementary Stewardship Information to highlight the extent of investments that are made for long-term benefit. The Department's expenditures (including carryover funds expended in FY 2011) in Human Capital, Research and Development, and Non-Federal Physical Property are shown below:

Summary of Stewardship Investments (in millions)					
	FY 2011	FY 2010	FY 2009	FY 2008	FY 2007
Research and Development	\$789	\$980	\$852	\$880	\$1,115
Human Capital	50	102	111	98	82
Non-Federal Physical Property	229	286	420	204	394
Total	\$1,068	\$1,368	\$1,383	\$1,182	\$1,591

1. Investments in Research and Development

Investments in research and development represent expenses incurred to support the search for new or refined knowledge and ideas. The intent of the investment is to apply or use such knowledge to improve and develop new products and processes with the expectation of maintaining or increasing national productive capacity or yielding other future benefits. TSA, U.S. Coast Guard, and S&T have made significant investments in research and development.

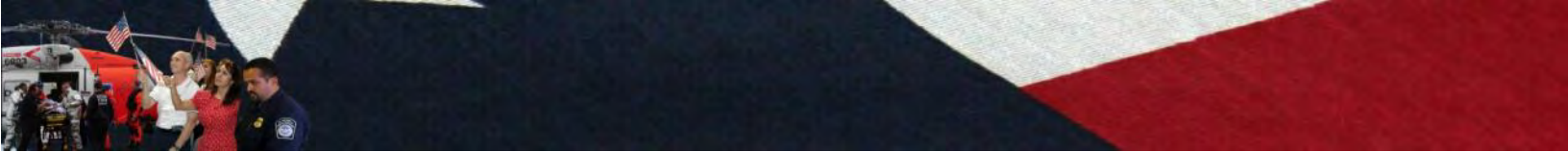
TSA

TSA has invested in three categories of applied research projects. These applied research projects include:

- Human factors research intended to enhance screener capabilities, improve the human operability of machines, and increase human system effectiveness.
- Ongoing certification testing of screening technologies including Explosive Detection System and Explosives Trace Detection technology.
- Infrastructure protection research related to using biometrics for passenger access controls.

U.S. Coast Guard

The U.S. Coast Guard Research & Development Program is the sole facility for performing research, development, and test and evaluation in support of its major missions. It executes a portfolio of 80 to 90 projects for a multitude of U.S. Coast Guard Headquarters Program Offices and Area Commanders across the current major research areas of oil spill response technology,



energy conservation and green technologies, C4ISR, e-navigation technologies, development of new Arctic capabilities, and applied operations research to improve U.S. Coast Guard operations.

The following are three key areas of ongoing developmental projects, including significant accomplishments in each:

- Ballast Water Treatment. Develop a means to certify ballast water treatment systems to ensure aquatic nuisance species are eradicated before entering U.S. waters. The U.S. Coast Guard delivered “Feasibility of Developing a Protocol for Automated Protist Analysis” that supported continued automated protist analysis work in ballast water treatment systems development
- Operations Research. Expand existing sensor modeling and simulation tools to incorporate multiple U.S. Coast Guard sensors against a wider range of targets from air, surface, and/or shore-based platforms to support analysis of multi-sensor searches in coordinated search and surveillance operations. The U.S. Coast Guard demonstrated the Arctic Tactical Modeling Environment, a prototype simulation model that measures the relative effectiveness of various force-deployment options in the Arctic Region.
- Oil Spill Response. Develop and evaluate the most promising capabilities and techniques for recovering heavy viscous oil on the ocean floor and in the water column and integrate those capabilities and techniques with heavy oil detection systems. The U.S. Coast Guard initiated development of prototype recovery systems, which can be integrated with previously evaluated detection systems and consolidated and assessed matters from previously held oil spill response workshops to identify areas of enhancement for removal of oil in ice environments.

The following major new applications developments are ongoing:

- Operations Research. Review acquisition, deployment, and operational assumptions about C4ISR in the Coast Guard and determine how increasing C4ISR investments are proposed to improve operational performance. Research tools, methods, and measures of effectiveness that can support a quantitative assessment of the operational performance impacts of C4ISR investments. Develop a prototyping capability for demonstration.
- Energy Conservation/ Green Technologies. Explore the U.S. Coast Guard’s needs with regard to alternative energy systems and the extent these systems are currently used throughout the U.S. Coast Guard. Baseline the carbon footprint of selected U.S. Coast Guard afloat assets. Investigate potential “green” technology projects for powering U.S. Coast Guard afloat assets and the technologies that have the potential for providing renewable energy while lowering the carbon footprint.
- Navigation Technologies. Conduct a review of distress notification methods and determine the most effective methods and systems, or combinations, and propose carriage regulation changes that allow alternatives or a combination of alternatives to current requirements that are found to be less than effective.

Significant accomplishments in research:

- Energy Conservation/Green Technologies. Completed deployment of a demonstration tidal energy generator in the vicinity of an active pier at U.S. Coast Guard Station, Eastport,



Maine. Developed a method to measure the carbon footprint of a U.S. Coast Guard vessel. Initiated studies of alternative fuel use on U.S. Coast Guard outboard-powered boats.

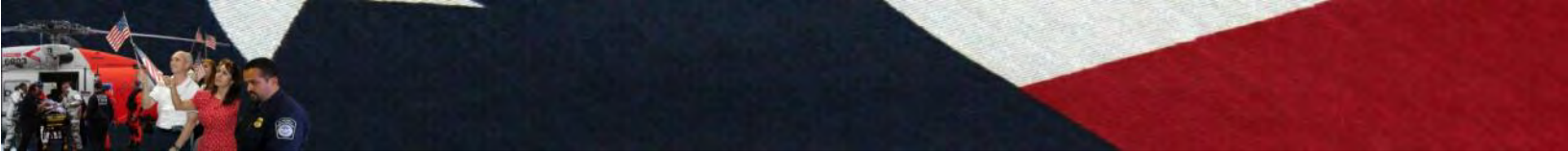
- **Biometrics:** Identified numerous issues with regard to leveraging different Federal Government biometric databases. Completed a 10-print capture demonstration in the Mona Pass and provided information for available Multi-digit Handheld Biometric Scanners giving U.S. Coast Guard decision makers vital information regarding migration to a multi-digit collection system. Conducted a multi-agency/stakeholder table top exercise to evaluate the proposed operational and management reporting display process.
- **Operations Research.** Enhanced existing sensor/target/environment models using physics-based assertions. Identified an affordable path forward for sensor performance modeling that allows for scalable improvements and future growth including RADAR and Electro-Optic sensor analysis (e.g., models including environment, targets, and sensors of interest to the U.S. Coast Guard). Initiated planning for model validation exercises with NATO.

S&T

The S&T Directorate has a research portfolio investment integrated through its divisions. For example, the Directorate conducts research in many areas to support the Department's missions to defend against chemical and biological threats, including protecting infrastructure and transportation systems from explosives, preparing the nation to respond to large- and small-scale events, and protecting the critical systems that run our financial and electrical power systems, to name a few. The S&T Directorate also develops new standards, educates the next-generation workforce, and conducts testing and evaluation activities to further increase the security of the nation.

Significant accomplishments in applied research include:

- DHS S&T developed the Advanced Heavy Breaching Tool called Controlled Impact Rescue Tool (CIRT), which can substantially reduce the time it takes to breach reinforced concrete walls by Urban Search and Rescue (USAR) teams. The faster breaching translates into shorter time to reach a victim increasing the probability of success during a rescue mission. CIRT has been transitioned into manufacturing as a commercial product and is included in FEMA's Authorized Equipment List (AEL). Currently, FEMA has acquired six units for their inventory of tools; in 2011, CIRT units were provided to ten USAR teams across the United States. Current S&T activities also include a signed project arrangement (PA) between DHS S&T and Singapore Ministry of Home Affairs (MHA) for a joint trial of the technology, which resulted in a request to purchase 20 tools.
- Funded development of an advanced Root-Kit Detection Tool. Root kits are malicious software programs that are designed to take control of a computer's operating system at the administrator, or root, level, where they can often hide from detection by standard anti-malware software. A number of high-security government agencies, including the Defense Advanced Research Projects Agency, the U.S. Navy, DHS, and DOD, are currently using this product.
- Worked with stakeholders to develop a multi-band radio for first responders that allows better communication regardless of the band on which they operate.



2. Investments in Human Capital

Investments in human capital include expenses incurred for programs to educate and train first responders. These programs are intended to increase or maintain national productive capacity as evidenced by outputs and outcomes. Based on a review of the Department's programs, FEMA, S&T, and TSA have made significant investments in human capital.

FEMA

FEMA has invested resources in education, training, and professional development in the following areas:

- FEMA developed the National Fire Academy to promote the professional development of the fire and emergency response community and its allied professionals. The National Fire Academy also develops and delivers educational and training courses with a national focus to supplement and support state and local fire service training programs.
- The Emergency Management Institute (EMI) serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of federal, state, local, and tribal government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters on the American public. EMI curricula are structured to meet the needs of this diverse audience, with an emphasis on how the various elements work together in emergencies to save lives and protect property.
- The Center for Domestic Preparedness (CDP) is a federal training center that specializes in providing advanced hands-on, all-hazards training for emergency responders. Its purpose is the “preparation of first responders by building, sustaining, and improving their capability to respond to all hazards.” The CDP offers training to America’s federal, state, local, tribal, and private emergency responders—to include responders working in rural jurisdictions—in their missions to prevent, deter, respond to, and recover from terrorist acts, especially those involving weapons of mass destruction or hazardous materials. The CDP’s training programs offer a selection of 43 courses and a fully certified, multi-disciplined instructional staff with an average of 19 years of experience in their respective emergency response fields. The CDP is the only congressionally chartered Weapons of Mass Destruction training center for civilians.

S&T

S&T provides grants to institutions, colleges, and universities through its Homeland Security Science, Technology, Engineering and Mathematics (HS-STEM) Career Development Grants Program. Funding can be used to award scholarships and fellowships to students in HS-STEM disciplines. Awards are also granted for Minority Serving Institute (MSI), Scientific Leadership Awards (SLA), and institutional awards to support the development of HS-STEM teaching initiatives, curriculum development, and scholarships in HS-STEM fields.

TSA

TSA’s Highway Watch Cooperative Agreement with the American Trucking Association (ATA) expanded ATA’s Highway Watch program, which taught highway professionals to identify and



report safety and security situations on our Nation's roads. The program provided training and communications infrastructure to prepare 400,000 transportation professionals to respond in the event they or their cargo are the target of a terrorist attack and to share valuable intelligence with TSA if they witness potential threats. The intelligence allows federal agencies and industry stakeholders to quickly move to prevent an attack or to immediately respond if an attack occurs.

3. Investments in Non-Federal Physical Property

Investments in non-federal physical property are expenses included in the calculation of net cost incurred by the reporting entity for the purchase, construction, or major renovation of physical property owned by state and local governments. TSA has made significant investments in non-federal physical property.

TSA

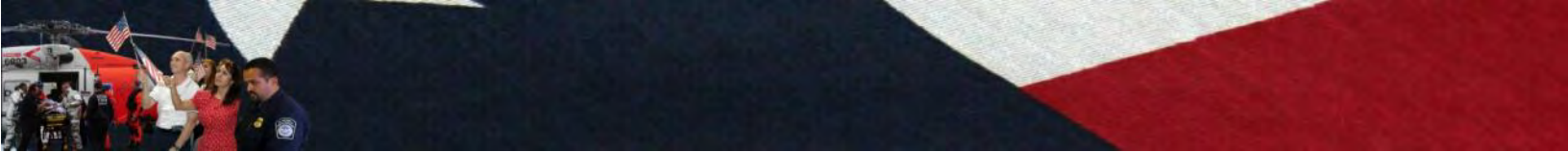
Airport Improvement Program. To help facilitate Explosive Detection System (EDS) installations, TSA purchases and installs in-line EDS equipment through a variety of funding mechanisms, including congressionally authorized letters of intent (LOI). Since the modifications tend to be costly, the LOI is used to offset the costs incurred by commercial service airports for the modifications. TSA has issued 12 LOIs for 12 agreements to provide for the facility modifications necessary to accommodate in-line EDS screening solutions.

Airport Renovation Program. Under this program, TSA employs other transaction agreements (OTAs) to fund the installation of integrated and non-integrated EDS and explosive trace detection equipment as well as improvements to be made to the existing systems in the baggage handling area. These OTAs establish the respective cost-sharing obligations and other responsibilities of TSA and the specific entity (board, port, or authority) conducting the installations or improvements. All work will be completed in order to achieve compliance with the *Aviation and Transportation Security Act (ATSA)*, (Pub. L. 107-71), November 19, 2001.

American Recovery and Reinvestment Act. TSA entered into OTAs with 36 airports. These agreements are funded by the *American Recovery and Reinvestment Act*. TSA obligated \$629 million: \$568 million for the electronic baggage screening program and \$62 million for closed circuit television cameras.

Intercity Bus Security Program. This program provided funds to improve security for intercity bus operators and passengers. DHS awarded grants based on the following program categories:

- Vehicle-specific security enhancements to protect or isolate the driver, such as alarms and security mirrors.
- Monitoring, tracking, and communication technologies for over-the-road buses.
- Implementation and operation of passenger and baggage screening programs at terminals and over-the-road buses.
- Development of an effective security assessment/security plan that identifies critical security needs and vulnerabilities.
- Training for drivers, dispatchers, ticket agents, and other personnel in recognizing and responding to criminal attacks and terrorist threats, evacuation procedures, passenger screening procedures, and baggage inspection.



Required Supplementary Information

Unaudited, see accompanying Auditors' Report

1. *Deferred Maintenance*

The Department Components use condition assessment to determine the deferred maintenance for each class of asset. The procedure includes reviewing equipment, building, and other structure logistic reports. Component logistic personnel identify maintenance not performed as scheduled and establish future performance dates. Logistic personnel use a condition assessment survey to determine the status of referenced assets according to the range of conditions shown below.

Good. Facility/equipment condition meets established maintenance standards, operates efficiently, and has a normal life expectancy. Scheduled maintenance should be sufficient to maintain the current condition. There is no deferred maintenance on buildings or equipment in good condition.

Fair. Facility/equipment condition meets minimum standards but requires additional maintenance or repair to prevent further deterioration, to increase operating efficiency, and to achieve normal life expectancy.

Poor. Facility/equipment does not meet most maintenance standards and requires frequent repairs to prevent accelerated deterioration and to provide a minimal level of operating function. In some cases, this includes condemned or failed facilities.

Based on periodic condition assessments, an indicator of condition is the percentage of facilities and items of equipment in each of the good, fair, or poor categories.

Deferred maintenance as of September 30, 2011, on general PP&E and heritage assets was estimated to range from \$832 million to \$1,113 million, and the condition of these assets ranges from poor to good. These amounts represent maintenance on vehicles, vessels, and buildings and structures owned by the Department that was not performed when it should have been, or was scheduled to be performed but was delayed for a future period.

In FY 2010, the Department reported estimated deferred maintenance ranging from \$995 million to \$1,222 million on general PP&E and heritage assets with a range of poor to good condition. These amounts represent maintenance on vehicles, vessels, and buildings and structures owned by the Department that was not performed when it should have been or was scheduled to be performed but was delayed for a future period.



A summary of deferred maintenance, by asset class, at September 30, 2011, follows (in millions):

	Low estimate	High estimate	Asset Condition
Building & Structures	\$743	\$980	Good to Poor
Equipment (vehicles and vessels)	59	72	Good to Fair
Equipment (Other)	28	35	Good to Fair
Heritage assets	2	26	Good to Poor
Total	\$832	\$1,113	

2. Statement of Budgetary Resources

The principal Statement of Budgetary Resources combines the availability, status, and outlays of the Department's budgetary resources during FY 2011 and FY 2010. Presented on the following pages is the disaggregation of this combined information by DHS Components, which represent the responsibility segments that carry out the Department's missions.

2. Statement of Budgetary Resources

Schedule of FY 2011 Budgetary Resources by Responsibility Segments (in millions) (page 1 of 2)

	CBP	USCG	USCIS	FEMA	FLETC	ICE	OHA	DeptOps	NPPD	USSS	S&T	TSA	TOTAL
BUDGETARY RESOURCES													
Unobligated Balance, Brought Forward, October 1	\$2,647	\$2,407	\$1,010	\$5,581	\$135	\$752	\$20	\$272	\$494	\$136	\$160	\$1,574	\$15,188
Recoveries of Prior Year Obligations	607	448	132	2,678	11	247	5	87	123	9	38	142	4,527
Budget Authority:													
Appropriations	12,424	10,383	2,767	7,224	271	5,798	140	1,631	1,219	1,764	829	5,660	50,110
Spending Authority from Offsetting Collections:													
Earned:													
Collected	1,465	521	28	3,953	125	173	36	710	1,126	30	152	2,056	10,375
Change in Receivable from Federal Sources	1	(10)	4	(34)	5	(16)	2	48	(4)	(4)	13	-	5
Change in Unfilled Customer Orders:													
Advance Received	(1)	(19)	(1)	37	-	-	-	(42)	1	-	(6)	3	(28)
Without Advance from Federal Sources	(10)	(10)	(4)	(335)	(13)	26	(5)	203	(95)	1	47	(1)	(196)
Previously Unavailable	-	2	-	33	-	-	-	-	-	-	-	-	35
Expenditure Transfers from Trust Funds	3	45	-	-	-	-	-	-	-	-	-	-	48
Subtotal	13,882	10,912	2,794	10,878	388	5,981	173	2,550	2,247	1,791	1,035	7,718	60,349
Nonexpenditure Transfers, Net; Anticipated and Actual	320	171	2	(16)	-	(6)	-	26	(2)	13	-	2	510
Temporarily Not Available Pursuant to Public Law	(3)	-	-	(37)	-	-	-	-	-	-	-	(1)	(41)
Permanently Not Available	(457)	(153)	(39)	(1,020)	(8)	(158)	(1)	(33)	(100)	(26)	(68)	(46)	(2,109)
TOTAL BUDGETARY RESOURCES	\$16,996	\$13,785	\$3,899	\$18,064	\$526	\$6,816	\$197	\$2,902	\$2,762	\$1,923	\$1,165	\$9,389	\$78,424
STATUS OF BUDGETARY RESOURCES													
Obligations Incurred:													
Direct	13,240	11,268	2,767	14,296	300	5,940	133	1,743	1,409	1,832	907	7,833	61,668
Reimbursable	1,488	602	21	152	126	177	36	903	1,131	26	200	8	4,870
Subtotal	14,728	11,870	2,788	14,448	426	6,117	169	2,646	2,540	1,858	1,107	7,841	66,538
Unobligated Balance:													
Apportioned	3	1,602	333	2,848	31	152	21	164	140	17	53	1,303	6,667
Exempt from Apportionment	-	2	-	4	-	-	-	-	-	-	-	-	6
Subtotal	3	1,604	333	2,852	31	152	21	164	140	17	53	1,303	6,673
Unobligated Balance Not Available	2,265	311	778	764	69	547	7	92	82	48	5	245	5,213
TOTAL STATUS OF BUDGETARY RESOURCES	\$16,996	\$13,785	\$3,899	\$18,064	\$526	\$6,816	\$197	\$2,902	\$2,762	\$1,923	\$1,165	\$9,389	\$78,424



Schedule of FY 2011 Budgetary Resources by Responsibility Segments (in millions) (page 2 of 2)

	CBP	USCG	USCIS	FEMA	FLETC	ICE	OHA	DeptOps	NPPD	USSS	S&T	TSA	TOTAL
CHANGE IN OBLIGATED BALANCES													
Obligated Balance, Net													
Unpaid Obligations Brought Forward, October 1	\$5,062	\$4,671	\$966	\$26,407	\$202	\$2,065	\$440	\$1,963	\$1,640	\$361	\$1,164	\$3,961	\$48,902
Uncollected Customer Payments from Federal Sources, Brought Forward, October 1	(172)	(386)	(9)	(945)	(127)	(95)	(10)	(455)	(257)	(22)	(161)	(5)	(2,644)
Total Unpaid Obligated Balance, Net	4,890	4,285	957	25,462	75	1,970	430	1,508	1,383	339	1,003	3,956	46,258
Obligations Incurred, Net	14,728	11,870	2,788	14,448	426	6,117	169	2,646	2,540	1,858	1,107	7,841	66,538
Gross Outlays	(14,470)	(11,058)	(2,604)	(13,608)	(442)	(5,938)	(262)	(2,388)	(2,491)	(1,812)	(1,143)	(7,385)	(63,601)
Obligated Balance Transferred, Net				(22)									(22)
Recoveries of Prior Year Unpaid Obligations	(607)	(448)	(132)	(2,678)	(11)	(247)	(5)	(87)	(123)	(9)	(38)	(142)	(4,527)
Change in Uncollected Customer Payments from Federal Sources	8	20	(1)	369	9	(10)	3	(250)	99	3	(60)	1	191
Obligated Balance, Net End of Period													
Unpaid Obligations	4,713	5,036	1,018	24,547	175	1,997	342	2,134	1,565	399	1,089	4,275	47,290
Uncollected Customer Payments from Federal Sources	(164)	(367)	(10)	(576)	(118)	(105)	(7)	(705)	(157)	(20)	(220)	(4)	(2,453)
Total, Unpaid Obligated Balance, Net, End of Period	4,549	4,669	1,008	23,971	57	1,892	335	1,429	1,408	379	869	4,271	44,837
NET OUTLAYS													
Net Outlays													
Gross Outlays	14,470	11,058	2,604	13,608	442	5,938	262	2,388	2,491	1,812	1,143	7,385	63,601
Offsetting Collections	(1,467)	(547)	(26)	(3,992)	(125)	(173)	(36)	(668)	(1,127)	(30)	(145)	(2,060)	(10,396)
Distributed Offsetting Receipts	(2,744)	(280)	(2,934)	139	-	(175)	-	(1)	(1)	-	-	(250)	(6,246)
Net Outlays	\$10,259	\$10,231	\$(356)	\$9,755	\$317	\$5,590	\$226	\$1,719	\$1,363	\$1,782	\$998	\$5,075	\$46,959

Schedule of FY 2010 Budgetary Resources by Responsibility Segments (in millions) (page 1 of 2)

	CBP	USCG	USCIS	FEMA	FLETC	ICE	OHA	DeptOps	NPPD	USSS	S&T	TSA	TOTAL
BUDGETARY RESOURCES													
Unobligated Balance, Brought Forward, October 1	\$3,067	\$1,994	\$886	\$4,201	\$155	\$596	\$40	\$340	\$443	\$142	\$171	\$1,348	\$13,383
Recoveries of Prior Year Obligations	458	211	135	2,783	11	359	6	114	115	9	97	165	4,463
Budget Authority:													
Appropriations	12,944	10,353	2,649	12,228	291	5,792	139	1,635	1,318	1,727	1,007	5,769	55,852
Borrowing Authority	-	-	-	-	-	-	-	-	-	-	-	-	-
Spending Authority from Offsetting Collections:													
Earned:													
Collected	1,586	419	32	3,819	134	174	38	652	1,087	15	90	1,900	9,946
Change in Receivable from Federal Sources	(21)	3	(34)	6	(15)	9	-	2	(29)	4	(3)	(1)	(79)
Change in Unfilled Customer Orders:													
Advance Received	1	(14)	1	(285)	-	(1)	-	49	1	-	17	1	(230)
Without Advance from Federal Sources	(7)	205	(3)	24	16	(35)	-	92	16	10	72	(5)	385
Previously Unavailable	-	-	-	30	-	-	-	-	-	-	-	-	30
Expenditure Transfers from Trust Funds	3	45	-	-	-	-	-	-	-	-	-	-	48
Subtotal	14,506	11,011	2,645	15,822	426	5,939	177	2,430	2,393	1,756	1,183	7,664	65,952
Nonexpenditure Transfers, Net; Anticipated and Actual	297	785	7	(15)	-	(1)	(2)	21	(3)	16	-	-	1,105
Temporarily Not Available Pursuant to Public Law	-	-	-	(32)	-	-	-	-	-	-	-	-	(32)
Permanently Not Available	(536)	(303)	(5)	(591)	(5)	(63)	-	(43)	(56)	(28)	(11)	(30)	(1,671)
TOTAL BUDGETARY RESOURCES	\$17,792	\$13,698	\$3,668	\$22,168	\$587	\$6,830	\$221	\$2,862	\$2,892	\$1,895	\$1,440	\$9,147	\$83,200
STATUS OF BUDGETARY RESOURCES													
Obligations Incurred:													
Direct	\$13,554	\$10,871	\$2,637	\$16,368	\$354	\$5,922	\$161	\$1,786	\$1,283	\$1,729	\$1,112	\$7,567	\$63,344
Reimbursable	1,591	419	23	220	98	156	40	805	1,114	29	168	5	4,668
Subtotal	15,145	11,290	2,660	16,588	452	6,078	201	2,591	2,397	1,758	1,280	7,572	68,012
Unobligated Balance:													
Apportioned	64	2,198	372	5,079	108	201	15	199	367	76	154	1,357	10,190
Exempt from Apportionment	-	2	-	3	-	-	-	-	-	-	-	-	5
Subtotal	64	2,200	372	5,082	108	201	15	199	367	76	154	1,357	10,195
Unobligated Balance Not Available	2,583	208	636	498	27	551	5	72	128	61	6	218	4,993
TOTAL STATUS OF BUDGETARY RESOURCES	\$17,792	\$13,698	\$3,668	\$22,168	\$587	\$6,830	\$221	\$2,862	\$2,892	\$1,895	\$1,440	\$9,147	\$83,200



Schedule of FY 2010 Budgetary Resources by Responsibility Segments (in millions) (page 2 of 2)

	CBP	USCG	USCIS	FEMA	FLETC	ICE	OHA	DeptOps	NPPD	USSS	S&T	TSA	TOTAL
CHANGE IN OBLIGATED BALANCES													
Obligated Balance, Net													
Unpaid Obligations brought forward, Oct 1	\$4,568	\$3,985	\$971	\$26,588	\$178	\$2,074	\$491	\$1,820	\$1,542	\$296	\$1,036	\$3,509	\$47,058
Uncollected customer payments from federal sources, brought forward, Oct 1	(200)	(178)	(47)	(915)	(126)	(121)	(9)	(360)	(270)	(8)	(92)	(11)	(2,337)
Total unpaid obligated balance, net	4,368	3,807	924	25,673	52	1,953	482	1,460	1,272	288	944	3,498	44,721
Obligations incurred, net	15,145	11,290	2,660	16,588	452	6,078	201	2,591	2,397	1,758	1,280	7,572	68,012
Gross Outlays	(14,194)	(10,391)	(2,529)	(13,960)	(417)	(5,729)	(247)	(2,334)	(2,183)	(1,685)	(1,056)	(6,955)	(61,680)
Obligated balance transferred, net	-	-	-	26	-	-	-	-	-	-	-	-	26
Recoveries of Prior Year Unpaid Obligations	(458)	(211)	(135)	(2,783)	(11)	(359)	(6)	(114)	(115)	(9)	(97)	(165)	(4,463)
Change in uncollected customer payments from Federal Sources	28	(209)	37	(30)	(1)	26	-	(94)	13	(15)	(68)	7	(306)
Obligated balance, net end of Period													
Unpaid Obligations	5,061	4,672	966	26,407	202	2,064	440	1,963	1,641	360	1,164	3,962	48,902
Uncollected customer payments from Federal Sources	(172)	(386)	(9)	(945)	(127)	(95)	(10)	(454)	(257)	(23)	(161)	(5)	(2,644)
Total, unpaid obligated balance, net, end of period	4,889	4,286	957	25,462	75	1,969	430	1,509	1,384	337	1,003	3,957	46,258
NET OUTLAYS													
Net Outlays													
Gross Outlays	14,194	10,391	2,529	13,960	417	5,729	247	2,334	2,183	1,685	1,056	6,955	61,680
Offsetting collections	(1,591)	(450)	(33)	(3,533)	(134)	(174)	(38)	(701)	(1,088)	(15)	(107)	(1,900)	(9,764)
Distributed offsetting receipts	(2,467)	(488)	(2,777)	(175)	-	(168)	-	(2)	1	-	-	(252)	(6,328)
Net Outlays	\$10,136	\$9,453	\$(281)	\$10,252	\$283	\$5,387	\$209	\$1,631	\$1,096	\$1,670	\$949	\$4,803	\$45,588



3. Statement of Custodial Activity

Substantially all duty, tax, and fee revenues collected by CBP are remitted to various General Fund accounts maintained by Treasury and the U.S. Department of Agriculture. Treasury further distributes these revenues to other federal agencies in accordance with various laws and regulations. CBP either transfers the remaining revenue (generally less than one percent of revenues collected) directly to other federal agencies or the Governments of Puerto Rico and the U.S. Virgin Islands. Refunds of revenues collected from import/export activities are recorded in separate accounts established for this purpose and are funded through permanent indefinite appropriations. These activities reflect the non-entity, or custodial, responsibilities that CBP, as an agency of the Federal Government, has been authorized by law to enforce.

CBP reviews selected documents to ensure all duties, taxes, and fees owed to the Federal Government are paid and to ensure all regulations are followed. If CBP determines duties, taxes, fees, fines, or penalties are due in addition to estimated amounts previously paid by the importer/violator, the importer/violator is notified of the additional amount due. CBP regulations allow the importer/violator to file a protest on the additional amount due for review by the Port Director. A protest allows the importer/violator the opportunity to submit additional documentation supporting the claim of a lower amount due or to cancel the additional amount due in its entirety. During this protest period, CBP does not have a legal right to the importer/violator's assets, and consequently CBP recognizes accounts receivable only when the protest period has expired or an agreement is reached. For FY 2011 and FY 2010, CBP had the legal right to collect \$2.7 billion and \$2.5 billion of receivables, respectively. In addition, there were \$2.3 billion and \$2.4 billion representing records still in the protest phase for FY 2011 and FY 2010, respectively. CBP recognized as write-offs \$109 million and \$43 million, respectively, of assessments that the Department had statutory authority to collect at September 30, 2011 and 2010, but have no future collection potential. Most of this amount represents fines, penalties, and interest.

4. Risk Assumed Information

The Department has performed an analysis of the contingencies associated with the unearned premium reserve for the NFIP. This FY 2011 estimate represents losses that might occur in FY 2012 on policies that were in-force as of September 30, 2011. The calculation utilizes the current estimate of the long-term average loss year, which includes an estimate of a rare but catastrophic loss year. A large portion of the long-term average loss year is derived from those catastrophic years.

The NFIP subsidizes rates for some classes of policyholders. These subsidized rates produce a premium less than the loss and loss adjustment expenses expected to be incurred during the long-term average loss year described above. Accordingly, there is a risk that paid flood losses during the remainder of the term for those subsidized policies will exceed the unearned premium liability.

The underlying calculation estimates the amount of subsidy in the total rates, removes the expense load, and applies the results to the unearned premium reserve. A range is developed and applied to the results of the calculation of unpaid expected losses by \$525 to \$575 million.



Actual flood losses are highly variable from year to year. For the majority of years, the unearned premium reserve for the NFIP is adequate to pay the losses and expenses associated with the unearned premium. In those years with catastrophic flooding, the reserve and the average across all years will be inadequate because of the subsidies in premium levels.



Independent Auditors' Report

Office of Inspector General

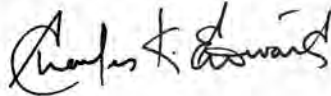
U.S. Department of
Homeland Security
Washington, DC 20528



Homeland Security

NOV 11 2011

MEMORANDUM FOR: The Honorable Janet Napolitano
Secretary

FROM: Charles K. Edwards 
Acting Inspector General

SUBJECT: *Independent Auditors' Report on DHS' FY 2011 Financial
Statements and Internal Control over Financial Reporting*

The attached report presents the results of the U.S. Department of Homeland Security's (DHS) financial statement audit for fiscal year (FY) 2011 and the results of an examination of internal control over financial reporting of the balance sheet as of September 30, 2011, and the statement of custodial activity for FY 2011. These are mandatory audits required by the *Chief Financial Officers Act of 1990*, as amended by the *Department of Homeland Security Financial Accountability Act of 2004*. This report is incorporated in the Department's FY 2011 *Annual Financial Report*. We contracted with the independent public accounting firm KPMG LLP (KPMG) to perform the integrated audit.

The Department continued to improve financial management in FY 2011 and has achieved a significant milestone. For the first time, the Department was able to produce an auditable balance sheet and statement of custodial activity; and the independent auditors rendered a qualified opinion on those financial statements. Nevertheless, the Department still has much work to do. KPMG was unable to perform procedures necessary to form an opinion on DHS' internal control over financial reporting of the FY 2011 balance sheet and statement of custodial activity. In order to sustain or improve upon the qualified opinion, the Department must continue remediating the remaining control deficiencies. Additionally, as the Department moves to achieve an opinion on the full set of financial statements, more challenges may arise.

Summary

KPMG expressed a qualified opinion on the Department's balance sheet as of September 30, 2011, and the related statements of custodial activity for FY 2011. DHS was unable to represent that property, plant, and equipment (PP&E), and environmental liabilities account balances were correct and was unable to provide sufficient evidence to support these balances in the financial statements. Additionally, KPMG was unable to perform the examination procedures necessary to form an opinion on DHS' internal control over financial reporting of the balance sheet as of September 30, 2011, and the statement of custodial activity for FY 2011.



The report discusses nine significant deficiencies in internal control, five of which are considered material weaknesses, and six instances of noncompliance with laws and regulations, as follows:

Significant Deficiencies That Are Considered To Be Material Weaknesses

- Financial Reporting
- Information Technology Controls and System Functionality
- Property, Plant, and Equipment
- Environmental and Other Liabilities
- Budgetary Accounting

Other Significant Deficiencies

- Entity-Level Controls
- Fund Balance with Treasury
- Grants Management
- Custodial Revenue and Drawback

Non-compliance with Laws and Regulations

- *Federal Managers' Financial Integrity Act of 1982 (FMFIA)*,
- *Federal Financial Management Improvement Act of 1996 (FFMIA)*
- *Single Audit Act Amendments of 1996*
- *Chief Financial Officers Act of 1990*
- *Anti-deficiency Act (ADA)*
- *Government Performance and Results Act of 1993*

Moving DHS' Financial Management Forward

Although the Department continued to remediate material weaknesses and reduce the number of conditions contributing to the material weaknesses, five of the six material weakness conditions identified in FY 2010 were repeated in FY 2011. DHS made some progress in remediating two of the material weaknesses. Specifically, DHS corrected the weakness conditions related to financial management, but not the deficiencies related to financial reporting; hence, financial management and reporting was reduced to financial reporting. Additionally, the auditors noted improvement in internal controls over actuarial liabilities, primarily because the U.S. Coast Guard (USCG) was able to assert to over \$40 billion of actuarial liabilities. However, USCG continues to have significant challenges in Environmental and Other Liabilities, which caused a material weakness in this area for the Department during FY 2011. Further, as in previous years, the DHS Secretary has issued a statement of no assurance on the Department's internal controls over financial reporting, due to the existence of a pervasive material weakness, and limits on the scope of DHS' self assessment while focusing on remediation of control deficiencies. Consequently, the



independent auditors were unable to render an opinion on DHS' internal controls over financial reporting in FY 2011.

KPMG is responsible for the attached Independent Auditor's Report dated November 11, 2011, and the conclusions expressed in the report. We do not express opinions on financial statements or internal control or conclusions on compliance with laws and regulations.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of this report to appropriate congressional committees with oversight and appropriation responsibilities over the Department. In addition, we will post a copy of the report on our public website.

We request that the Office of the Chief Financial Officer provide us with a corrective action plan that demonstrates progress in addressing the report's recommendations.

We appreciate the cooperation extended to the auditors by the Department's financial offices. Should you have any questions, please call me, or your staff may contact Anne L. Richards, Assistant Inspector General for Audits, at 202-254-4100.

Attachment



Department of Homeland Security **Office of Inspector General**

Independent Auditors' Report on DHS' FY 2011 Financial Statements and Internal Control over Financial Reporting



OIG-12-07

November 2011



Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

NOV 11 2011



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The attached report presents the results of the DHS financial statements audit for fiscal year (FY) 2011 and the results of an examination of internal control over financial reporting of the balance sheet as of September 30, 2011, and the statement of custodial activity for FY 2011. We contracted with the independent public accounting firm KPMG LLP (KPMG) to perform the audits. The contract required that KPMG perform its audits according to generally accepted government auditing standards and guidance from the Office of Management and Budget and the Government Accountability Office. KPMG expressed a qualified opinion on DHS' balance sheet as of September 30, 2011, and the statement of custodial activity for FY 2011. However, KPMG was unable to complete procedures necessary to form an opinion on DHS' internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for FY 2011. The report discusses nine significant deficiencies in internal control, of which five are considered material weaknesses, and six instances of noncompliance with laws and regulations. KPMG is responsible for the attached report and the conclusions expressed in the report. We do not express opinions on DHS' financial statements or provide conclusions on compliance with laws and regulations.

The recommendations herein have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Charles K. Edwards
Acting Inspector General



U.S. DEPARTMENT OF HOMELAND SECURITY

Excerpts from the DHS Annual Financial Report

Table of Contents

<u>Description</u>	<u>Page Number</u>
Independent Auditors' Report.....	1-6
Introduction to Exhibits on Internal Control and Compliance and Other Matters.....	i. 1-2
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard	I.1-8
Exhibit II – Material Weaknesses – DHS Civilian Components.....	II.1-9
Exhibit III – Significant Deficiencies – All DHS Components.....	III.1-6
Exhibit IV – Compliance and Other Matters – All DHS Components.....	IV.1-3
Exhibit V – Status of Prior Year Findings.....	V.1-3
Criteria – Index of Financial Reporting and Internal Control Criteria.....	Index.1-4
Management Response.....	Appendix A
Report Distribution.....	Appendix B



KPMG LLP
2001 M Street, NW
Washington, DC 20036

INDEPENDENT AUDITORS' REPORT

Secretary and Inspector General
U.S. Department of Homeland Security:

We have audited the accompanying balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2011 and the related statement of custodial activity for the year then ended (referred to herein as the "fiscal year (FY) 2011 financial statements"). The objective of our audit was to express an opinion on the fair presentation of these financial statements. We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended. In connection with our audit, we also considered DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the FY 2011 financial statements.

We were also engaged to audit the accompanying balance sheet of the DHS as of September 30, 2010 and the related statement of custodial activity for the year then ended (referred to herein as the "FY 2010 financial statements"). We were not engaged to audit the accompanying statements of net cost, changes in net position, and budgetary resources, for the years ended September 30, 2011 and 2010 (referred to herein as "other FY 2011 and 2010 financial statements"), or to examine internal control over financial reporting over the other FY 2011 financial statements.

Summary

Except as discussed in our Report on the Financial Statements, we concluded that the balance sheet as of September 30, 2011 and the related statement of custodial activity for the year ended, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles. The scope of our work was not sufficient to express an opinion on the DHS balance sheet as of September 30, 2010 or the related statement of custodial activity for the year then ended.

As discussed in note 15 of the FY 2011 financial statements, the Department has intergovernmental debt of approximately \$17.8 billion used to finance the *National Flood Insurance Program* (NFIP). Due to the subsidized nature of the NFIP, the Department has determined that future insurance premiums and other anticipated sources of revenue may not be sufficient to repay this debt. The financial statements do not include any adjustments that might result from the outcome of this uncertainty.

As stated in our Report on Internal Control over Financial Reporting, we were unable to perform procedures necessary to form an opinion on DHS' internal control over financial reporting of the balance sheet as of September 30, 2011 and the related statement of custodial activity for the year then ended.

Material weaknesses in internal control over financial reporting, as defined in the Report on Internal Control over Financial Reporting section of this report, have been identified in the following areas:

- Financial Reporting
- Information Technology Controls and Financial System Functionality
- Property, Plant, and Equipment
- Environmental and Other Liabilities
- Budgetary Accounting

Significant deficiencies, as defined in the Report on Internal Control over Financial Reporting section of this report, have been identified in the following areas:

- Entity-Level Controls
- Fund Balance with Treasury
- Grants Management



- Custodial Revenue and Drawback

The results of our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements disclosed the following instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended:

- *Federal Managers' Financial Integrity Act of 1982*
- *Federal Financial Management Improvement Act of 1996*
- *Single Audit Act Amendments of 1996*
- *Chief Financial Officers Act of 1990*
- *Anti-deficiency Act*
- *Government Performance and Results Act of 1993*

We also reported other matters related to compliance with the *Anti-deficiency Act* at the National Protection and Programs Directorate (NPPD), U.S. Coast Guard (Coast Guard), and the Management Directorate.

The following sections discuss our opinion on the accompanying DHS FY 2011 financial statements; why we are unable to express an opinion on the DHS FY 2010 financial statements; why we were unable to express an opinion on internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended; our tests of DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements and other matters, and management's and our responsibilities.

Report on the Financial Statements

We have audited the accompanying balance sheet of the U.S. Department of Homeland Security as of September 30, 2011, and the related statements of custodial activity for the year then ended. We were also engaged to audit the accompanying balance sheet of the DHS as of September 30, 2010 and the related statement of custodial activity for the year then ended.

The Coast Guard has adopted a multi-year plan to reconcile its balance sheet accounts, obtain sufficient evidential matter that support historical transactions, and prepare auditable financial statements. Pursuant to this plan, the Coast Guard did not assert to the reliability of general property, plant, and equipment including heritage and stewardship assets, environmental liabilities, and the related effects, if any, on other balances presented in the accompanying balance sheet at September 30, 2011. Coast Guard general property, plant, and equipment including heritage and stewardship assets, and environmental liabilities as reported in the accompanying FY 2011 financial statements were \$9.9 billion and \$973 million, respectively as of September 30, 2011. It was not practicable to extend our auditing procedures sufficiently to satisfy ourselves as to the fairness of these balances.

In our opinion, except for the effects on the FY 2011 financial statements of such adjustments, if any, as might have been determined to be necessary had we been able to apply adequate procedures to general property, plant, and equipment including heritage and stewardship assets, environmental liabilities, and related other balances presented in the accompanying balance sheet at September 30, 2011, as discussed in the preceding paragraph, the FY 2011 financial statements referred to above present fairly, in all material respects, the financial position of DHS as of September 30, 2011 and its custodial activity for the year then ended, in conformity with U.S. generally accepted accounting principles.

In FY 2010, the Coast Guard was unable to provide sufficient evidential matter that support transactions and certain balance sheet accounts including fund balance with Treasury, accounts receivable, inventory and related property, general property, plant and equipment including heritage and stewardship assets, certain actuarially-derived liabilities, environmental and other liabilities, and net position, as reported in the accompanying DHS balance sheet as of September 30, 2010. It was impractical to extend our procedures sufficiently to determine the extent, if any, to which the DHS balance sheet as of September 30, 2010, and the related statement of custodial activity for the year then ended, may have been affected by the matters discussed in this paragraph. Accordingly, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on the FY 2010 financial statements and the related notes thereto. The total assets and liabilities of the Coast Guard, as reported in



the accompanying DHS FY 2010 financial statements were \$20.3 billion or 23 percent of total DHS consolidated assets, and were \$46.4 billion or 56 percent of total DHS consolidated liabilities as of September 30, 2010.

We were not engaged to audit the accompanying statements of net cost, changes in net position, and budgetary resources for the years ended September 30, 2011 and 2010, and accordingly, we do not express an opinion on these other FY 2011 and 2010 financial statements.

As discussed in note 15 of the FY 2011 financial statements, the Department has intergovernmental debt of approximately \$17.8 billion used to finance the *National Flood Insurance Program*. Due to the subsidized nature of the NFIP, the Department has determined that future insurance premiums, and other anticipated sources of revenue, may not be sufficient to repay this debt. The financial statements do not include any adjustments that might result from the outcome of this uncertainty.

As discussed in Note 24, DHS did not present the Statements of Net Cost as of September 30, 2011 and 2010 by major program, goals and outputs as described in a strategic and performance plan, and also omitted certain related financial statement disclosures, required by OMB Circular No. A-136, *Financial Reporting Requirements*, as amended.

The information in the Management's Discussion and Analysis (MD&A), Required Supplementary Stewardship Information (RSSI), and Required Supplementary Information (RSI) sections of the DHS FY 2011 Annual Financial Report (AFR) is not a required part of the financial statements, but is supplementary information required by U.S. generally accepted accounting principles. We were unable to complete limited procedures over MD&A, RSSI, and RSI as prescribed by professional standards because of the limitations on the scope of our audit described in the second and fourth paragraphs of this section of our report. Certain information presented in the MD&A, RSSI, and RSI is based on other FY 2011 and 2010 financial statements on which we have not expressed an opinion. We did not audit the MD&A, RSSI, and RSI, and accordingly, we express no opinion on it. However, we noted that DHS did not include summary performance information that is aligned with approved and adopted strategic goals within the MD&A section of the FY 2011 AFR, as required by OMB Circular No. A-136, *Financial Reporting Requirements*, as amended. DHS recently completed a quadrennial review for the purpose of developing an updated strategic plan around new priorities established by the Secretary.

The information in the Other Accompanying Information section of DHS' FY 2011 AFR is presented for purposes of additional analysis, and is not a required part of the financial statements. This information has not been subjected to auditing procedures, and accordingly, we express no opinion on it.

Report on Internal Control over Financial Reporting

We were engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended, based on the criteria established in OMB Circular No. A-123, *Management's Responsibility for Internal Control* (OMB Circular No. A-123), Appendix A. DHS management is responsible for establishing and maintaining effective internal control over financial reporting, and for its assertion on the effectiveness of internal control over financial reporting, included in the FY 2011 DHS *Secretary's Assurance Statement*, included in MD&A on page 34 of the DHS FY 2011 AFR, as required by OMB Circular No. A-123. We did not test all controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*.

The FY 2011 DHS *Secretary's Assurance Statement* states that the Department was unable to provide assurance that internal control over financial reporting was operating effectively at September 30, 2011. This conclusion is based on the Department's evaluation and analysis of control deficiencies at the Coast Guard, Transportation Security Administration, Federal Emergency Management Agency, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and other components that in combination represent Departmental material weaknesses. In addition, management acknowledges that pervasive material weaknesses exist in key financial processes, and has devoted attention on remediation of those material weaknesses during FY 2011. Management is therefore unable to make an assertion on the effectiveness of internal control over financial reporting in key financial statement processes.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that



controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. Material weaknesses in internal control over financial reporting have been identified in the following areas:

- Financial Reporting
- Information Technology Controls and Financial Systems Functionality
- Property, Plant, and Equipment
- Environmental and Other Liabilities
- Budgetary Accounting

Deficiencies at the Coast Guard that contribute to a material weakness at the consolidated level, when aggregated with deficiencies existing at other components, are presented in Exhibit I. Deficiencies at other DHS components that contribute to a material weakness at the consolidated level, when aggregated with deficiencies existing at the Coast Guard, are presented in Exhibit II.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. Our consideration of internal control was for the purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in DHS' internal control that might be significant deficiencies. However, in accordance with *Government Auditing Standards*, we are required to report significant deficiencies in internal control identified during our examination. Significant deficiencies have been identified in the following areas:

- Entity-Level Controls
- Fund Balance with Treasury
- Grants Management
- Custodial Revenue and Drawback

Deficiencies in all components that contribute to a significant deficiency at the consolidated level, when aggregated, are presented in Exhibit III.

Because of the limitation on the scope of our audit described in the second paragraph of the Report on the Financial Statements section, and the nature of management's assertion on the effectiveness of internal control over financial reporting described in the second paragraph of the Report on Internal Control over Financial Reporting section, the scope of our examination was not sufficient to enable us to express, and we do not express an opinion on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2011, and related statement of custodial activity for the year then ended. It was impractical to extend our procedures sufficiently to determine the extent, if any, to which the FY 2011 financial statements may have been affected by these circumstances.

We were not engaged to examine internal controls over financial reporting of the accompanying statements of net cost, changes in net position, and budgetary resources, for the year ended September 30, 2011. Other deficiencies in internal control, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported had we been able to apply sufficient audit procedures to property, plant, and equipment including heritage and stewardship assets, and environmental liabilities balances, as described in the second paragraph of our Report on the Financial Statements; had we been able to perform all procedures necessary to express an opinion on DHS' internal control over financial reporting of the FY 2011 financial statements; and had we been engaged to audit the other FY 2011 and 2010 financial statements and to examine internal control over financial reporting of the other FY 2011 financial statements.

A summary of the status of FY 2010 material weaknesses and significant deficiencies is included as Exhibit V. We also noted certain additional deficiencies involving internal control over financial reporting and its operation that we will report to the management of DHS in a separate letter.



Report on Compliance and Other Matters

The results of certain of our tests of compliance as described in the Responsibilities section of this report, exclusive of those referred to in the *Federal Financial Management Improvement Act of 1996* (FFMIA), disclosed the following six instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 07-04, and are described in Exhibit IV:

- *Federal Managers' Financial Integrity Act of 1982*
- *Federal Financial Management Improvement Act of 1996*
- *Single Audit Act Amendments of 1996*
- *Chief Financial Officers Act of 1990*
- *Anti-deficiency Act*
- *Government Performance and Results Act of 1993*

The results of our other tests of compliance as described in the Responsibilities section of this report, exclusive of those referred to in FFMIA, disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 07-04.

The results of our tests of FFMIA disclosed instances described in Exhibits I, II, and III where DHS' financial management systems did not substantially comply with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level.

Other instances of noncompliance with laws, regulations, contracts, and grant agreements may have been identified and reported, had we been able to apply sufficient audit procedures to property, plant, and equipment including heritage and stewardship assets, and environmental liabilities balances as described in the second paragraph of our Report on the Financial Statements; perform all procedures necessary to complete our examination of internal control over financial reporting of the balance sheet as of September 30, 2011 and the related statements of custodial activity for the year then ended; and had we been engaged to audit the other FY 2011 financial statements and to examine internal control over financial reporting over the other FY 2011 financial statements.

Other Matters: Management of the NPPD, Coast Guard, and Management Directorate have initiated reviews of certain collections, classification and use of funds, expenditures and/or obligations recorded that may identify a violation of the *Anti-deficiency Act*, or other violations of appropriation law in FY 2011 or in previous years.

Responsibilities

Management's Responsibilities. Management is responsible for the financial statements; establishing and maintaining effective internal control; and complying with laws, regulations, contracts, and grant agreements applicable to DHS.

Auditors' Responsibilities. Our responsibility is to express an opinion on the FY 2011 financial statements of DHS based on our audit. Except as discussed in the second paragraph of our Report on Financial Statements above, we conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin No. 07-04. Those standards and OMB Bulletin No. 07-04 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit also includes:

- Examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements;
- Assessing the accounting principles used and significant estimates made by management; and
- Evaluating the overall financial statement presentation.



We believe that our audit provides a reasonable basis for our opinion.

As part of obtaining reasonable assurance about whether DHS' FY 2011 financial statements are free of material misstatement, we performed tests of DHS' compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of the balance sheet amounts as of September 30, 2011, and the related statement of custodial activity for the year then ended, and certain provisions of other laws and regulations specified in OMB Bulletin No. 07-04, including the provisions referred to in Section 803(a) of FFMIA. We limited our tests of compliance to the provisions described in the preceding sentence, and we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to DHS. However, providing an opinion on compliance with laws, regulations, contracts, and grant agreements was not an objective of our audit, and accordingly, we do not express such an opinion.

DHS management has indicated in a separate letter immediately following this report that it concurs with the findings presented in Exhibits I, II, III, and IV of our report. We did not audit DHS' response, and accordingly, we express no opinion on it.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General, OMB, U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 11, 2011



Independent Auditors' Report
Introduction to Exhibits on Internal Control and Compliance and Other Matters

Our report on internal control over financial reporting and compliance and other matters is presented in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. The internal control weaknesses and findings related to compliance with certain laws, regulations, contracts, and grant agreements presented herein were identified during our audit of the U.S. Department of Homeland Security (Department or DHS)'s balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended (financial statements), and to examine internal control over financial reporting of those financial statements. We were not engaged to audit the Department's fiscal year (FY) 2011 statements of net cost, changes in net position, and budgetary resources (referred to as other FY 2011 financial statements), or to examine internal controls over financial reporting of the other FY 2011 financial statements. Our findings and the status of prior year findings are presented in five exhibits:

- Exhibit I** Significant deficiencies in internal control identified at the United States Coast Guard (Coast Guard). All of the significant deficiencies reported in Exhibit I are considered material weaknesses at the DHS consolidated level, when combined with other significant deficiencies reported in Exhibit II.
- Exhibit II** Significant deficiencies in internal control identified throughout the Department or at other DHS components (components other than Coast Guard are collectively referred to as DHS Civilian Components). All of the significant deficiencies reported in Exhibit II are considered material weaknesses at the DHS consolidated level, when combined with other significant deficiencies reported in Exhibit I.
- Exhibit III** Significant deficiencies that are not considered a material weakness at the DHS consolidated financial statement level.
- Exhibit IV** Instances of noncompliance with certain laws, regulations, contracts, and grant agreements that are required to be reported under *Government Auditing Standards* or Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.
- Exhibit V** The status of our findings reported in FY 2010.
- Criteria** *Index of Financial Reporting and Internal Control Criteria*

As stated in our Independent Auditors' Report, the scope of our work was not sufficient to enable us to express an opinion on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2011, and related statement of custodial activity for the year then ended. Consequently, additional deficiencies in internal control over financial reporting, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported, had we been able to perform all procedures necessary to express an opinion on DHS' internal control over financial reporting, and had we been engaged to audit the other FY 2011 financial statements, and to examine internal control over financial reporting of the other FY 2011 financial statements.

The determination of which findings rise to the level of a material weakness is based on an evaluation of how deficiencies identified in all components, considered in aggregate, may affect the DHS balance sheet as of September 30, 2011, or the related statement of custodial activity for the year then ended.

We have also performed follow-up procedures on findings identified in previous engagements to audit the DHS financial statements. To provide trend information for the DHS Civilian Components, Exhibits II and III contain Trend Tables next to the heading of each finding. The Trend Tables in Exhibits II and III depict the severity and current status of findings, by component that has contributed to that finding from FY 2009 through FY 2011.

The criteria supporting our findings, such as references from technical accounting standards, various rules and regulations, including requirements issued by the Office of Management and Budget and the U.S. Treasury, and internal Departmental and component directives, is presented in the *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.



Independent Auditors' Report
Introduction to Exhibits on Internal Control and Compliance and Other Matters

A summary of our findings in FY 2011 and FY 2010 are presented in the Tables below:

Table 1 Presents a summary of our internal control findings, by component, for FY 2011.

Table 2 Presents a summary of our internal control findings, by component, for FY 2010.

We have reported five material weaknesses and four significant deficiencies at the Department level in FY 2011, shown in Table 1.

TABLE 1 – SUMMARIZED DHS FY 2011 INTERNAL CONTROL FINDINGS

Comments / Financial Statement Area		DHS Consol.	CG	CBP	USCIS	FEMA	FLETC	ICE	MGMT	TSA
			Military	Civilian						
Material Weakness:			Exhibit I	Exhibit II						
A	Financial Reporting	MW								
B	IT Controls and System Functionality	MW								
C	Property, Plant, and Equipment	MW								
D	Environmental and Other Liabilities	MW								
E	Budgetary Accounting	MW								
Significant Deficiencies:				Exhibit III						
F	Entity-Level Controls	SD								
G	Fund Balance with Treasury	SD								
H	Grants Management	SD								
I	Custodial Revenue and Drawback	SD								

TABLE 2 – SUMMARIZED DHS FY 2010 INTERNAL CONTROL FINDINGS

Comments / Financial Statement Area		DHS Consol.	CG	CBP	USCIS	FEMA	FLETC	ICE	NPPD	TSA
			Military	Civilian						
Material Weakness:			Exhibit I	Exhibit II						
A	Financial Management and Reporting	MW								
B	IT Controls and System Functionality	MW								
C	Fund Balance with Treasury	MW								
D	Property, Plant, and Equipment	MW								
E	Actuarial and Other Liabilities	MW								
F	Budgetary Accounting	MW								
Significant Deficiencies:				Exhibit III						
G	Other Entity-Level Controls	SD								
H	Custodial Revenue and Drawback	SD								

	Control deficiency findings are <i>more significant</i> to the evaluation of effectiveness of controls at the Department-Level
	Control deficiency findings are <i>less significant</i> to the evaluation of effectiveness of controls at the Department-Level
	Material weakness at the Department level exists when all findings are aggregated
	Significant deficiency at the Department level exists when all findings are aggregated

All components of DHS, as defined in Note 1A – *Reporting Entity*, to the financial statements, were included in the scope of our audit of the consolidated balance sheet of DHS as of September 30, 2011, and the related statement of custodial activity for the year then ended, and our engagement to examine internal control over financial reporting of those financial statements. Accordingly, our audit and engagement to examine internal control considered significant account balances, transactions, and accounting processes of other DHS components not listed above. Control deficiencies identified in other DHS components that are not identified in the table above did not individually, or when combined with other component findings, contribute to a material weakness or significant deficiency at the DHS consolidated financial statement level.



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

I-A Financial Reporting

Background: In previous years, we reported that the U.S. Coast Guard (Coast Guard) had several internal control deficiencies that led to a material weakness in financial reporting. In response, the Coast Guard developed its *Financial Strategy for Transformation and Audit Readiness* (FSTAR), which is a comprehensive plan that includes various Mission Action Plans (MAPs) designed to identify and correct conditions that are causing control deficiencies and, in some cases, preventing the Coast Guard from preparing auditable financial statements.

The Coast Guard made progress in fiscal year (FY) 2011, by completing its planned corrective actions over selected internal control deficiencies. Specifically, the Coast Guard implemented new policies and procedures, and automated tools to improve internal controls and the reliability of its financial statements throughout FY 2011. These remediation efforts allowed management to make new assertions in FY 2011 related to the auditability of its financial statement balances, including \$6.3 billion of fund balance with Treasury. The FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012. Consequently, some conditions of the financial reporting control weaknesses that we reported in the past remain uncorrected at September 30, 2011.

Conditions: The Coast Guard does not have properly designed, implemented, and effective policies, procedures, processes, and controls surrounding its financial reporting process, as necessary, to:

- Support beginning balance and year-end close-out related activity, and the cumulative results of operations analysis in its general ledgers individually and/or in the aggregate.
- Ensure that all journal entries and edit queries impacting the general ledger are adequately researched and supported. Specifically, documenting that adequate research regarding the underlying cause(s) was performed, and maintaining the appropriate transactional-level supporting detail.
- Ensure that all accounts receivable balances exist, are complete and accurate, and properly presented in the financial statements. For example, the underlying data used to support accounts receivable balances was not always accurate (e.g., incorrect standard rates applied), reimbursable activity may not be identified and recorded timely due to intra-governmental reconciliation difficulties, and accounts receivable activity is not always properly recorded in the financial statements on a timely basis.
- Ensure all financial statement information (e.g., statement of net cost, statement of budgetary resources, statement of changes in net position) and related disclosures submitted for incorporation in the DHS consolidated financial statements are accurate and complete.
- Ascertain that intra-governmental activities and balances are identified, monitored, properly recorded, and differences, especially with agencies outside DHS, are being resolved in a timely manner in coordination with the Department's Office of Financial Management (OFM).

Cause/Effect: The Coast Guard has not developed and implemented an effective general ledger system. The Core Accounting System (CAS), Aircraft Logistics Management Information System (ALMIS), and Naval Engineering Supply Support System (NESSS) general ledgers do not comply with the requirements of the *Federal Financial Management Improvement Act of 1996* (FFMIA). The general ledgers do not allow for compliance with the United States Standard General Ledger (USSGL) at the transaction level, and period-end and opening balances are not supported by transactional detail in the three general ledgers. The conditions described below in Comment I-B, *Information Technology Controls and Financial Systems Functionality* contribute to the financial reporting control deficiencies, and make correction more difficult. Some remediation initiatives implemented in FY 2011 were not fully implemented for the entire year, and the FSTAR calls for continued remediation in FY 2012.

Because of the conditions noted above, the Coast Guard and the Department were unable to provide reasonable assurance that internal controls over financial reporting were operating effectively at September 30, 2011, and has acknowledged that pervasive material weaknesses and various internal control deficiencies continue to exist in some key financial processes. Consequently, the Coast Guard cannot assert



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

to the reliability of general property, plant, and equipment, environmental liabilities, and their related effects, if any, on other balances presented in the Department's financial statements as of September 30, 2011.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that the Coast Guard:

1. Continue the implementation of the FSTAR and completion of MAPs, as planned;
2. Implement accounting and financial reporting processes including an integrated general ledger system that is FFMIA compliant; and
3. Establish new or improve existing policies, procedures, and related internal controls to ensure that:
 - a. The year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval, and beginning balances in the following year are determined to be reliable and auditable;
 - b. All journal entries and edit queries impacting the general ledger are adequately researched and supported;
 - c. Accounts receivable balances are complete and accurate, and properly presented in the financial statements;
 - d. Financial statement disclosures submitted for incorporation in the Department of Homeland Security (DHS or Department) financial statements are accurate and complete; and
 - e. All intra-governmental activities and balances are reconciled on a timely basis, accurately reflected in the financial statements, and differences are resolved in a timely manner in coordination with the Department's Office of Financial Management (OFM).

I-B Information Technology Controls and Financial Systems Functionality

Background: Information Technology (IT) general and application controls are essential for achieving effective and reliable reporting of financial and performance data. IT general controls (ITGCs) are tested using the objectives defined by the U.S. Government Accountability Office (GAO)'s *Federal Information System Controls Audit Manual* (FISCAM), in five key control areas: security management, access control, configuration management, segregation of duties, and business continuity. Our procedures included a review of the Coast Guard's key ITGC environments.

We also considered the effects of financial systems functionality when testing ITGCs. We noted that financial system limitations contribute to the Coast Guard's challenge of addressing systemic internal control weaknesses, strengthening the control environment, and complying with relevant Federal financial system requirements and guidelines, notably FFMIA, Office of Management and Budget (OMB) Circular A-127, *Financial Management Systems*, and DHS policies.

In FY 2011, our ITGC control testing identified 21 findings, of which 16 were repeat findings from the prior year and 5 were new findings. In addition, we determined that Coast Guard remediated 12 findings identified in previous years. Specifically, the Coast Guard took actions to improve aspects of its IT security controls, including password configurations, data center physical security, and audit log reviews.

Conditions: Our findings related to financial system controls and functionality are as follows:

Related to IT controls:

Conditions: We noted that IT security access controls and configuration management controls supporting Coast Guard's financial systems are not operating effectively, and continue to present risks to DHS financial data confidentiality, integrity, and availability. Financial data in the Coast Guard general ledgers may be compromised by automated and manual changes that are not adequately controlled. For example, the Coast Guard uses an IT scripting process to address functionality and data quality issues within its core



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

financial system, as necessary, to process and report financial data. During our FY 2011 testing, we noted that some previously identified IT scripting control deficiencies were remediated, while other deficiencies continue to exist. Four key areas continue to impact the Coast Guard IT script control environment, as follows:

- Script testing – limited guidance exists to guide Coast Guard staff in the development of test plans and to support the completion of functional testing;
- Script audit logging – controls supporting audit logs are not consistently implemented to log privileged user actions, and to ensure that only approved scripts are executed;
- Script approvals and recertification – the recertification reviews conducted by the Coast Guard were not comprehensive to include all user roles associated with the Mashups and Dimensions systems. Additionally, the documentation retained in support of the reviews was not adequately completed in accordance with policy throughout the year; and
- Script recording – test and production data is not consistently recorded, and there are limited controls to ensure data accuracy. Additionally, field reconciliation discrepancies are not always consistently documented and explained.

We also noted weaknesses in the script change management process as it relates to the Internal Control over Financial Reporting (ICOFR) process (e.g., the financial statement impact of the changes to Coast Guard's core accounting system through the script change management process). The Coast Guard has not fully developed and implemented procedures to ensure that a script, planned to be run in production, has been through an appropriate level of review to fully assess if it has a financial statement impact.

All of our ITGC findings are described in detail in a separate *Limited Official Use* (LOU) letter provided to the Coast Guard and DHS management.

Related to financial system functionality:

We noted many cases where financial system functionality is inhibiting the Coast Guard's ability to implement and maintain internal controls, notably IT application controls supporting financial data processing and reporting. Financial system functionality limitations increase the difficulty of compliance with Federal financial system requirements and guidelines, notably FFMIA and OMB Circular A-127. Examples of financial system functionality conditions we identified include:

- As noted above, Coast Guard's core financial system configuration management process is not operating effectively due to inadequate controls over IT scripts. The IT script process was instituted as a solution primarily to compensate for system functionality and data quality issues.
- Financial system audit logs are not readily generated and reviewed, as some of the financial systems continue to lack the capability to perform this task efficiently.
- The Coast Guard is unable to routinely query its various general ledgers to obtain a complete population of financial transactions, and consequently must create many manual custom queries that delay financial processing and reporting processes.
- A key Coast Guard financial system is limited in processing overhead cost data and depreciation expenses in support of the property, plant and equipment (PP&E) financial statement line item.
- Production versions of financial systems are outdated and do not provide the necessary core functional capabilities (e.g., general ledger capabilities).
- Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls that would improve accuracy, reliability, and facilitate efficient processing of certain financial data such as:
 - Ensuring proper segregation of duties and access rights, such as automating the procurement process to ensure that only individuals who have proper contract authority can approve transactions or setting system access rights within the fixed asset subsidiary ledger;



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

- Maintaining sufficient data to support Fund Balance with Treasury related transactions, including suspense activity;
- Maintaining adequate posting logic transaction codes to ensure that transactions are recorded in accordance with generally accepted accounting principles (GAAP); and
- Tracking detailed transactions associated with intragovernmental business and eliminating the need for default codes such as Trading Partner Identification Number that cannot be easily researched.

Cause/Effect: The current system configurations for many Coast Guard financial systems cannot be easily reconfigured to meet FFMLA, OMB Circular A-127, and DHS security requirements. The conditions supporting our findings collectively limit the Coast Guard's ability to process, store, and report financial data in a manner to ensure accuracy, confidentiality, integrity, and availability. Some of the weaknesses may result in material errors in the Coast Guard's financial data that are not detected in a timely manner through the normal course of business. In addition, because of the presence of IT control and financial system functionality weaknesses, there is added pressure on mitigating controls to operate effectively. Because mitigating controls are often more manually focused, there is an increased risk of human error that could materially affect the financial statements. See Comment I-A, *Financial Reporting*, for a discussion of the related conditions causing noncompliance with the requirements of FFMLA. Configuration management weaknesses are also among the principle causes of the Coast Guard's inability to support certain financial statement balances for audit purposes.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that the DHS Office of Chief Information Officer (OCIO), in coordination with the Office of the Chief Financial Officer (OCFO):

1. Continue to develop and implement policies, procedures, and processes to address scripting weaknesses, including weaknesses related to functional testing, audit logging, approvals, and recertifications, and the documentation and review of script records.
2. For new and updated script procedures, revise associated trainings and provide the training to impacted staff.
3. Continue to improve the script change management process and other associated internal controls as they relate to the financial statement impact of the changes to the CAS suite of financial databases.
4. Make necessary improvements to financial management systems and supporting IT security controls.

Specific recommendations are provided in a separate *Limited Official Use* letter provided to Coast Guard management.

I-C Property, Plant, and Equipment

Background: The Coast Guard maintains approximately 49 percent of all DHS property, plant, and equipment (PP&E), including a large fleet of boats and vessels. Many of the Coast Guard's assets are constructed over a multi-year period, have long useful lives, and undergo extensive routine servicing that may increase their value or extend their useful lives. DHS stewardship PP&E primarily consists of Coast Guard heritage assets, which are PP&E that are unique due to historical or natural significance; cultural, educational, or artistic (e.g., aesthetic) importance; or architectural characteristics. Coast Guard heritage assets consist of both collection type heritage assets, such as artwork and display models, and non-collection type heritage assets, such as lighthouses, sunken vessels, and buildings.

In FY 2011, the Coast Guard continued to execute remediation efforts to address PP&E process and control deficiencies, specifically those associated with vessels, small boats, aircraft, and select construction in process (CIP) projects, and also related to the inventory of heritage assets. Inventory procedures were performed in FY 2011 to assist in the substantiation of existence and completeness of PP&E balances, however, they were not performed over all asset classes (e.g., land, buildings and other structures, and electronic equipment). Additionally, an analysis to ensure the proper accounting of internal use software



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

has not yet been completed. Remediation efforts are scheduled to occur over a multi-year timeframe beyond FY 2011. Consequently, many of the conditions cited below have been repeated from our FY 2010 report.

Conditions: The Coast Guard has not:

Regarding PP&E:

- Established accurate and auditable PP&E balances as of September 30, 2011. In cases where original acquisition documentation has not been maintained, the Coast Guard has not fully implemented methodologies and assumptions to support the value of all PP&E.
- Implemented appropriate controls and related processes to accurately, consistently, and timely record additions to PP&E, (including all costs necessary to place the asset in service e.g., other direct costs), transfers from other agencies, disposals in its fixed asset system, CIP activity, and support the valuation and classification of repairable PP&E.
- Implemented accurate and complete asset identification, system mapping, and tagging processes that include sufficient detail (e.g., serial number) to clearly differentiate and accurately track physical assets to those recorded in the fixed assets system.
- Developed and implemented a process to identify and evaluate all lease agreements to ensure that they are appropriately categorized as operating or capital, and properly reported in the financial statements and related disclosures.
- Properly accounted for improvements and impairments to buildings and structures, capital leaseholds, selected useful lives for depreciation purposes, and appropriate capitalization thresholds, consistent with GAAP.
- Identified and tracked all instances where PP&E accounting is not in compliance with GAAP and prepared a non-GAAP analysis that supports management's accounting policies. This analysis should be maintained and available for audit.

Regarding Heritage Assets:

- Fully designed and implemented policies, procedures, and internal controls to support the completeness, existence, accuracy, and presentation assertions over data utilized in developing required financial statement disclosures and related supplementary information for heritage assets.

Cause/Effect: The Coast Guard has had difficulty establishing its opening PP&E balances primarily because of poorly designed policies, procedures, and processes implemented more than a decade ago, combined with ineffective internal controls, and IT functionality difficulties. See Comment **I-B, Information Technology Controls and Financial Systems Functionality**. PP&E was not properly accounted for or tracked, for many years preceding the Coast Guard's transfer to DHS in FY 2003, and now the Coast Guard is faced with the formidable challenge of performing retroactive analyses in order to properly establish the existence, completeness, and accuracy of PP&E. Additionally, the fixed asset module of the Coast Guard's general ledger accounting system is not updated timely for effective tracking and reporting of PP&E on an ongoing basis. As a result, the Coast Guard is unable to accurately account for its PP&E, and provide necessary information to DHS OFM for consolidated financial statement purposes.

The Coast Guard management deferred correction of the stewardship PP&E (heritage assets) weaknesses reported in previous years, and acknowledged that the conditions we reported in prior years remained throughout FY 2011. The lack of comprehensive and effective policies and controls over the identification and reporting of Stewardship PP&E could result in misstatements in the required financial statement disclosures and related supplementary information for Stewardship PP&E.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

Recommendations: We recommend that the Coast Guard:

Regarding PP&E:

1. Continue to implement remediation efforts associated with establishing PP&E balances, including designing and implementing inventory procedures over all PP&E categories and implementing methodologies, including the use of Statement of Federal Financial Accounting Standard (SFFAS) No. 35, to support the value of all PP&E;
2. Implement appropriate controls and related processes to accurately and timely record additions to PP&E, transfers from other agencies, improvements, impairments, capital leases, indirect costs, depreciable lives, disposals in its fixed assets system, and valuation and classification of repairable PP&E. Additionally, continue to implement remediation efforts associated with control over the completeness, existence, accuracy, and valuation of all CIP related balances;
3. Adhere to procedures to timely update the fixed asset module of the Coast Guard's general ledger accounting system to improve tracking and reporting of PP&E on an ongoing basis. Implement processes and controls to record any identifying numbers in the fixed asset system at the time of asset purchase to facilitate identification and tracking, and to ensure that the status of assets is accurately tracked in the subsidiary ledger;
4. Develop and implement a process to identify and evaluate all lease agreements to ensure that they are appropriately categorized as operating or capital, and are properly reported in the financial statements and related disclosures;
5. Ensure that appropriate supporting documentation is maintained and readily available to support PP&E life-cycle events (e.g., improvements, in-service dates, disposals, etc.); and
6. Perform and document a non-GAAP analysis for all instances where accounting policies are not in compliance with GAAP.

Regarding Stewardship PP&E:

1. Design and implement policies, procedures, and internal controls to support the completeness, existence, accuracy, and presentation and disclosure assertions related to the data utilized in developing disclosures and related supplementary information for Stewardship PP&E that is consistent with GAAP.

I-D Environmental and Other Liabilities

Background: The Coast Guard's environmental liabilities consist of environmental remediation, cleanup, and decommissioning and represent approximately \$973 million or 93 percent of total DHS environmental liabilities. Environmental liabilities are categorized as relating to shore facilities or vessels. Shore facilities include any facilities or property other than ships (e.g., buildings, fuel tanks, lighthouses, small arms firing ranges, etc.). During FY 2011, the Coast Guard continued to implement a multi-year remediation plan to address process and control deficiencies related to environmental liabilities. In FY 2011, progress was made with respect to implementation of policies and procedures; however, the majority of the conditions cited in our FY 2010 report remain.

The Coast Guard estimates accounts payable by adjusting the prior year accrual estimate based on an analysis of actual payments made subsequent to September 30 of the prior year.

The Coast Guard's contingent legal liability balance is comprised of estimates associated with various administrative proceedings, legal actions, and tort claims that arise in the normal course of Coast Guard operations.

A component of Coast Guard's accrued payroll and benefits liability balance is annual leave. Annual leave is composed of earned annual and other vested compensatory leave that is accrued as it is earned. Subsequently, as leave is taken, the liability is reduced.



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

Conditions: We noted the following internal control weaknesses related to environmental and other liabilities.

The Coast Guard has not:

Regarding environmental liabilities:

- Fully supported the completeness, existence, and accuracy assertions of the data utilized in developing the estimate for the FY 2011 environmental liabilities account balance.
- Fully implemented policies and procedures to develop, prepare, record, and periodically review environmental liability estimates related to shore facilities and vessels. Specifically, procedures to confirm the existence of and legal liability for environmental damage/contamination sites, ensure the completeness of the environmental site universe, and verify the historical accuracy of assumptions used and estimates made for environmental liabilities.

Regarding other liabilities:

- Designed a methodology used to estimate accounts payable that considers and uses all potentially relevant current year data. As a result, current year data that may have a significant impact on the estimate could be overlooked and not identified until a true-up is performed in the subsequent year.
- Ensured that policies and procedures associated with management's review of the underlying data supporting contingent legal and payroll liability (i.e., unfunded leave) balances are fully implemented and operating effectively. Specifically, deficiencies in management's review attributed to errors in the underlying data supporting the interim contingent legal liability and unfunded leave balances.

Cause/Effect: The Coast Guard has not fully completed its remediation plans to develop, document, and implement policies and procedures to, prepare, and record environmental liability estimates in accordance with applicable accounting standards. As a result, the Coast Guard is unable to assert to the accuracy of its environmental liability balances as stated in the September 30, 2011 balance sheet, and provide necessary information to OFM for DHS financial statement purposes.

The Coast Guard's methodology used to estimate accounts payable is based on the prior year estimate, validated via a subsequent payment analysis, and does not consider or use all applicable current year data. Without consideration of applicable current year data, a misstatement in the accounts payable estimate may occur and not be identified in a timely manner (i.e., until a true-up is performed in a subsequent period).

The Coast Guard did not fully adhere to existing policies and procedures associated with the review of underlying data supporting interim contingent legal and payroll liability balances. A lack of adequate management review over the underlying data supporting account balances increases the risk that a misstatement may go undetected.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that the Coast Guard:

Regarding environmental liabilities:

Fully implement policies, procedures, processes, and controls to ensure the identification and recording of all environmental liabilities, to define the technical approach, to establish cost estimation methodology, and to develop overall financial management oversight of its environmental remediation projects. Consider the "Due Care" requirements defined in Federal Accounting Standards Advisory Board (FASAB) Technical Release No. 2 *Determining Probable and Reasonably Estimable for Environmental Liabilities in the Federal Government*. The policies should include procedures to:

1. Ensure the proper calculation and review of cost estimates for consistency and accuracy in financial reporting, including the use of tested modeling techniques, use of verified cost parameters, and assumptions;
2. Periodically validate estimates against historical costs; and



Independent Auditors' Report
Exhibit I – Material Weaknesses in Internal Control – U.S. Coast Guard

3. Ensure that detailed cost data is maintained and reconciled to the general ledger.

Regarding other liabilities:

1. Analyze and make appropriate improvements to the methodology used to estimate accounts payable to include potentially relevant current year data, and support all assumptions and criteria with appropriate documentation used to develop and subsequently validate the estimate for financial reporting; and
2. Adhere to existing policies and procedures associated with the review of underlying data supporting contingent legal and accrued payroll and benefits liabilities.

I-E Budgetary Accounting

Background: Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded. Each Treasury Account Fund Symbol (TAFS) with separate budgetary accounts must be maintained in accordance with OMB and U.S. Treasury guidance. The Coast Guard has over 80 TAFS covering a broad spectrum of budget authority, including annual, multi-year, and no-year appropriations; and several revolving, special, and trust funds.

Conditions: We noted the following internal control weaknesses related to budgetary accounting, which were repeated from our FY 2010 report. The Coast Guard has not:

- Fully implemented policies, procedures, and internal controls over its process for validation and verification of undelivered order (UDO) balances. Recorded obligations and UDO balances were not always complete, valid, or accurate, and proper approvals are not always maintained.
- Finalized and implemented policies and procedures to monitor unobligated commitment activity in CAS throughout the fiscal year.
- Designed and implemented effective procedures, processes, and internal controls to verify the completeness and accuracy of the year-end obligation “pipeline” which are obligations executed on or before September 30, but not recorded in the Coast Guard’s CAS, and to record all executed obligations. These deficiencies affected the completeness, existence, and accuracy of the year-end “pipeline” adjustment that was made to record obligations executed before year end.

Cause/Effect: A lack of fully implemented policies, procedures, and internal controls surrounding commitments, obligations, UDOs, delivered orders, and disbursements has caused various control gaps in the internal control environment. Weak controls in budgetary accounting, and associated contracting practices increase the risk that the Coast Guard misstates budgetary balances, and unintentionally violate the *Anti-deficiency Act* by overspending its budget authority. Also, the untimely release of commitments may prevent funds from being used for other more critical needs.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that the Coast Guard:

1. Continue to improve policies, procedures, and the design and effectiveness of controls in both accounting and contracting related to processing obligation transactions, and periodic review and validation of UDOs. Emphasize to all fund and program managers the need to perform effective reviews of open obligations, obtain proper approvals, and retain supporting documentation;
2. Finalize policies and procedures to periodically review commitments, and make appropriate adjustments in the financial system; and
3. Improve procedures, processes, and internal controls to verify the completeness and accuracy of the year-end obligation “pipeline” adjustment to record all executed obligations for financial reporting.



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

II-A Financial Reporting (TSA, USCIS)

Background: The Transportation Security Administration (TSA) has adopted a multi-year effort to develop and install the appropriate financial reporting processes, together with proper internal controls over financial reporting (ICOFR). In fiscal year (FY) 2011, TSA made progress by hiring accounting personnel, and substantially completing the reconciliation of its balance sheet accounts. However, TSA has not fully implemented all of the planned processes, and associated internal controls. Consequently, some financial reporting control weaknesses reported in FY 2010 continued to exist, and some new deficiencies were identified.

	2011	2010	2009
TSA			
FEMA	C		
USCIS		N/A	N/A
CBP	C	C	

The United States Citizen and Immigration Service (USCIS) requires advance payments of the fees for adjudication of applications or petitions for immigration and naturalization benefits. These advance receipts account for the majority of deferred revenue reported in the Department of Homeland Security (DHS or Department) financial statements. In FY 2011, the Department implemented a change in accounting to report the user fees collected by USCIS as exchange revenue on the statement of net cost. Previously, these user fees were reported as revenue on the statement of custodial activity. This change resulted in an immaterial correction of an error in the presentation of user fees as reported in previous years, and identification of a control deficiency in the financial reporting process at USCIS.

Key – Trend Table	
C	Deficiencies are corrected
N/A	No deficiencies reported
	Deficiencies are less severe*
	Deficiencies are more severe*
* See Introduction	

FEMA implemented corrective actions in financial reporting processes, and substantially remediated the conditions we reported in FY 2010.

Conditions: We noted the following internal control weaknesses related to Financial Reporting at TSA and USCIS.

1. TSA:

- Has not fully developed its financial reporting process with sufficient policies, procedures, and internal controls to ensure the reliability of certain significant financial statement balances. For example, we noted that TSA:
 - Has ineffective internal controls, including supervisory reviews and monitoring, at some significant process-level risk points, e.g., where there is a risk of material error within a process;
 - Lacks some policies and procedures to ensure that changes in accounting policies and methodologies are reviewed, tested, and vetted prior to adoption;
 - Has not distributed the financial reporting workload to ensure that resources and skills are aligned with tasks, making optimal use of technical resources, and improving internal controls over financial reporting;
 - Is unable to fully identify and present its intragovernmental balances and transactions by trading partner; and
 - Is not fully compliant with the United States Government Standard General Ledger (USSGL) requirements at the transaction level.

2. USCIS:

- Did not update its accounting policies and practices in a timely manner to address a change in financial accounting which arose from a change in legislation. USCIS' presentation of certain fees



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

as custodial revenue should have been presented as exchange revenue since FY 2005, when the change in legislation occurred.

- Did not have sufficient policies and procedures, or documentation supporting the process used to develop adjustments to deferred revenue. This process was previously performed by an outside contractor.

Cause/Effect: TSA hired a number of accounting staff during the current year, which required substantial training and oversight by existing employees during the process. Additionally accounting staff were often committed to projects or focusing on remediation of control deficiencies, as such, TSA was unable to make optimal use of its technical resources in a review and monitoring capacity. As a result, in some cases, adjustments to correct errors in accounts were recorded without appropriate supporting analysis, documentation, and reviews.

USCIS Financial Management Division (FMD) was aware of the change in legislation in FY 2005 that affected the accounting for certain fees collected, but did not finalize the change in accounting to match the legislation until this year. USCIS and DHS Office of Financial Management (OFM) decided to delay making the change pending further guidance from various outside sources such as the Office of Management and Budget (OMB) and Department of Treasury. While the guidance was ultimately useful, the accounting change should be made in the same year as the triggering event (change in legislation in this case). In addition, USCIS was unable to perform certain functions previously done by an outside contractor, due to a lack of documentation describing the procedures, resulting in errors in interim financial statements.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that:

1. TSA:
 - a. Expand the annual risk assessment process to identify risk-points where control weaknesses exist and update policies and procedures to mitigate risk of error in the financial statements;
 - b. Develop formal policies and procedures to ensure that changes in accounting policies and methodologies are reviewed, tested, and vetted prior to adoption, and ensure compliance with the USSGL requirements at the transaction level;
 - c. Update annual performance plans for staff to outline goals and expected results that align to implementing corrective actions, maintaining internal controls, mitigating risks identified through the annual risk assessment process and maintaining routine communication with organizations that impact financial reporting; and
 - d. Work with its accounting service provider to ensure that the proper trading partner code is recorded for each intragovernmental transaction.
2. USCIS:
 - a. Work with DHS OFM to identify and implement necessary changes to accounting policies in the reporting period that the triggering event occurs; and
 - b. Establish additional controls, either manual or automated, to ensure all steps in the monthly and quarterly deferred revenue estimation process are completed accurately and timely.



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

II-B Information Technology Controls and Financial System Functionality (CBP, USCIS, FEMA, ICE)

Background: As part of the DHS financial statement integrated audit, we evaluated select Information Technology (IT) general controls (ITGC) using the objectives defined by U.S. Government Accountability Office (GAO)'s *Federal Information System Controls Audit Manual (FISCAM)*, in five key control areas: security management, access control, configuration management, segregation of duties, and business continuity. In addition to ITGC's, we evaluated select application controls, which are controls supporting the structure, policies, and procedures that apply to the use, operability, interface, edit, and monitoring controls of a financial application. We also considered the effects of financial system functionality when testing internal controls. Many key DHS financial systems are not compliant with *Federal Financial Management Improvement Act of 1996 (FFMIA)* and OMB Circular Number A-127, *Financial Management Systems* (as revised and effective on October 1, 2009). DHS financial system functionality limitations add to the Department's challenges of addressing systemic internal control weaknesses, and limit the Department's ability to effectively and efficiently process and report financial data.

	2011	2010	2009
CBP	■	■	■
USCIS	■	■	■
FEMA	■	■	■
FLETC	C	■	■
ICE	■	■	■
TSA	C	C	■
See page II.2 for table explanation.			

During our FY 2011 assessment of IT general and application controls, we noted that the DHS Civilian Components made progress in remediation of IT findings we reported in FY 2010. We have closed approximately 30 percent of our prior year IT findings. ICE, FEMA, and FLETC made the most progress in closing IT findings from the prior year. As evidence of further progress made by DHS, we identified approximately one-half of the number of new findings in FY 2011 compared to the number of new findings identified in FY 2010. The majority of these new deficiencies were noted at CBP.

However, at the end of FY 2011, over approximately 135 IT control weaknesses existed, of which more than 65 percent are repeated from last year. Approximately 25 percent of our repeat findings were for IT deficiencies that management represented were corrected during FY 2011.

The primary (circle) bullets listed below each FISCAM heading are a cross-representation of the nature of IT general control deficiencies identified throughout the Department's components. The secondary (dash) bullets represent single or multiple occurrence findings in one or more components.

Conditions: Our findings related to IT controls and financial systems functionality follow:

Related to IT controls:

1. *Access controls:*

- Deficiencies in management of application and/or database accounts, network, and remote user accounts.
 - System administrator root access to financial applications was not properly restricted, logged, and monitored. Emergency and temporary access was not properly authorized, and contractor development personnel were granted conflicting access to implement database changes;
 - Complex password configurations were not implemented and/or enforced;
 - User account lists were not periodically reviewed for appropriateness, improper authorizations and excessive user access privileges were allowed at some DHS components, and users were not disabled or removed promptly upon personnel termination; and
 - The process for authorizing and managing virtual private network (VPN) access to external state emergency management agencies, and component contractors, did not comply with DHS and component requirements.
- Ineffective safeguards over logical and physical access to sensitive facilities and resources.



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

- During after-hours physical security walkthroughs, we identified the following unsecured items: Personally Identifiable Information (PII); credit cards; financial system passwords; laptops; sensitive documentation, and server names and IP addresses; and
 - While performing social engineering testing, we identified instances where DHS employees provided their system user names and passwords to an auditor posing as a help desk employee.
 - Lack of generation, review, and analysis of system audit logs and adherence to DHS requirements.
2. *Configuration management:*
- Lack of documented policies and procedures.
 - Financial systems change control documentation was not updated to represent the current operating environment, including sensitive user functions, roles and privileges; and
 - Configuration, vulnerability, and patch management plans have not been established and implemented, or did not comply with DHS policy.
 - Security patch management and configuration deficiencies were identified during the vulnerability assessment on the platforms supporting the key financial applications and general support systems.
3. *Security management:*
- Systems certification and accreditation were not completed and maintained, or documented.
 - Several component financial and associated feeder systems as well as general support systems, were not properly certified and accredited, in compliance with DHS policy;
 - Compliance with the Federal Desktop Core Configuration (FDCC) security configurations is in progress, but has not been completed; and
 - System security plans and annual evaluations were not completed and maintained.
 - IT Security personnel lack mandatory role-based training or compliance is not documented and monitored.
 - Background investigations of federal employees and contractors employed to operate, manage and provide security over IT systems were not being properly conducted.
4. *Contingency Planning:*
- Service continuity plans were not tested nor updated to reflect the current environment, and an alternate processing site has not been established for high risk systems.
 - Authorized access to backup media was not periodically reviewed and updated; at one component procedures to periodically test backups was not implemented.
5. *Segregation of Duties:*
- Lack of evidence to show that least privilege and segregation of duties controls exist, including policies and procedures to define conflicting duties and access rights.

These control findings, including other significant deficiencies, are described in greater detail in a separate *Limited Official Use* letter provided to DHS management.

Related to financial system functionality:

We noted many cases where financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT application controls supporting financial data processing and reporting. Financial system functionality limitations also contribute to other control deficiencies reported in Exhibits I, II, and III, and compliance findings presented in Exhibit IV. We noted persistent and pervasive financial system functionality conditions at all of the significant DHS components in the following general areas:



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

- Lack of integration between the core financial systems and key feeder systems, such as property management systems, leading to errors and inefficiencies in the processing and reporting of financial data.
- Inability of financial systems to process, store, and report financial and performance data to facilitate decision making, safeguarding and management of assets, and prepare financial statements that comply with generally accepted accounting principles (GAAP).
- Technical configuration limitations, such as outdated systems that are no longer fully supported by the software vendors, impairing DHS' ability to fully comply with policy in areas such as IT security controls, notably password management, audit logging, user profile changes, and the restricting of access for off-boarding employees and contractors.
- System capability limitations prevent or restrict the use of applications controls to replace less reliable, more costly manual controls. Or in some cases, require additional manual controls to compensate for IT security or control weaknesses.

Cause/Effect: Many financial system and IT control weaknesses have resulted from DHS' long-standing inability to upgrade its financial system capabilities. The Transformation and Systems Consolidation (TASC) initiative, postponed during FY 2011, is the latest DHS financial systems modernization effort to be postponed, delayed, or canceled. DHS broad and systemic financial system and IT control limitations will not be fully addressed until DHS and/or the components implement a stable financial system platform. Once a new strategy and plan are developed, it will likely take DHS several years to implement process and system improvements.

The conditions supporting our findings collectively limit DHS' ability to process, store, and report financial data in a manner to ensure accuracy, confidentiality, integrity, and availability. Many of the weaknesses may result in material errors in DHS' financial data that are not detected in a timely manner through the normal course of business. In addition, because of the presence of IT control and financial system functionality weaknesses, there is added pressure on mitigating controls to operate effectively. Because mitigating controls are often more manually focused, there is an increased risk of human error that could materially affect the financial statements.

Recommendations: We recommend that the DHS Office of the Chief Information Officer (OCIO), in coordination with the Office of the Chief Financial Officer (OCFO), make necessary improvements to the Department's financial management systems and supporting IT security controls. Specific recommendations are provided in a separate *Limited Official Use* letter provided to DHS management.

II-C Property, Plant, and Equipment (TSA, CBP, MGMT)

Background: TSA owns a substantial number and variety of assets that are used for passenger screening at airports throughout the United States. TSA is also developing new software to support various mission related objectives, such as *Secure Flight*. The costs required to procure, ship, temporarily store, install, operate, and maintain this equipment and software are substantial and consume a large portion of TSA's annual operating budget. Unique accounting processes and systems are necessary to track the status and accumulate costs, and to accurately value, account for, and depreciate and amortize the equipment and software.

Customs and Border Protection (CBP) has acquired substantial new technology, facilities, and other assets in recent years through purchase and construction. CBP's new assets include construction of border fencing (both physical and virtual), purchase of inspection equipment at ports of entry, and new construction at port of entry facilities.

Management Directorate (MGMT) underwent a process in FY 2011 to

	2011	2010	2009
TSA			
CBP			
MGMT		N/A	N/A
FEMA	N/A	N/A	
USCIS	C	C	
ICE	C	C	
NPPD	C	C	
See page II.2 for table explanation			



Independent Auditors' Report

Exhibit II – Material Weaknesses – DHS Civilian Components

identify assets that had been inappropriately expensed in prior fiscal years, resulting in a corrective adjustments made in the financial statements, and the identification of a control deficiency.

Conditions: We noted the following internal control weaknesses related to PP&E at TSA, CBP, and MGMT:

1. TSA:

- Has not implemented policies, procedures, and controls to properly identify risks and potential errors related to general property, equipment, internally developed software, asset additions and disposals, and other direct costs incurred to transport, store and install screening equipment at airports, as necessary, to maintain the accuracy and completeness of those account balances. Several adjustments some of which were auditor-identified, were required to fairly state PP&E accounts affected by these items.
- Controls were not fully effective to properly track and record all assets at U.S. airports and at the Federal Air Marshal Facility, accurately in the system of record, and to properly track, reconcile, and value idle assets.
- Controls were not fully effective to accurately depreciate assets on a continuous basis.
- Lacks effective higher level controls, including supervisory reviews, reconciliations and monitoring, of property, plant, and equipment, and to ensure that balances recorded in the general ledger were supported by available supporting documentation.

2. CBP:

- Does not have adequate accounting policies, procedures, processes, and controls to properly account for new equipment purchases and transfers, construction, depreciation, or disposal of assets in a timely manner. For example, CBP did not:
 - Accurately record and correctly classify construction-in-process (CIP) to reflect the correct assets, and current status of construction or percentage of completion of long-term projects throughout the year;
 - Transfer certain assets from CIP to “in-use” assets in a timely manner;
 - Record some asset additions and disposals in accordance with its policy; and
 - Record transactions affecting PP&E timely, and based on complete documentation that is retained for audit, and reflected in the proper USSGL account.
- Did not properly perform and/or document certain real and personal physical inventories in accordance with standard operating procedures.

3. MGMT:

- Does not have adequate asset management processes and controls in place to record and track PP&E at the transaction level.
- Does not have processes and controls in place to maintain sufficient asset tracking records, as well as conduct periodic inventories.

Cause/Effect: TSA focused primarily on developing and implementing new policies and remediating control deficiencies in the current year. At the same time, TSA hired a number of new employees during the current year which required additional oversight and training on new processes. As a consequence a general lack of coordination and communication (including training, oversight, and monitoring) with some key personnel outside of the TSA OFM contributed to control deficiencies that exist over PP&E at TSA. These conditions led to a number of errors in the financial statements that were discovered during our audit.



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

This deficiency is also related to the conditions described in Comment **II-A**, *Financial Reporting* and Comment **III-F**, *Entity-Level Controls*.

CBP does not have documented and/or fully implemented policies and procedures, or does not have sufficient oversight of its policies and procedures, to ensure that all PP&E transactions are recorded timely and accurately. As a result, CBP's PP&E balance may be misstated by the recording of transactions, which are incorrect, unsupported, or untimely. Also, CBP IT systems lack functionality to track and account for assets in various stages of completion and deployment leading to increased manual involvement to accurately report assets. This deficiency is also related to the conditions described in Comment **II-B**, *Information Technology Controls and Financial Systems Functionality*.

MGMT's reliance on manual compensating controls over asset management increases the risk of misstatement in the PP&E balance. MGMT does not have fully developed asset management policies and procedures for recording and reporting PP&E balances in the financial statements, and relies on a labor intensive process to analyze and make manual adjustments to record PP&E for financial reporting purposes.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that:

1. TSA:
 - a. Strengthen existing policies and procedures to properly identify risks, potential errors, and account for, monitor, and report general property, equipment, internal use software balances, asset additions and disposals, and other direct costs;
 - b. Develop and implement sufficient procedures to properly document, track, and value in-use and idle assets on an on-going basis;
 - c. Enhance controls to ensure that depreciation is accurately computed and recorded on a continuous basis; and
 - d. Enhance controls to ensure that balances recorded in the general ledger are supported by available supporting documentation that can be readily available for management and auditor review as needed.
2. CBP:
 - a. Develop, document, and communicate policies and procedures for classifying, recording, and reviewing all capital transactions, particularly for construction projects, to ensure that the financial statements are materially correct and presented in accordance with GAAP. Consideration should be given to the adequacy of policies to account for CIP, including methodologies to apply overhead charges, and establishing an appropriate useful life for annual depreciation charges;
 - b. Determine whether existing policies and procedures for recording asset additions, reclassifications, and retirements are sufficient. Revise policies where necessary, including retention of supporting documentation and authorization of transactions, and communicate policies throughout CBP;
 - c. Develop supervisory and monitoring controls to ensure that erroneous transactions are identified and remediated promptly;
 - d. Determine and request the necessary system changes to CBP's financial IT system to facilitate the timely and accurate recording of asset additions and reclassifications; and
 - e. Improve guidance for the performance and documentation of PP&E inventories.
3. MGMT:
 - a. Finalize and implement asset management policies and procedures over recording and processing PP&E activity, including an automated asset property management process and controls to record and track PP&E at the transaction level.
 - b. Implement policies and processes to conduct periodic inventories of PP&E.



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

II-D Not Used

II-E Budgetary Accounting (FEMA)

Background: Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded. DHS has over 350 separate TAFS combined, each with separate budgetary accounts that must be maintained in accordance with OMB and Treasury guidance. The TAFS cover a broad spectrum of budget authority, including annual, multi-year, and no-year appropriations, and several revolving, special, and trust funds. Accounting for budgetary transactions in a timely and accurate manner is essential to managing the funds of the Department and preventing overspending of allotted budgets.

	2011	2010	2009
FEMA			
CBP	C		
See page II.2 for table explanation			

In FY 2011, FEMA continued to improve its processes and internal controls over the obligation and monitoring process; however, some control deficiencies remain.

CBP implemented corrective actions in budgetary accounting processes in FY 2011, and substantially remediated the conditions we reported in FY 2010.

Conditions: We noted the following internal control weaknesses related to budgetary accounting at FEMA:

- Did not effectively monitor the status of its obligations as part of its normal operations to ensure timely deobligation when appropriate.
- Lacks enforcement of existing policy, around the obtaining approvals, recording obligations, and making payments.
- Could not readily provide all supporting documentation for undelivered orders (UDO), tested at June 30, 2011 and September 30, 2011. We noted that for certain portions of the population, significant effort was required to coordinate and identify the responsible parties, to access certain files, or to provide information in a form that clearly supported the balances reported in the financial statements.
- Was required to correct erroneous entries recorded by the Budget Planning & Analysis Division (BPAD) or to record transactions that should have been recorded by the BPAD but were not.
- Did not properly review budgetary funding transactions recorded in the general ledger.

Cause/Effect: FEMA's UDO annual certification and quarterly validation processes are not effectively implemented. Additionally, FEMA's administrative functions are geographically separated from programmatic operations which make consistent enforcement of policy challenging. Certain offices within FEMA do not have effective document maintenance policies and procedures, making the location of certain UDO documentation difficult. Without supporting documentation, FEMA is unable to support the validity of certain UDO balances. Certain personnel within the BPAD do not have the necessary skills or training to correctly record budgetary entries in FEMA's general ledger. In addition, BPAD budgetary funding transaction review procedures implemented in the current year were not consistently adhered to. As a result, FEMA's financial information submitted to DHS may contain significant budgetary account errors if they are not detected by the FEMA's OCFO.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that FEMA:

1. Adhere to the established UDO annual certification and quarterly validation processes to ensure that outstanding obligations are properly classified and reviewed for validity quarterly;
2. Enforce existing policies to ensure that all obligations are approved and recorded and that all payments made are supported by appropriate documentation;



Independent Auditors' Report
Exhibit II – Material Weaknesses – DHS Civilian Components

3. Continue to improve procedures for storing and locating documentation supporting UDO information, including points of contact, so that supporting information is readily available for management review and audit purposes;
4. Dedicate the appropriate resources to adequately staff, train, and supervise BPAD personnel to ensure that the BPAD is properly recording all necessary budgetary transactions; and
5. Fully implement new review procedures for budgetary funding transactions recorded in the general ledger.



Independent Auditors' Report
Exhibit III – Significant Deficiencies – All DHS Components

III-F Entity-Level Controls (TSA, FEMA)

Background: In the past three years, the Department of Homeland Security (DHS or the Department) has undertaken and completed several steps designed to strengthen its entity and process level internal controls, and thereby improve the reliability of financial reporting. These steps are documented in the *Internal Control over Financial Reporting Playbook* and in component level Mission Action Plans (MAPs) prepared annually. The Department's Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, assessment is also designed to assist with the remediation of control deficiencies.

	2011	2010	2009
TSA		C	
USCG	C		
FEMA			
CBP	C		NA
See page II.2 for table explanation			

The comments below should be read in conjunction with Comment II-B, *Information Technology Controls and Financial System Functionality*, which describe entity-level control weaknesses related to Department and Component IT systems.

The Transportation Security Administration (TSA) makes extensive use of capital assets and new technologies to perform its mission. As a result, accounting for certain assets and activities require inputs from operating and program personnel who are outside the traditional financial accounting processes. In addition, considering TSA's business, the appropriate application of some accounting standards can be complex, requiring extensive knowledge of both TSA's business activities and accounting standards.

Federal Emergency Management Agency (FEMA) made continued progress toward correction of its entity-level control deficiencies in FY 2011. While progress has been made, some entity-level control deficiencies identified at FEMA in previous years continued during FY 2011, and are repeated below.

The U.S. Coast Guard (Coast Guard) made continued progress following its *Financial Strategy for Transformation and Audit Readiness* (FSTAR) plan, see comment I-A, *Financial Reporting*.

Conditions: We noted the following internal control weaknesses related to entity-level controls at TSA, Coast Guard, and FEMA:

1. TSA:

- Has not fully developed processes to proactively manage risks identified through the annual risk assessment process, and to monitor adherence to financial management policies and procedures of staff that reside outside the Office of Financial Management.
- Lacks reliable processes to identify changes in business operations that could also result in changes to accounting processes or financial reporting in a timely manner.

2. FEMA:

- Has not certified its formal policies and procedures on a biennial basis to validate they are accurate and current, as required by FEMA Directive No. 112-1.
- Has not committed sufficient resources to ensure that personnel attend required ethics training.
- Has not developed sufficient policies and procedures to properly conduct and track the status of background investigations and maintain related documentation.

Cause/Effect: TSA has not yet fully developed its processes and controls throughout the agency to ensure accurate and complete information is identified and reported to the Office of Financial Management (OFM). Consequently, TSA was at times dependent on the external financial statement audit process to identify business process changes with financial reporting impact and the associated risks of misstatement or account balance errors in the financial statements.

In FY 2011, FEMA devoted substantial resources to remediating certain IT findings. Consequently, FEMA devoted comparatively less attention to correcting other control deficiencies in FY 2011. Decentralized and



Independent Auditors' Report
Exhibit III – Significant Deficiencies – All DHS Components

informal background investigation processes continue to present potential risks to FEMA's operations and IT systems.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that:

1. TSA:
 - a. Develop and adopt policies and procedures to improve coordination and communication and provide guidance to certain program managers, engineers, and accountants, who are outside of the OFM, but who provide key financial data necessary to accurately present account balances, in compliance with accounting standards. This may involve training for Business Resource Managers within the operational TSA organizations to better equip them to recognize events that may impact financial reporting, and to ensure appropriate communications to manage financial statement risk; and
 - b. Develop and implement sufficient procedures to timely identify changes in business processes that could result in changes to accounting processes or financial reporting.
2. FEMA:
 - a. Complete the efforts underway to ensure that formal policies and procedures are catalogued, reviewed, and certified on a biennial basis in accordance with FEMA Directive No. 112-1;
 - b. Complete development and implementation of procedures and dedicate resources to provide, track compliance with, and monitor the annual and new hire ethics training requirements; and
 - c. Develop and implement policies and procedures to properly track the status and completion of background investigations and maintain related documentation.

III-G Fund Balance with Treasury (Coast Guard only)

Background: As noted in comment I-A, *Financial Reporting*, Fund Balance with Treasury (FBWT) at the Coast Guard totaled approximately \$6.3 billion, or approximately 11 percent of total DHS FBWT at September 30, 2011. The majority of these funds represented appropriated amounts that were obligated, but not yet disbursed, as of September 30, 2011. In FY 2010, we reported a material weakness in internal control over FBWT at the Coast Guard. In FY 2011, the Coast Guard corrected several significant FBWT control deficiencies, specifically issues associated with the accuracy and completeness of the SF 224 process. Consequently, we consider the remaining control deficiencies, all of which were reported in our FY 2010 report, to be less severe, but important enough to warrant management's attention.

	2011	2010	2009
USCG			
See page II.2 for table explanation			

Conditions: We noted the following internal control deficiencies associated with FBWT:

Coast Guard:

- Did not properly implement the FBWT monthly activity reconciliation process for two or more of its Agency Location Codes (ALC). Specifically, during a reconciliation of certain ALC's in September, adjustments to the general ledger FBWT were made without performing sufficient research to identify the underlying reconciling items and transactions were reported against the wrong appropriation.
- Does not have a process in place to provide transaction-level supporting documentation for all reconciling items associated with the Government-wide Accounting (GWA) reconciliation. For example, some intragovernmental transactions are recorded solely based on information obtained from the vendor without verification by Coast Guard. As a result, charges are incurred and reported against funds without appropriately verified supporting documentation.



Independent Auditors' Report
Exhibit III – Significant Deficiencies – All DHS Components

- Did not follow existing policies and procedures to ensure that transactions are adequately researched, then applied against the appropriate funding source. Specifically, we noted an instance where transactions were incorrectly applied to the operating expense fund.

Cause/Effect: The Coast Guard has not developed and implemented accounting processes to fully support all reconciling items associated with FBWT activity. Failure to implement timely and effective reconciliation processes could increase the risk of undetected errors and/or violations of appropriation laws, including instances of undiscovered *Anti-deficiency Act* violations or fraud, abuse, and mismanagement of funds, which could lead to inaccurate financial reporting and affect DHS' ability to effectively monitor its budget status.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that the Coast Guard:

1. Perform complete and timely FBWT reconciliations using the Treasury GWA tools. Adequate documentation should be maintained and readily available for all data (e.g., receipts, disbursements, journal entries, etc.) used in the reconciliation process. Documentation should be sufficient to support items at the transactional level, and enable transactions and balances to be reconciled to the general ledger, as appropriate.
2. Implement procedures to ensure that intragovernmental transactions are recorded based on information obtained from the vendor and after verification by Coast Guard; and
3. Ensure existing policies and procedures related to the clearance of transactions are adhered to.

III-H Grants Management (FEMA only)

Background: FEMA is recognized as the primary grant-making component of DHS, managing multiple Federal disaster and non-disaster grant programs.

	2011	2010	2009
FEMA			
See page II.2 for table explanation			

Conditions: We noted the following internal control weaknesses related to grants management at FEMA:

- Does not have sufficient policies and procedures in place to fully comply with the *Single Audit Act Amendments of 1996 (Single Audit Act)* and related OMB Circular No. A-133, *Audits of States, Local Governments, and Nonprofit Organizations (OMB Circular A-133)* (see Comment IV-L, *Single Audit Act Amendments of 1996*).
- Does not maintain accurate and timely documentation related to site visits/desk reviews performed for grantees. Specifically, our control testwork performed over a sample of 71 site visits/desk reviews performed during the nine-month period ended June 30, 2011, identified 11 exceptions related to documentation.
- Does not consistently follow-up with grantees who have failed to submit quarterly financial and/or programmatic reports timely.
- Does not have a process in place to create and track comprehensive lists of FEMA grants that are eligible for close-out.

Cause/Effect: FEMA has not implemented policies and procedures over its grant program in order ensure compliance with the *Single Audit Act* and OMB Circular A-133. In addition, FEMA has not implemented effective monitoring procedures over certain grant activities and the maintenance of related documentation. As a result, misreported grantee expenses may not be detected, which may impact the fair presentation of FEMA's grant accrual balances, undelivered orders, and expenses. Further, the diversity of grant programs and systems within FEMA causes difficulty in assembling a comprehensive status of grants eligible for close-out, which could result in untimely closure of grants and an overstatement of undelivered orders.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.



Independent Auditors' Report
Exhibit III – Significant Deficiencies – All DHS Components

Recommendations: We recommend that FEMA:

1. Implement policies and procedures to ensure full compliance with the *Single Audit Act* and the related OMB Circular No. A-133;
2. Implement monitoring procedures over completing financial site visits, obtaining and reviewing required quarterly grantee reports, and maintaining related documentation; and
3. Develop and implement procedures to create and track comprehensive lists of FEMA grants that are eligible for close-out.

III-I Custodial Revenue and Drawback (CBP Only)

Background: Customs and Border Protection (CBP) collects approximately \$33.9 billion in annual import duties, taxes, and fees on merchandise arriving in the United States from foreign countries (identified below as the Entry Process). Receipts of import duties and related refunds are presented in the statement of custodial activity in the DHS financial statements.

	2011	2010	2009
CBP			
See page II.2 for table explanation			

Drawback is a remittance, in whole or in part, of duties, taxes, or fees previously paid by an importer. Drawback typically occurs when the imported goods on which duties, taxes, or fees have been previously paid, are subsequently exported from the United States or destroyed prior to entering the commerce of the United States.

Our findings over the Entry Process include conditions identified in In-bond, Bonded Warehouse and Foreign Trade Zones. In-bond entries occur when merchandise is transported through one port; however, the merchandise does not officially enter U.S. commerce until it reaches the intended port of destination. Bonded Warehouses (BW) are facilities, under the joint supervision of CBP and the Bonded Warehouse Proprietor, used to store merchandise that has not made entry into the United States commerce. Foreign Trade Zones (FTZ) are secured areas under CBP supervision that are used to manufacture goods that are considered outside of the United States commerce for duty collection.

The conditions cited below have existed for several years; however, through FY 2009 CBP's planned remediation for many of these conditions were tied to systems modernization through the Automated Commercial Environment (ACE). In FY 2010, funding for the implementation of ACE was reduced; therefore, CBP has modified and extended the time-frame for remediation of these conditions.

In previous years, weaknesses in the Trade Compliance Measurement (TCM) program were cited; however, in FY 2010 a module in ACE was implemented and a significant number of TCM deficiencies were remediated in FY 2011. Additionally, conditions surrounding In-bond cited below are expected to be remediated by the final planned ACE deployment in January 2012.

For the remaining conditions in Drawback, BW, and FTZ, a systems fix is currently unfunded. However, improvements have been made in the controls surrounding BW's and FTZ's, specifically at the BW and FTZ facilities. Furthermore, in FY 2010 and FY 2011, CBP began to reassess the Drawback conditions and started an extensive review of the Drawback process as a whole.

Conditions: We noted the following internal control weaknesses related to custodial activities at CBP:

Related to drawback:

- The Automated Commercial System (ACS) lacks the controls necessary to prevent, or detect and correct excessive drawback claims. The programming logic in ACS does not link drawback claims to imports at a detail level. In addition, ACS does not have the capability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries and export documentation upon which the drawback claim is based. Further, ACS has not been configured to restrict drawback claims to 99 percent of each entry summary.



Independent Auditors' Report Exhibit III – Significant Deficiencies – All DHS Components

- Drawback review policies do not require drawback specialists to review all, or a statistically valid sample, of prior drawback claims against a selected import entry to determine whether, in the aggregate, an excessive amount was claimed.

Related to the Entry Process:

- CBP is unable to determine the status of the in-bond shipments and lacks policies and procedures that require monitoring the results of in-bond audits and require the review of overdue air in-bonds. CBP does not formally analyze the rate and types of violations found, to determine the effectiveness of the in-bond program, and does not identify a projected total amount of uncollected duties and fees on in-bond merchandise that has physically entered U.S. commerce without formal entry to ensure there is not a potentially significant loss of revenue.
- In-bond cargo examinations were not performed at some ports in FY 2011 because of the low frequency of in-bond cargo examinations generated by CBP's system that selects in-bond examinations and audits.
- Headquarters has developed national databases which contain an inventory of all BWs and FTZs; however, these databases are not currently used to document the assessed risk of each BW or FTZ, scheduled compliance reviews, or the results of compliance reviews. Annually, CBP headquarters distributes a memo to the ports with the intention of notifying the ports of compliance results; however, the FY 2011 memo provided limited information of the overall findings on the program effectiveness.

Cause/Effect: IT system functionality and outdated IT systems contribute to the weaknesses identified above, in Comment II-B, *Information Technology Controls and Financial System Functionality*. For example, CBP is unable to determine the status of the in-bond shipments with the information available within ACS, and CBP does not have the ability to run an oversight report to determine if ports have completed all required audits. CBP cannot perform a comprehensive analysis to determine the overall compliance rate of the in-bond program. For drawback, much of the process is manual until IT system functionality improvements are made, placing an added burden on limited resources.

The inability to effectively and fully monitor the in-bond process and verify the arrival of in-bond merchandise at the ports could lead to loss of revenue due to uncollected duties and fees on in-bond merchandise that has physically entered U.S. commerce without formal entry.

CBP does not have the ability to perform a complete analysis over the effectiveness of the BW and FTZ programs. CBP headquarters cannot effectively monitor the BW/FTZ program if a complete population of all BWs and FTZs is not compiled. This risk of undetected exceptions to, and deviations from, CBP headquarters guidance cannot be mitigated by the review of the annual port surveys since these surveys cannot be compiled prior to fiscal year-end.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria* behind Exhibit V.

Recommendations: We recommend that CBP:

1. *Related to drawback:*

- a. Since the incorporation of drawback processing is not in the near term schedule for the ACE production, CBP should continue to pursue alternative compensating controls and measures that may ultimately identify the potential revenue loss exposure to CBP. These alternative internal controls over drawback claims may lead to the ability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries and export documentation for which the drawback claim is based, and identify duplicate or excessive drawback claims;
- b. Develop and implement automated controls to prevent overpayment of a drawback claim; and
- c. Analyze current policies and procedures performed at the Drawback Centers. Determine the benefit of current procedures and revise as necessary.



Independent Auditors' Report
Exhibit III – Significant Deficiencies – All DHS Components

2. *Related to the Entry Process:*

- a. CBP headquarters should continue to monitor, perform outreach, and review the in-bond process to ensure a high in-bond compliance rate;
- b. Once a planned new in-bond compliance system is deployed, certain monitoring reports will cease to exist; therefore, CBP should develop and issue formal requirements for all ports to follow under the new system;
- c. Continue the implementation of a national database of BWs and FTZs and develop procedures to ensure completeness of compliance reviews; and
- d. Increase CBP headquarters monitoring over the BW and FTZ compliance review program by developing a method to determine the program's overall effectiveness.

III.6



Independent Auditors' Report
Exhibit IV – Compliance and Other Matters – All DHS Components

All of the compliance and other matters described below are repeat conditions from FY 2010.

IV-J Federal Managers' Financial Integrity Act of 1982 (FMFIA)

Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, requires agencies and Federal managers to: (1) develop and implement internal controls; (2) assess the adequacy of internal controls; (3) separately assess and document internal control over financial reporting; (4) identify needed improvements; (5) take corresponding corrective action; and (6) report annually on internal controls. During fiscal year (FY) 2011 and 2010, the Department of Homeland Security (DHS or Department) developed an annual *Internal Control Playbook* to implement corrective actions and support management assurances by performing tests of design and operating effectiveness of entity level controls and other financial accounting and reporting processes. DHS' implementation of OMB Circular No. A-123 facilitates compliance with the *Federal Managers' Financial Integrity Act of 1982* (FMFIA). The *DHS Financial Accountability Act of 2004* requires DHS to submit an annual audit opinion of internal control over financial reporting. The Secretary of DHS has stated in the Secretary's Assurance Statement dated November 11, 2011, as presented in Management's Discussion and Analysis (MD&A) of the Department's 2011 *Annual Financial Report* (AFR), that based on the material weaknesses identified from the OMB Circular A-123 assessment, the Department provides no assurance that internal control over financial reporting was operating effectively as of September 30, 2011.

While we noted the Department overall has taken positive steps toward full compliance with FMFIA, OMB Circular No. A-123, and the *DHS Financial Accountability Act of 2004*, the Department has not fully established effective systems, processes, policies, and procedures to ensure that internal controls are operating effectively throughout the Department.

Recommendation: We recommend that the Department continue its corrective actions to address internal control deficiencies, in order to ensure full compliance with FMFIA and its OMB- Circular No. A-123 in future years. We also recommend that DHS continue to follow and complete the actions defined in the *Internal Control Playbook*, to ensure that audit recommendations are resolved timely and corrective action plans addressing all DHS audit findings are developed and implemented together with appropriate supervisory review in FY 2012.

IV-K Federal Financial Management Improvement Act of 1996 (FFMIA)

FFMIA Section 803(a) requires that agency Federal financial management systems comply with (1) applicable Federal accounting standards; (2) Federal financial management system requirements; and (3) the United States Government Standard General Ledger (USSGL) at the transaction level. FFMIA emphasizes the need for agencies to have systems that can generate timely, reliable, and useful information with which to make informed decisions to ensure ongoing accountability.

While we noted the Department overall has taken positive steps toward full compliance with FFMIA, the Coast Guard, US Customs and Border Protection, the Federal Emergency Management Agency (FEMA), U.S. Immigration and Customs Enforcement, and Transportation Security Administration did not fully comply with at least one of the requirements of FFMIA. The reasons for noncompliance are reported in Exhibits I, II, and III. The Secretary of DHS has stated in the Secretary's Assurance Statements dated November 11, 2011 that the Department's financial management systems do not substantially conform to government wide requirements mandated by FFMIA. The Department's remedial actions and related timeframes are also presented in the FY 2011 AFR.

An element within FFMIA Federal system requirements is ensuring security over financial management information. This element is addressed further in the *Federal Information Security Management Act of 2002* (FISMA), which was enacted as part of the *E-Government Act of 2002*. FISMA requires the head of each agency to be responsible for (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained and (ii) information systems used or operated; (2) complying with the requirements of the Act and related policies, procedures, standards, and guidelines, including (i) information security standards under the United States Code, Title 40, Section



Independent Auditors' Report
Exhibit IV – Compliance and Other Matters – All DHS Components

11331 and (ii) information security standards and guidelines for national security systems; and (3) ensuring that information security management processes are integrated with agency strategic and operational planning processes.

We noted weaknesses in financial systems security, reported by us in Comments **I-B** and **II-B**, *Information Technology Controls and Financial System Functionality*, which impact the Department's ability to fully comply with FISMA.

Recommendation: We recommend that DHS improve its financial management systems to ensure compliance with the FFMIA, and implement the recommendations provided in Exhibits I, II, and III, in FY 2012.

IV-L Single Audit Act Amendments of 1996 (Single Audit)

FEMA is the only DHS component that has a significant grant making operation. OMB Circular No. A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, requires agencies awarding grants to ensure they receive grantee reports timely and to follow-up on *Single Audit* findings to ensure that grantees take appropriate and timely action. Although FEMA has adopted procedures to monitor grantees and their audit findings, FEMA did not fully comply with provisions in OMB Circular No. A-133 in FY 2011. We noted that FEMA does not always obtain and review grantee *Single Audit* reports in a timely manner, or follow-up on questioned costs and other matters identified in these reports. Because *Single Audits* typically are performed by other entities outside of DHS, procedures related to these reports are not always entirely within the control of DHS and its components.

Recommendations: We recommend that:

1. FEMA further develop and implement procedures to ensure compliance with its policy to obtain and review grantee *Single Audit* reports in a timely manner, and follow-up on questioned costs and other matters identified in these reports. We also recommend that FEMA perform the following in FY 2012:
 - a. Further develop and implement a tracking system to identify each grantee for which a *Single Audit* is required, and the date the audit report is due;
 - b. Use the tracking system to ensure audit reports are received timely, and follow-up when reports are overdue; and
 - c. Perform reviews of grantee audit reports, issue-related management decisions, and ensure that the grantees take appropriate corrective action, on a timely basis.

IV-M Chief Financial Officers Act of 1990

The *DHS Financial Accountability Act of 2004* made DHS subject to the *Chief Financial Officers Act of 1990*, as amended, which requires DHS to submit to the Congress and OMB audited financial statements annually. DHS' Office of the Inspector General (OIG) has engaged an independent auditor to audit the September 30, 2011 balance sheet and related statement of custodial activity. Other financial statements, including the statements of net cost, changes in net position, and budgetary resources, are not currently auditable. DHS must be able to represent that its balance sheet is fairly stated, and obtain at least a qualified opinion before it is practical to extend the audit to other financial statements.

Recommendation: We recommend that DHS and its components continue to implement the Mission Action Plans described in DHS' *Internal Control Playbook* (see Comment **IV – J**, *Federal Managers' Financial Integrity Act of 1982*, above) to remediate the FY 2011 material weaknesses and significant deficiencies, and improve its policies, procedures, and processes, as necessary, to allow management to assert that all financial statements are fairly stated in compliance with accounting principles generally accepted in the United States, and are ready for an independent audit in FY 2012.

IV-N Anti-deficiency Act (ADA)

Various management reviews and OIG investigations are on-going within the Department and its components that may identify ADA violations. The Coast Guard management continues to work to resolve



Independent Auditors' Report
Exhibit IV – Compliance and Other Matters – All DHS Components

four potential ADA violations relating to (1) funds used in advance of an approved apportionment from OMB, (2) funds used for construction and improvement projects, (3) funds that may have been inappropriately administered for modifications to fixed price contracts, and (4) the improper execution of the obligation and disbursement of funds for the lease of passenger vehicles. National Protection and Programs Directorate (NPPD) management is continuing their review, initiated in FY 2007, over the classification and use of certain funds that may identify an ADA violation. The Management Directorate is currently investigating whether rental charges incurred in FY 2009 were not properly committed or obligated.

Recommendations: We recommend that the Department, along with the OIG and the other components, complete the internal reviews currently planned or being performed, and properly report the results in compliance with the ADA, if necessary.

IV-O Government Performance and Results Act of 1993

The *Government Performance and Results Act of 1993* requires each agency to prepare performance plans that include a description of the operational processes, skills and technology, and the resources required to meet the goals, and a description of the means used to verify and validate the measured results. DHS completed the FY 2010 Quadrennial Homeland Security Review (QHSR) for the purpose of developing an updated strategic plan around priorities established by the Secretary. However the Department has not approved a new strategic plan based on the QHSR. Since DHS has not approved its strategic plan, the Statements of Net Cost for the year ended September 30, 2011 and 2010 have not been presented by major program, goals and outputs, and certain related financial statement disclosures, required by OMB Circular No. A-136, *Financial Reporting Requirements* are not complete. In addition, the information included in the FY 2010 Annual Performance Report (published in FY 2011) is aligned with the QHSR but not an approved strategic plan.

Recommendation: We recommend that DHS approve the strategic plan aligned with the QHSR to ensure full compliance with the *Government Performance Results Act of 1993* in FY 2012.



Independent Auditors' Report
Exhibit V – Status of Prior Year Findings

FY 2010 Control Deficiencies As Reported	Summary of Significant Change in FY 2011	FY 2011 Control Deficiencies As Reported
Material Weaknesses:		
<p>A – Financial Management and Reporting (USCG, FEMA, TSA)</p>	<ul style="list-style-type: none"> Department-wide Entity level conditions were substantially corrected. FEMA made progress in correcting financial reporting deficiencies. New financial reporting control weaknesses were identified at USCIS, related to a change in accounting for user fees. The Department filled key accounting positions in FY 2011. The word “Management” was dropped from the title. TSA made progress by hiring accounting personnel, and substantially completing the reconciliation of its balance sheet accounts, but some significant financial reporting control weaknesses remain. USCG corrected some deficiencies and asserted to the accuracy of additional financial statement balances, but some significant financial reporting control weaknesses remain. 	<p>Repeated (Exhibits I-A and II-A) (USCG, TSA, USCIS)</p>
<p>B – Information Technology Controls and Financial Systems Functionality (USCG, CBP, FEMA, USCIS, FLETC, ICE)</p>	<ul style="list-style-type: none"> DHS Civilian Components and USCG made progress in remediation of IT findings we reported in FY 2010. The total number of IT findings reported dropped from 157 in FY 2010 to 135 in FY 2011. Approximately 70 percent of the IT findings reported in FY 2011 are repeated from last year. Approximately 30 percent of our FY 2010 IT findings have been closed. FEMA, USCG, ICE, and FLETC made the most progress in closing IT findings reported in FY 2010. We identified fewer new findings in FY 2011 compared to the number of new findings identified in FY 2010. The majority of these new deficiencies were noted at CBP. Financial systems functionality continues to be a significant contributor to the IT material weakness. 	<p>Repeated (Exhibits I-B and II-B) (USCG, CBP, FEMA, USCIS, ICE)</p>
<p>C – Fund Balance with Treasury (USCG)</p>	<ul style="list-style-type: none"> The Coast Guard corrected several significant FBWT control deficiencies. Consequently, we consider the remaining control deficiencies, all of which were reported in our FY 2010 report, to be less severe, but important enough to warrant management’s attention. 	<p>Partially Repeated (Exhibit III-G) (USCG)</p>
<p>D – Property, Plant, and Equipment (USCG, TSA, CPB)</p>	<ul style="list-style-type: none"> The Coast Guard continued to execute remediation efforts to address PP&E process and control deficiencies, however, remediation efforts are scheduled to occur over a multi-year timeframe beyond FY 2011. Consequently, many of the control weaknesses reported in FY 2010 have been repeated in our FY 2011 report. TSA and CBP continue to have control weaknesses in PP&E, however, control deficiencies at TSA are more severe. New PP&E control weaknesses were identified at MGMT, related to assets that had been inappropriately expensed in prior fiscal years. 	<p>Repeated (Exhibits I-C and II-C) (USCG, TSA, CBP, MGMT)</p>
<p>E – Actuarial and Other Liabilities (USCG, FEMA)</p>	<ul style="list-style-type: none"> The USCG corrected control deficiencies related to actuarial liabilities. Environmental liability control deficiencies at USCG have been repeated in FY 2011. 	<p>Partial Repeat (Exhibits I-D and III-H) (USCG, FEMA)</p>

V.1



Independent Auditors' Report
Exhibit V – Status of Prior Year Findings

	<ul style="list-style-type: none"> Grants management control deficiencies at FEMA are substantially repeated as a separate significant deficiency in FY 2011. 	
F – Budgetary Accounting (USCG, CBP, FEMA)	<ul style="list-style-type: none"> Budgetary accounting control deficiencies at USCG were repeated in FY 2011. FEMA continued to improve its processes and internal controls over the obligation and monitoring process; however, some control deficiencies remain. CBP implemented corrective actions in budgetary accounting processes in FY 2011, and substantially remediated the conditions we reported in FY 2010. 	Partially Repeated (Exhibits I-E and II-E) (USCG, FEMA)
Significant Deficiencies:		
G – Other Entity Level Controls (USCG, CBP, FEMA)	<ul style="list-style-type: none"> The Coast Guard continued to follow the <i>Financial Strategy for Transformation and Audit Readiness</i> (FSTAR) adopted in FY 2009, and has substantially remediated its entity level control deficiencies. CBP substantially corrected its entity level control deficiencies reported in FY 2010. FEMA continued to improve its entity level internal controls however, some control deficiencies reported in FY 2010 remain. New entity level weaknesses were identified at TSA, primarily related to financial reporting infrastructure in operational and program areas. 	Partially Repeated (Exhibit III-F) (FEMA, TSA)
H – Custodial Revenue and Drawback (CBP)	<ul style="list-style-type: none"> Weaknesses reported in FY 2010, and previous years, have been repeated in FY 2011. Financial systems functionality issues reported in Exhibit II-B that require a multi-year effort to address, continue to be a significant cause of these deficiencies. 	Repeated (Exhibit III-I) (CBP)
Compliance and Other Matters:		
I – Federal Managers' Financial Integrity Act of 1952 and Laws and Regulations Supporting OMB Circular No. A-50, <i>Audit Follow-up</i>	<ul style="list-style-type: none"> The Department overall has taken positive steps toward full compliance with FMFLA, OMB Circular No. A-123, and the <i>DHS Financial Accountability Act</i> of 2004, the Department has not fully established effective systems, processes, policies, and procedures to ensure that internal controls are operating effectively throughout the Department. The Department is substantially compliant with OMB Circular No. 50, <i>Audit Follow-up</i>, in FY 2011. 	Partially Repeated (Exhibit IV – J)
J – Federal Financial Management Improvement Act of 1996	<ul style="list-style-type: none"> The Department overall has taken positive steps toward full compliance with FFMIA, the USCG, CBP, FEMA, ICE, and TSA did not fully comply with at least one of the requirements of FFMIA. The reasons for noncompliance are reported in Exhibits I, II, and III. 	Repeated (Exhibit IV – K)
K – Single Audit Act Amendments of 1996	<ul style="list-style-type: none"> FEMA has adopted procedures to monitor grantees and their audit findings, FEMA did not fully comply with provisions in OMB Circular No. A-133 in FY 2011. 	Repeated (Exhibit IV – L)
L – Chief Financial Officers Act of 1990	<ul style="list-style-type: none"> DHS is required to submit to the Congress and OMB audited financial statements annually, however all required financial statements were not auditable in FY 2011. 	Repeated (Exhibit IV – M)

V.2



Independent Auditors' Report

Exhibit V – Status of Prior Year Findings

<i>M – Anti-deficiency Act</i>	<ul style="list-style-type: none">Various management reviews and OIG investigations are on-going within the Department and its components that may identify ADA violations.	Repeated (Exhibit IV – N)
<i>N – Government Performance and Results Act of 1993</i>	<ul style="list-style-type: none">DHS completed the Quadrennial Homeland Security Review (QHSR) for the purpose of developing an updated strategic plan around priorities established by the Secretary. However the Department has not approved a new strategic plan based on the QHSR.	Repeated (Exhibit IV – O)



Department of Homeland Security
Index of Financial Reporting and Internal Control Criteria
(Listed Alphabetically by Criteria Source)

Criteria	Reference	Report Exhibit
CBP Office of Field Operations, Cargo and Conveyance Security's <i>Updated Guidance for Bonded Facilities and Oversight of In-Bond Procedures</i> , dated November 15, 2010		III-F
CBP Personal Property Management Handbook	HB 5200-13B, Chapter 8	II-C
CBP's FY 2011 Personal Property Inventory/Quality Assurance Review		II-C
CBP's Real Property Inventory Procedures		II-C
Coast Guard Financial Accounting and Reporting of Personal Property	Procedures No. 5.3.8.29 and 5.3.8.31	I-C
Coast Guard's "Open Obligation Validation User's Guide"		I-E
Coast Guard PPC's Standard Operating Procedures		I-D
<i>Code of Federal Regulations Title 5</i>	Sections 2634, 2638	III-F
<i>Code of Federal Regulations, Title 19</i>	Sections 18.2(d), 18.6(b), 18.8(b), 19.4, 146.3, and 191.51(b)(1)	III-F
<i>Code of Federal Regulations, Title 44</i>	Part 206	II-E
Compliance Review Handbook for Bonded Warehouses (HB 3500-09, December 2007)		III-F
Compliance Review Handbook for Foreign Trade Zones (HB 3500-10, July 2008)		III-F
DHS Management Directive 0480.1	Section 5	III-F
DHS 4300A Sensitive Systems Handbook	1.0 Introduction	I-B, II-B
DHS Component Requirements Guide for Financial Reporting	Section 42	I-C
DHS Sensitive Systems Policy Directive, 4300A	1.0, 4.0	I-B, II-B, III-F
Disaster Assistance Directorate, Individual Assistance program guidance on CCP		II-E
Disaster Assistance Directorate, Individual Assistance program guidance on DUA		II-E
Ethics Guide to FEMA Employees (July 2010)		III-F
<i>Ethics in Government Act of 1978</i>	Title I, sections 101-104, 106, 107, 109, and 111	III-F
<i>Federal Financial Accounting And Auditing Technical Release 2: Determining Probable and Reasonably Estimable for Environmental Liabilities in the Federal Government</i>		I-D
<i>Federal Financial Management Improvement Act of 1996</i>	Section 803, (a)	I-A, I-C, I-F, II-A, II-C, III-G
	Section 802	I-B, II-B
<i>Federal Information Security Management Act</i>		I-B, II-B
<i>Federal Managers' Financial Integrity Act of 1982</i>	Section 2	II-A, II-C, III-F
FEMA Budget Procedures Memorandum 10-02		II-E
FEMA Directive Number 112-1, Directives Management System		III-F
FEMA Form 90-129		II-E

Index.1



**Department of Homeland Security
Index of Financial Reporting and Internal Control Criteria
(Listed Alphabetically by Criteria Source)**

Criteria	Reference	Report Exhibit
FEMA Instruction 1100.1		III-F
FEMA's SOP for Financial Processing of Mission Assignments, March 17, 2011		II-E
Financial Resource Management Manual, SOP for Recording and Reporting Contingent Legal Liabilities (CG-0945), and the CG-842 Desk Procedures		I-D
<i>Fund Balance with Treasury Reconciliation Procedures, a Supplement to the Treasury Financial Manual, 1 TFM 2-5100</i>	Section V, C Transmittal Letter 588	III-G
<i>GAO's Standards for Internal Control in the Federal Government</i>	Purpose and Anticipated Users of the Manual	I-B
	Control Activities	I-A, I-C, I-D, II-E, III-F, III-H, III-I
	Definition and Objectives	III-F
	Examples of Control Activities (Accurate and Timely Recording of Transactions and Events)	I-E, II-E
	Examples of Control Activities (Appropriate Documentation of Transactions and Internal Control)	I-A, I-C, I-D, II-E, III-F, III-H, III-I
	Monitoring	I-A, I-D, II-A, II-E
	Presentation of the Standards	I-A
<i>GAO's Principles of Federal Appropriations Law</i>	Section 7	I-E
Grants Programs Directorate, Grants Management Division, Grants Policy and Procedures 09-12, Grants Monitoring Policy	Section VII, B, 5	III-H
1 TFM, 2-5100, <i>Reconciling Fund Balance with Treasury Accounts</i>	Appendix 2	III-G
Interpretation of Federal Financial Accounting Standards Interpretation No. 7, Items Held for Remanufacture	Paragraphs 7, 8, 13	I-C
Joint Financial Management Improvement Program (JFMIP), <i>Property Management Systems Requirements</i>	Acquiring / Receiving Property	I-C
Memorandum: In-Bond Guidance, dated April 7, 2010		III-I
Office of Federal Financial Management, Core Financial System Requirements	Accounting Period Maintenance and Closing Process / Audit Trails Process	I-A
Office of Field Operations, <i>Guide for In-Bond Cargo, Version 1.0</i> , March 31, 2006		III-I
OFM <i>Component Requirements Guide for Financial Reporting</i>	Section 18	I-C
<i>Oil Pollution Act of 1990</i>	Section 1002 (a)	I-A
OMB Bulletin No. 07-04, Audit Requirements for Federal Financial Statements	Compliance with FFMIA (Footnote 16)	II-A
OMB Circular No. A-11, <i>Preparation, Submission, and Execution of the Budget</i>	Section 20	I-E
	Section 15.4	II-E
OMB Circular No. A-123, <i>Management's Responsibility for Internal Control</i>	I. Introduction	I-F, II-A, II-C, II-E, III-F, III-I
	II. Establishing Management Controls	II-E

Index 2



Department of Homeland Security
Index of Financial Reporting and Internal Control Criteria
(Listed Alphabetically by Criteria Source)

Criteria	Reference	Report Exhibit
	(Recording and Documentation)	
	II. Standards, Subsection A A. Control Environment	II-A, II-C, II-E, III-F
	II. Standards, Subsection C	I-C, I-D, I-E
	II. Standards, Subsection D	III-F
	II. Standards, Subsection E	I-D
	III. Assessing Internal Control Over Financial Reporting, Subsection E	I-B,
	IV. Assessing Internal Control	I-B, I-E III-I
	Memorandum (3. Policy)	II-A, II-E, III-I
OMB Circular No. A-127, <i>Financial Management Systems</i>	Section 6 (Subsection N); Section 8 (Subpart C)	I-A, I-C
OMB Circular No. A-130, <i>Management of Federal Information Resources</i>	Memorandum (1. Purpose)	I-B, II-B
OMB Circular No. A-133, <i>Audits of States, Local Governments, and Non-Profit Organizations</i> , Revised to show changes published in the Federal Register of June 27, 2003 and June 26, 2007	Subparts B, D	III-H
OMB Circular No. A-136, <i>Financial Reporting Requirements</i>	Section V, Subsection V.1	I-A, II-A
OMB Circular No. A-50, <i>Audit Follow-up</i>	Memorandum	III-H
OMB memorandum M-07-03, <i>Business Rules for Intragovernmental Transactions</i> , dated November 13, 2006		II-A
Single Audit Act Amendments of 1996	Subsections 7502, 7504	III-H
Statement of Federal Financial Accounting Standards (SFFAS) No. 1, <i>Accounting for Selected Assets and Liabilities</i>	Paragraph 77	I-E
	Paragraph 41	II-C
	Paragraph 39	III-G
Statement of Federal Financial Accounting Standards (SFFAS) No. 10, <i>Accounting for Internal Use Software</i>	Executive Summary (Paragraph 5); Paragraphs 16, 20	II-C
Statement of Federal Financial Accounting Standards (SFFAS) No. 14, <i>Amendments to Deferred Maintenance Reporting</i>	Executive Summary, Paragraph 1	I-C
Statement of Federal Financial Accounting Standards (SFFAS) No. 29, <i>Heritage Assets and Stewardship Land</i>	Paragraph 4	I-C
Statement of Federal Financial Accounting Standards (SFFAS) No. 4, <i>Managerial Cost Accounting Concepts and Standards for the Federal Government</i>	Paragraphs 70, 71 [FN 24]	I-A
Statement of Federal Financial Accounting Standards (SFFAS) No. 5, <i>Accounting for Liabilities of the Federal Government</i>	Executive Summary, Paragraphs 30, 31, 38 [FN 27]	II-E
Statement of Federal Financial Accounting Standards (SFFAS) No. 6, <i>Accounting for Property, Plant, and Equipment</i>	Paragraphs 26, 34, 35, 38, 39	I-C, II-C
	Paragraphs 6, 13, 20, 29, 77	I-C



**Department of Homeland Security
Index of Financial Reporting and Internal Control Criteria
(Listed Alphabetically by Criteria Source)**

Criteria	Reference	Report Exhibit
Statement of Federal Financial Accounting Standards (SFFAS) No. 7, <i>Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting</i>	Paragraph 78	I-E
	Paragraph 36	II-A
<i>Treasury Financial Manual</i> , Bulletin 2011-04, <i>Intragovernmental Business Rules</i>	III. Guidance	I-A, II-A
<i>Treasury Financial Manual</i> , Volume 1 <i>T/L 663 Revised by Bulletin No. 2011-08</i>	Part 2, Chapter 4700	I-A, II-A
TSA Personal Property Management Manual	Section 4.3	II-C
<i>U.S. Government Standard General Ledger Fiscal Year 2010 Fiscal Year 2010 Reporting</i>	Supplement Section III. Account Transactions	I-A
<i>US Code Title 31, Chapter 13</i>	Section 1341	I-E
<i>US Code Title 31, Chapter 15</i>	Section 1501, Section 1554.	I-E
<i>US Code Title 44, Chapter 31</i>	Subsection 3101	I-C, I-D



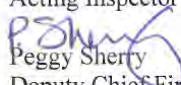
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

November 11, 2011

MEMORANDUM FOR: Charles K. Edwards
Acting Inspector General

FROM: 
Peggy Sherry
Deputy Chief Financial Officer

SUBJECT: Fiscal Year (FY) 2011 Financial and Internal Controls Audit

Thank you for the opportunity to comment on the Independent Public Accountant's audit of our balance sheets, the related statement of custodial activities and internal controls as of September 30, 2011 and 2010. We agree with the Independent Public Accountant's conclusions.

Although the report indicates that DHS still faces financial management challenges, the auditor noted the Department's progress in improving the quality and reliability of our financial reporting. During FY 2011, our Components implemented corrective actions that significantly improved key financial management and internal control areas. This year's qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity demonstrates that the Department is committed to being a responsible steward of taxpayer dollars.

The FY 2011 audit results show that our corrective actions are working, and we are already focusing our efforts on remediating the remaining issues as we prepare for a full-scope audit in FY 2012. I want to thank you for your efforts and the continued dedication by your staff to work collaboratively in addressing our challenges. As we continue our steadfast progress, I look forward to working with the Office of Inspector General and the Independent Public Accountant.



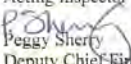
Appendix A Management's Response

U.S. Department of Homeland Security
Washington, DC 20528



November 11, 2011

MEMORANDUM FOR: Charles K. Edwards
Acting Inspector General

FROM: 
Peggy Sherry
Deputy Chief Financial Officer

SUBJECT: Fiscal Year (FY) 2011 Financial and Internal Controls Audit

Thank you for the opportunity to comment on the Independent Public Accountant's audit of our balance sheets, the related statement of custodial activities and internal controls as of September 30, 2011 and 2010. We agree with the Independent Public Accountant's conclusions.

Although the report indicates that DHS still faces financial management challenges, the auditor noted the Department's progress in improving the quality and reliability of our financial reporting. During FY 2011, our Components implemented corrective actions that significantly improved key financial management and internal control areas. This year's qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity demonstrates that the Department is committed to being a responsible steward of taxpayer dollars.

The FY 2011 audit results show that our corrective actions are working, and we are already focusing our efforts on remediating the remaining issues as we prepare for a full-scope audit in FY 2012. I want to thank you for your efforts and the continued dedication by your staff to work collaboratively in addressing our challenges. As we continue our steadfast progress, I look forward to working with the Office of Inspector General and the Independent Public Accountant.



Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Acting Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees,
as appropriate



ADDITIONAL INFORMATION AND COPIES

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

OIG HOTLINE

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

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

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



Other Accompanying Information

The *Other Accompanying Information* section contains information on Tax Burden/Tax Gap, Summary of Financial Statement Audit and Management Assurances, Improper Payments Act, and Other Key Regulatory Requirements. Also included in this section is the OIG Report on the Major Management Challenges Facing the Department of Homeland Security, followed by Management's Response.

Unaudited, see accompanying Auditors' Report



Tax Burden/Tax Gap

Revenue Gap

The Entry Summary of Trade Compliance Measurement (TCM) program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations, and agreements, and is used to produce a dollar amount for estimated net under-collections, and a percent of revenue gap. The revenue gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and trade agreements using a statistically valid sample of the revenue losses and overpayments detected during TCM entry summary reviews conducted throughout the year.

For FY 2010 and 2009, the estimated revenue gap was \$238 and \$285 million, respectively. CBP calculated the preliminary FY 2011 estimated revenue gap to be \$331 million. As a percentage, the preliminary revenue gap for FY 2011 was 0.88 percent of all collectable revenue for the year. The estimated over-collection and under-collection amounts due to noncompliance for FY 2011 and FY 2010 were \$71 million and \$401 million and \$123 million and \$361 million, respectively. The overall trade compliance rates for FY 2010 and FY 2009 were 98.63 percent and 98.2 percent respectively. The preliminary overall compliance rate for FY 2011 is 97.6 percent.

The final overall trade compliance rate and estimated revenue gap for FY 2011 will be issued in February 2012.



Summary of Financial Statement Audit and Management Assurances

Table 1 and Table 2 below provide a summary of the financial statement audit and management assurances for FY 2011.

Table 1. FY 2011 Summary of the Financial Statement Integrated Audit Results

Audit Opinion	Qualified				
Restatement	No				
Material Weakness	Beginning Balance	New	Resolved	Consolidated	Ending Balance
Financial Reporting	1				1
IT Controls and System Functionality	1				1
Fund Balance with Treasury	1		✓		0
Property, Plant, & Equipment	1				1
Environmental and Other Liabilities	1				1
Budgetary Accounting	1				1
Total Material Weaknesses	6	0	(1)	0	5

In FY 2011, the Independent Auditor's Report on the integrated financial statement audit identified five material weakness conditions at the Department level. Corrective actions were implemented by management, which resulted in several conditions at the Department level being reduced in severity or resolved from the prior year. Fund Balance with Treasury at U.S. Coast Guard and Grants Management at FEMA were reduced to significant deficiencies; Financial Reporting at FEMA was resolved; IT Controls and System Functionality was resolved at FLETC and reduced in severity at ICE; Budgetary Accounting at CBP was resolved; and Actuarial Liabilities at U.S. Coast Guard was resolved, and the material weakness was reduced in scope and re-titled as Environmental and Other Liabilities.



Table 2. FY 2011 Summary of Management Assurances

Effectiveness of Internal Control Over Financial Reporting (FMFIA Section 2)						
Statement of Assurance	No Assurance					
Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Financial Reporting at USCG	1					1
Financial Systems at USCG and FEMA	1					1
Fund Balances with Treasury at USCG	1				✓	0
Property Management at USCG and TSA	1					1
Environmental and Other Liabilities at USCG	0	✓				1
Budgetary Resource Management at USCG	1					1
Total Material Weaknesses	5	1	0	0	(1)	5
Effectiveness of Internal Controls over Operations (FMFIA Section 2)						
Statement of Assurance	Qualified					
Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Property Management at DHS and TSA	1				✓	0
Financial Assistance Awards Policy and Oversight at DHS and FEMA	1					1
Acquisition Management at DHS	1					1
Funds Control at USCG, ICE, and USSS	1					1
Entity Level Controls at NPPD	0	✓				1
Total Material Weaknesses	4	1	0	0	(1)	4
Conformance with financial management systems requirements (FMFIA Section 4)						
Statement of Assurance	Systems do not conform to financial management systems requirements					
Non-Conformances	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Federal Financial Management Systems Requirements, including Financial Systems Security and Integrated Financial Management Systems	1					1
Noncompliance with the U.S. Standard General Ledger	1					1
Federal Accounting Standards	1					1
Total Non-conformances	3	0	0	0	0	3
Compliance with Federal Financial Management Improvement Act (FFMIA)				DHS	Auditor	
Overall Substantial Compliance				No	No	
1. System Requirements					No	
2. Accounting Standards					No	
3. USSGL at Transaction Level					No	

In FY 2011, DHS renamed the previously reported Financial Reporting and Other Liabilities material weakness to better align with the title used by the Independent Auditors. As such, Environmental and Other Liabilities was added as a new title in FY 2011.

Effectiveness of Internal Control Over Financial Reporting

Pursuant to the *Department of Homeland Security Financial Accountability Act (FAA)*, the Department has focused its efforts on evaluating corrective actions to assess whether previously reported material weaknesses continue to exist. In cases where material weaknesses continue to exist, the Department focused on identifying significant financial reporting areas where assurance can be provided and developed interim compensating measures to support the Secretary’s commitment to obtain a balance sheet opinion. Since FY 2005 DHS has reduced audit qualifications from 10 to 1 and material weaknesses by half. For the sixth consecutive year, we have made tremendous progress in strengthening Department-wide internal controls over financial reporting, as evidenced by the following FY 2011 achievements:

- The U.S. Coast Guard successfully executed the FY 2011 *Financial Strategy for Transformation and Audit Readiness*, providing financial reporting assertions to support the Department’s Consolidated Balance Sheet. In addition, U.S. Coast Guard corrective actions significantly reduced risk related to financial scripts and Fund Balance with Treasury



reconciliations. Most significantly, the U.S. Coast Guard corrected a longstanding entity level control deficiency based on the Commandant’s leadership to set the tone at the top and delegation of responsibility for internal control from senior management to all financial management staff levels and across business lines of the U.S. Coast Guard enterprise.

- The Offices of the Chief Financial Officer and Chief Information Security Officer partnered to provide direct assistance to Components in executing financial system security corrective actions and performing validation and verification procedures, resulting in a significant deficiency correction at FLETC, a material weakness downgrade at ICE, and substantial risk reductions of system security vulnerabilities at FEMA and scripting risks at U.S. Coast Guard.
- FEMA executed corrective actions to correct a Financial Reporting significant deficiency by implementing processes and controls to support account balances and adjustments, including improving financial disclosure procedures.
- CBP implemented corrective actions to correct a significant deficiency in budgetary accounting by implementing controls to improve the timeliness of undelivered orders deobligations.

Significant internal control challenges remain at the U.S. Coast Guard, FEMA, and TSA. To support these Components, the Department’s Deputy Chief Financial Officer conducts weekly risk management meetings with Senior Management and Staff. Table 3 below summarizes financial statement audit material weaknesses in internal controls as well as planned corrective actions with estimated target correction dates.

Table 3. FY 2011 Internal Control Over Financial Reporting Corrective Actions

Material Weakness	Component	Year Identified	Target Correction Date
	USCG	FY 2003	FY 2012
Financial Reporting	U.S. Coast Guard has not established an effective financial reporting process due to the lack of integrated financial processes and systems. In addition, significant deficiencies were identified at TSA, which contribute to the overall material weakness.		
Corrective Actions	The DHS OCFO will continue to support U.S. Coast Guard and TSA in implementing corrective actions to establish effective financial reporting control activities.		

Material Weakness	Component	Year Identified	Target Correction Date
	USCG and FEMA	FY 2003	FY 2012
IT Controls and System Functionality	The Department’s Independent Public Auditor has identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to inherited control deficiencies surrounding general computer and application controls. In addition, significant deficiencies were identified at CBP, ICE, and USCIS, which contribute to the overall material weakness. The <i>Federal Information Security Management Act</i> mandates that federal agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance. In addition, the Department’s financial systems do not conform to the <i>Federal Financial Management Improvement Act</i> .		



Corrective Actions	The DHS OCFO and OCIO will support the U.S. Coast Guard, FEMA, and other Components to design and implement internal controls in accordance with DHS 4300A, Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Financial Systems. In addition, the Department will continue to move forward with financial system modernization.
---------------------------	---

Material Weakness	Component	Year Identified	Target Correction Date
	USCG and TSA	FY 2003	FY 2012
Property, Plant, and Equipment	The controls and related processes surrounding U.S. Coast Guard and TSA Property, Plant, and Equipment (PP&E) to accurately and consistently record activity are either not in place or contain errors and omissions. In addition, significant deficiencies were identified at CBP and MGMT, which contribute to the overall material weakness.		
Corrective Actions	U.S. Coast Guard will implement policies and procedures to support completeness, existence, and valuation assertions for PP&E. The DHS OCFO will continue efforts to support U.S. Coast Guard and TSA implementing corrective actions to address capital asset conditions and develop policies and procedures to establish effective financial reporting control activities.		

Material Weakness	Component	Year Identified	Target Correction Date
	USCG	FY 2006	FY 2012
Environmental and Other Liabilities	U.S. Coast Guard did not have policies and procedures to fully support the completeness, existence, and accuracy assertions of data used in developing environmental liability estimates.		
Corrective Actions	Corrective actions for environmental liabilities will be taken in coordination with PP&E corrective actions to develop a complete population of locations where environmental liabilities exist.		

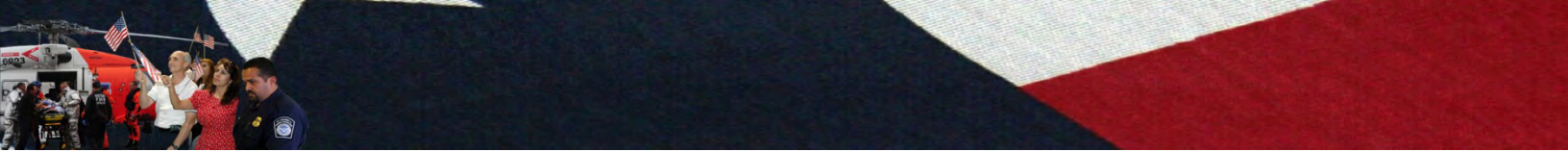
Material Weakness	Component	Year Identified	Target Correction Date
	USCG	FY 2004	FY 2012
Budget Resource Management	U.S. Coast Guard policies and procedures over obligations, disbursements, and validation and verification of undelivered orders for accurate recording of accounts payable were not effective. In addition, significant deficiencies were identified at CBP and FEMA, which contribute to the overall material weakness.		
Corrective Actions	Use lessons learned in FY 2011 from the Audit Command Language to develop corrective actions for budgetary accounts.		



Effectiveness of Internal Control Over Operations

The DHS Management Directorate is dedicated to ensuring that Departmental offices and Components perform as an integrated and cohesive organization, focused on the Department's frontline operations to lead efforts to achieve a safe, secure, and resilient homeland. Critical to this mission is a strong internal control structure. As we strengthen and unify DHS operations and management, we will continually assess and evaluate internal controls to ensure the effectiveness and efficiency of operations and compliance with laws and regulations. For the sixth consecutive year, we have made tremendous progress in strengthening Department-wide internal controls over operations, as evidenced by the following FY 2011 achievements:

- Supported the Deputy Secretary with the “Improving the Health of DHS Financial Assistance” initiative to establish a unified financial assistance line of business. An Executive Steering Committee was also established to create five working groups to improve audits and assessments, program development and implementation, programmatic goals and objectives, reporting and post-award administration, and financial assistance program requirements.
- Strengthened internal controls over government charge cards by establishing a Bankcard Assessment Team to prevent waste, fraud, and abuse of resources. The Bankcard Assessment Team implemented and actively monitored the effectiveness of these controls to ensure government charge card programs and operations are instilled with the highest level of integrity and accountability. Internal control assessments are currently under way to baseline government charge card processes and controls. These assessments will help to better define the roles and responsibilities of cardholders, program officials, management, and those charged with coordinating charge card activities.
- Received a grade of “A” from the Small Business Administration for our success in contract awards. Achieved a competition rate of 67 percent, exceeding the goal of 60 percent. Conducted oversight reviews at three Components as well as six DHS-wide special reviews and three Component-specific special reviews, resulting in performance improvement opportunities and identification of best practices. Updated the Homeland Security Acquisition Manual to reflect new regulatory and policy requirements.
- Graduated 30 contracting employees from the Acquisition Professional Career Program, resulting in 191 active employees in the Acquisition Professional Career Program as of September 30, 2011. There were 3,020 acquisition certifications issued and 6,734 individuals trained across 319 classes in 61 different acquisition courses.
- Conducted in-depth technical reviews for 20 percent of the Department's IT systems to assess quality assurance and validate compliance with DHS security requirements. The Office of the Chief Information Security Office conducts rotating assessments over a five year schedule to achieve 100 percent coverage of the Department's IT systems.
- Increased the level of IT program and portfolio governance across the Department by establishing seven program Executive Steering Committees (ESCs) and five Domain ESCs, executing annual Portfolio Reviews in support of the OCFO FY 2013 Program Review Board, and conducting four Departmental TechStat reviews and 25 Accelerated TechStats in support of OMB's 25 Point Plan.
- Migrated the Email Security Gateway to each DHS enterprise data center and discontinued Directory Services Exchange Services at the Operations Support Center in Martinsburg, West Virginia.



- Achieved internal control program efficiencies by leveraging enterprise-wide business processes documentation project that was initiated and completed in FY 2011 and led by the Chief Administrative Officer's Records Management Program Division.
- Made substantial improvements to Office of the Chief Administrative Officer (OCAO)-wide communications and information delivery processes through the development and implementation of a comprehensive website plan. In addition, the OCAO successfully established improved communications across DHS-wide Administrative Service groups.
- Successfully implemented five out of seven of the President's Hiring Reform Initiatives and will continue to simplify the hiring process to increase efficiencies and increase the quality of candidates. Training of hiring managers is a significant element of the DHS hiring reform action plan, and we will continue to train, engage, and hold all hiring managers accountable for the effective and efficient hiring of talented individuals.
- Coordinated a collaborative process to develop a new DHS Coordinated Recruiting and Outreach Strategy, which is currently in the review process. This streamlined approach will leverage recruiting assets from around the country and will strengthen the unity of the DHS brand. Moreover, recruiting efforts will target all underrepresented groups, including individuals with disabilities and veterans.
- Developed a comprehensive Leader Development framework relevant for all levels of employees. For example, the Cornerstone program, a top priority for the Deputy Secretary, provides a single framework of requirements for the development of some 27,000 supervisors across the Department, and encompasses pre-supervisory awareness, supervisor onboarding, 40 hours of development during the first 11 months of appointment, and an annual requirement to give back 12 hours in "leader as teacher" activity.
- Surpassed the target of 3,500 contractor conversions through Balanced Workforce Strategy activity and launched a related Strategic Workforce Planning model. Elements of the new model include: revalidated Mission Critical Occupations (MCOs) aligned with each major DHS mission articulated in the Quadrennial Homeland Security Review (QHSR); a prototype of human capital indicators linked to MCOs, to be piloted and evaluated in FY 2012 as a means for assessing basic risk to mission accomplishment; and a general framework for validating and measuring competencies for the Department's MCOs, which will be evaluated and implemented in FY 2012.
- The DHS HSPD-12 Program, under the direction of the Office of the Chief Security Officer, has fostered greater collaboration and opportunities for improving how DHS handles employee identification information through all business processes. Accomplishments included: issuing a cumulative total of 262,881 Personal Identity Verification cards to DHS employees and contractors and deploying Personal Identity Verification card issuance workstations to more than 650 DHS locations in support of card issuance surge activities.

To address challenges to internal control over operations, the Department's Under Secretary for Management conducts quarterly Internal Progress Review oversight meetings. Table 4 summarizes material weaknesses in internal control over operations as well as planned corrective actions with estimated target correction dates.



Table 4. FY 2011 Internal Control Over Operations Corrective Actions

Material Weakness	Component	Year Identified	Target Correction Date
	DHS and FEMA	FY 2008	FY 2014
Financial Assistance Awards Policy and Oversight	There are four basic conditions affecting stewardship of federal assistance funding across DHS: (1) the lack of published department-wide financial assistance policy to guide Components' and Awardees' actions; (2) the lack of Component oversight and monitoring to ensure their adherence to such policy; (3) the lack of Office of the Inspector General and DHS Management actions to resolve and close annual awardee audit findings; and (4) the lack of basic information regarding how DHS goes about conducting its financial assistance line of business, including identification of high areas of risk and gaps in key controls; in established areas of responsibility, business models; and systems and efficient and effective operations.		
Corrective Actions	The Deputy Secretary has formed an Executive Steering Committee to oversee corrective actions with audits and assessments, program development and implementation, programmatic goals and objectives, reporting and post-award administration, and requirements for financial assistance programs.		

Material Weakness	Component	Year Identified	Target Correction Date
	DHS	FY 2008	FY 2012
Acquisition Management	There are six conditions affecting acquisition management at DHS: (1) inability to effectively achieve proper organizational alignment from achieving mission; (2) systems oversight and accountability within the acquisition function which has improved, but is still not sufficient; (3) investment decision models need to be strengthened to better manage risks to ensure programs meet needed mission capabilities and are delivered within cost, benefit, and schedule considerations; (4) program cost growth and the inadequacy of the cost-estimating process at DHS; (5) gaps identified in an acquisition workforce survey; and (6) use of suspension and debarment actions for poorly performing contractors.		
Corrective Actions	To improve organizational alignment, DHS developed a Management Directive that recognizes the Under Secretary for Management as the Chief Acquisition Officer. In addition, DHS is working to improve the effectiveness of the acquisition lifecycle and provide better linkages between requirements development, resource allocation, procurement, and program management, with S&T as a full partner to the Management Directorate. S&T will continue to play a key role in each phase of the acquisition life cycle, especially in the earliest phases of concept development through program execution. S&T will evaluate new and emerging technologies to address capability gaps, which ultimately enhances department-wide technology expertise and assists the department in making better technology decisions.		



Material Weakness	Component	Year Identified	Target Correction Date
		USCG, ICE, and USSS	FY 2006
Funds Control	U.S. Coast Guard repeated the prior year Antideficiency Act (ADA) controls material weakness. ICE made progress against prior-year conditions by developing an Administrative Control of Funds Directive; however, additional work is needed to implement the Directive across ICE program offices. Finally, USSS has not completely implemented funds control policies and procedures to address prior-year ADA violations reported by GAO.		
Corrective Actions	U.S. Coast Guard is developing enterprise-wide policies and procedures for assessing ADA risks, testing effectiveness of controls, and monitoring to fully implement DHS policy. ICE plans to conduct verification and validation procedures to ensure their Administrative Control of Funds Directive is effectively implemented. USSS will complete implementation of policies and procedures regarding the administrative control of funds.		

Material Weakness	Component	Year Identified	Target Correction Date
		NPPD	FY 2011
Entity Level Control at NPPD	NPPD has recently undergone major organizational change with new responsibilities, reorganization, and expansion of programs. NPPD Component management does not always address indicators of problems or manage risks to ensure top management is aware of actions taken or needed at components of the NPPD organization. The organization structure is inefficient, and it is difficult to determine the organizations or individuals that control parts of NPPD management functions.		
Corrective Actions	NPPD will implement corrective actions to improve its control environment.		



Improper Payments Information Act

The *Improper Payments Information Act (IPIA) of 2002* (Pub. L. 107-300) requires agencies to review their programs and activities to identify those susceptible to significant improper payments. The IPIA was amended on July 22, 2010, by the *Improper Payments Elimination and Recovery Act (IPERA) of 2010* (Pub. L. 111-204). IPERA strengthened the requirement for government agencies to carry out cost-effective programs for identifying and recovering overpayments made to contractors, also known as “recovery auditing.” OMB has established specific reporting requirements for agencies with programs that possess a significant risk of improper payments and for reporting on the results of recovery auditing activities. As noted below, DHS will implement corrective action plans for all programs with estimated improper error amounts above \$10 million. Key achievements for FY 2011 include: a reduction in estimated improper payments for FEMA’s high-risk programs; targeted recovery audit contract work examining telecommunications payments, which identified significant improper payments eligible for recoupment and cost savings opportunities; and a 94 percent cumulative recoupment rate for high-dollar overpayments identified in the Secretary’s quarterly report to the DHS OIG, OMB, and the public. In the tables which follow, all table amounts are rounded to the nearest whole dollar.

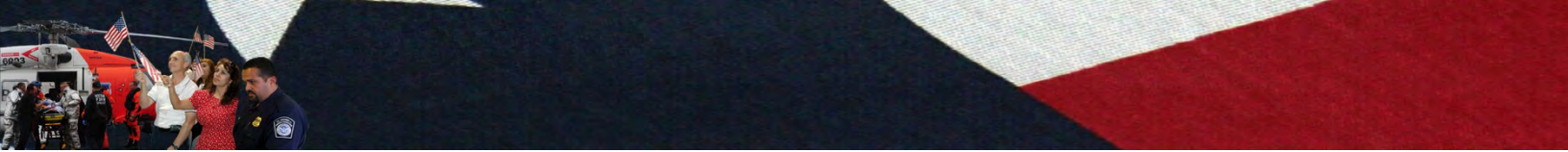
I. Risk Assessments

In FY 2011, DHS conducted risk assessments on 96 DHS programs, totaling \$53 billion in FY 2010 disbursements. We completed risk assessments for all programs unless total disbursements were less than \$10 million or testing was required based on prior years results. We assessed all payment types except for federal intragovernmental payments which were excluded based on changes to the definition of an improper payment contained in IPERA and as listed in the resulting OMB implementing guidance and government charge card payments which are separately tested under OMB Circular A-123 Appendix B, *Improving the Management of Government Charge Card Programs*. Agencies were also given the option of excluding payroll payments. This option was exercised at one Component.

Improper payment estimates in this section are based on statistical estimates for FY 2010 payments. These estimates are then projected for FY 2011 and beyond based on the timing and significance of improvements expected from completing corrective actions.

The susceptibility of programs making significant improper payments was determined by qualitative and quantitative factors. These factors included:

- Payment Processing Controls – Management’s implementation of internal controls over payment processes, including existence of current documentation, the assessment of design and operating effectiveness of internal controls over payments, the identification of deficiencies related to payment processes and whether or not effective compensating controls are present, and the results of prior IPIA payment sample testing.
- Quality of Internal Monitoring Controls – Periodic internal program reviews to determine if payments are made properly. Strength of documentation requirements and standards to support test of design and operating effectiveness for key payment controls. Presence or absence of compensating controls.



- Human Capital – Experience, training, and size of payment staff. Ability of staff to handle peak payment requirements. Level of management oversight and monitoring against fraudulent activity.
- Complexity of Program – Time program has been operating. Complexity and variability of interpreting and applying laws, regulations, and standards required of the program.
- Nature of Payments and Recipients – Type, volume, and size of payments. Length of payment period. Quality of recipient financial infrastructure and procedures. Recipient experience with federal award requirements.
- Operating Environment – Existence of factors that necessitate or allow for loosening of financial controls. Any known instances of fraud. Management’s experience with designing and implementing compensating controls.
- Additional Grant Programs Factors – Federal Audit Clearinghouse information on quality of controls within grant recipients. Identification of deficiencies or history of improper payments within recipients. Type and size of program recipients and sub-recipients. Maturity of recipients’ financial infrastructure, experience with administering federal payments, number of vendors being paid, and number of layers of sub-grantees.

A weighted average of these qualitative factors was calculated. This figure was then weighted with the size of the payment population to calculate an overall risk score.

Based on this year’s assessment process, the following programs were deemed to be vulnerable to significant improper payments:

Table 5. Programs at High-Risk for Improper Payments Based on FY 2011 Risk Assessments and Prior Year Payment Sample Testing

Component	Program Name	FY 2011 Disbursements (Based on FY 2010 Actual Data) (\$ Millions)
CBP	Border Security Fencing	\$251
	Custodial – Refund & Drawback	\$1,198
FEMA ¹	Disaster Relief Program – Individuals and Households Program (IHP)	\$679
	Disaster Relief Program – Vendor Payments	\$582
	Insurance – National Flood Insurance Program (NFIP)	\$1,085
	Grants – Public Assistance Programs (PA)	\$3,532
	Grants – Homeland Security Grant Program (HSGP)	\$1,516
	Grants – Assistance to Firefighters Grants (AFG)	\$385
	Grants – Emergency Food and Shelter Program (EFSP)	\$201
	Grants – Transit Security Grants Program (TSGP)	\$109
ICE ²	Enforcement and Removal Operations (ERO)	\$1,332
NPPD ³	Federal Protective Service (FPS)	\$811
TSA	Aviation Security – Payroll	\$2,458
USCG	Active Duty Military Payroll (ADMP)	\$2,918
Total Disbursements		\$17,057

Notes:

1. All FEMA disbursement totals are national figures. Selected states and territories were tested for the state-administered programs HSGP, PA, TSGP. See Table 6 for a listing of states and territories tested for these programs.
2. ERO was listed as Detention and Removal Operations (DRO) in the FY 2010 DHS Annual Financial Report. Only the non-payroll portion of this program was found to be high-risk. Disbursement figures are for non-payroll disbursements.



3. FPS transferred from ICE to NPPD in FY 2010. The Office of Management and Budget IPERA implementing guidance allowed agencies the option of excluding payroll payments. This option was invoked for the FPS program. Consequently, the disbursement total listed excludes payroll payments.

II. Statistical Sampling

For FY 2011 reporting, a stratified sampling design was used to test payments based on FY 2010 disbursement amounts and the assessed risk of the program. The design of the statistical sample plans and the extrapolation of sample errors across the payment populations were completed by a statistician under contract.

Sampling plans provided an overall estimate of the percentage of improper payment dollars within +/-2.5 percent precision at the 90 percent confidence level, as specified by OMB M-03-13 guidance. An expected error rate of 3 to 10 percent of total payment dollars was used in the sample size calculation.

Using a stratified random sampling approach, payments were grouped into mutually exclusive “strata,” or groups based on total dollars. A stratified random sample typically required a smaller sample size than a simple random sample to meet the specified precision goal at any confidence level. Once the overall sample size was determined, the individual sample size per stratum was determined using the Neyman Allocation method.

The following procedure describes the sample selection process:

- Grouped payments into mutually exclusive strata;
- Assigned each payment a randomly number generated using a seed;
- Sorted the population by stratum and random number within stratum; and
- Selected the number of payments within each stratum (by ordered random numbers) following the sample size design. For the certainty strata, all payments are selected.

To estimate improper payment dollars for the population from the sample data, the stratum-specific ratio of improper dollars (gross, underpayments, and overpayments, separately) to total payment dollars was calculated.

DHS sample test results are listed in Table 6.



Table 6. DHS Sample Test Results

Component	Program	FY 2011 Payment Population (Based on FY 2010 Actual Data) (\$ millions)	FY 2011 Sample Size (Based on FY 2010 Actual Data) (\$ millions)	FY 2011 Est. Error Amount (Based on FY 2010 Actual Data) (\$ millions)	FY 2011 Est. Error Percentage (Based on FY 2010 Actual Data) (%)
CBP	Border Security Fencing	\$251	\$202	\$0	0.01%
	Refund & Drawback	\$1,198	\$91	\$3	0.28%
FEMA	Disaster Relief Program – Individuals and Households Program (IHP)	\$679	\$2	\$2	0.31%
	Disaster Relief Program – Vendor Payments	\$582	\$222	\$17	2.87%
	Insurance – National Flood Insurance Program (NFIP)	\$1,085	\$39	\$13	1.21%
	Grants – Public Assistance Programs (PA) ¹	\$238	\$109	\$0	0.32%
	Grants – Homeland Security Grant Program (HSGP) ²	\$510	\$225	\$1	0.34%
	Grants – Assistance to Firefighters Grants (AFG)	\$385	\$57	\$20	5.09%
	Grants – Transit Security Grants Program (TSGP) ³	\$40	\$22	\$0	0.68%
	Grants – Emergency Food and Shelter Program (EFSP)	\$201	\$34	\$15	7.64%
ICE	Enforcement and Removal Operations (ERO)	\$1,332	\$319	\$108	8.12%
NPPD	Federal Protective Service	\$811	\$131	\$27	3.27%
TSA	Aviation Security – Payroll	\$2,458	\$1	\$0	0.01%
USCG	Operating Expenses - Active Duty Military Payroll	\$2,918	\$6	\$4	0.13%
DHS	All Programs⁴	\$12,688	\$1,460	\$210	1.66%⁵
DHS	High-Risk Programs	\$4,396	\$802	\$200	4.55%⁵

Notes:

1. Sample testing of the Public Assistance Program was done in two stages covering seven states (AK, MA, MD, ME, PA, WA, and WY) and Puerto Rico. These states and territory paid out \$238 million out of a national total of \$3,532 million. The totals in the table are the stage two payment populations for the states and territory tested. See Table 11 Improper Payment Reduction Outlook for the national estimated error of \$11 million.
2. Sample testing of the Homeland Security Grant Program was done in two stages covering 17 states (AL, HI, IA, ID, IL, IN, KS, ND, NY, OK, RI, SC, TN, VA, WI, WV, and WY). These states paid out \$510 million out of a national total of \$1,516 million. The totals in the table are the stage two payment populations for the states tested. See Table 11 Improper Payment Reduction Outlook for the national estimated error of \$5 million.
3. Sample testing of the Transit Security Grant Program was done in two stages covering nine states (AZ, DE, GA, IN, KY, LA, NY, TN, and WI). These regions paid out \$40 million out of a national total of \$109 million. The totals in the table are the stage two payment populations for the nine regions. See Table 11 Improper Payment Reduction Outlook for the national estimated error of \$1 million.
4. Program total of \$12,668 in this table differs from \$17,057 total in Table 11 Improper Payment Reduction Outlook. For state-administered grant programs, the table above lists the population totals for the states tested, while Table 11 Improper Payment Reduction Outlook lists the national payment populations.
5. Percentage figures based on cumulative totals.

Several programs considered at high risk based on risk assessment grading were not confirmed as high risk based on sample test results. The main reason for the estimated error rates falling below \$10 million for these programs was the presence of strong compensating controls such as additional levels of payment review for manually intensive processes.



Based on the results of sample testing, corrective action plans are required for the following seven programs due to national estimated error amounts above \$10 million:

- FEMA’s Assistance to Firefighters Grants.
- FEMA’s Disaster Relief Program - Vendor Payments.
- FEMA’s Emergency Food and Shelter Program.
- FEMA’s National Flood Insurance Program.
- FEMA’s Public Assistance Program.
- ICE’s Enforcement and Removal Operations Program.
- NPPD’s Federal Protective Service Program.

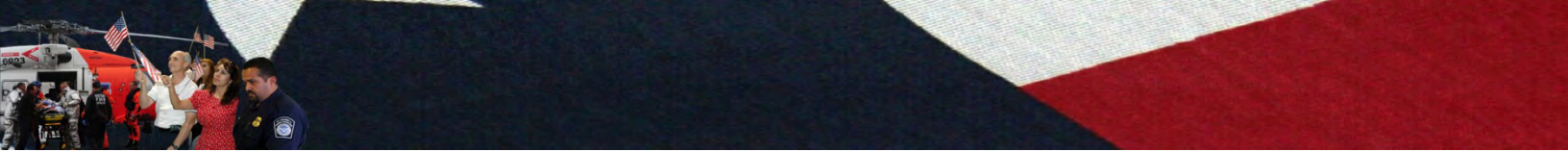
III. Corrective Actions

The following tables list corrective actions for programs with estimated improper error amounts above \$10 million. These corrective actions are targeted at addressing the root causes behind administrative and documentation errors caused by the absence of the supporting documentation necessary to verify the accuracy of the claim; or inputting, classifying, or processing applications or payments incorrectly by DHS, a state agency, or a third party who is not the beneficiary. Authentication and medical necessity errors and verification errors were either not identified or were immaterial to the estimated error rates and amounts of DHS high-risk programs.

Corrective Action Plans for FEMA High-Risk Programs

Table 7. Planned Assistance to Firefighters Grant Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect Information on Application		
1. Failure to Provide Accurate Information on Application	1. Update AFG Program Guidance and tutorials to instruct potential applicants to register in the National Fire Incident Reporting System and provide required information in support of their grant application.	March 2012
	2. Perform additional grantee outreach and direct applicants to include their Fire Department Identification Number as part of their grant application.	May 2012
Category of Error: Purchase Outside Allowable Timeframe		
1. Purchase Made Outside the Period of Performance	1. Conduct semi-annual grantee outreach and include language in the correspondence reminding grantees to monitor their disbursement progress as it relates to their respective grant’s period of performance.	March 2012
	2. Develop and deliver training for program staff to include a notification in Comments section in the AFG system when reviewing payments during or after the tenth month of a grantee’s period of performance.	March 2012



Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Unallowable Use of Excess Funds		
1. Use of Excess Funds without Supporting Amendment or to Purchase Ineligible Goods and/or Services	1. Require each applicant to complete the <i>AFG Grant Management Tutorial</i> that is currently available on the AFG Program website.	March 2012
Category of Error: Insufficient Documentation		
1. Failure to Submit Supporting Documentation	1. Develop grantee documentation organization and retention guidance and offer associated record keeping training.	March 2012
	2. Develop a plan that outlines procedures for conducting annual audits of grantee supporting documentation.	May 2012

Table 8. Planned Disaster Relief Fund Vendor Payments Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Policies to Prevent Improper Payments		
1. Acquisition manual needs to be strengthened	1. Update acquisition manual to include a chapter on procurement roles and responsibilities for contract payments. Specific points to include: contracting officer delegations; invoice requirements including reviews against regulations, contract terms and conditions; requirements for adequate supporting documentation; procedures for establishing billing rates; and a description of billing mechanisms required for different contract types.	March 2012
	2. Revise acquisition manual sections on standard billing language, procedures for product substitution and/or pricing variances, and requirements and procedures for issuing contract modifications.	March 2012
2. COTR manual needs to be strengthened	1. Add a chapter on how to review invoices for approval.	March 2012
3. Vendor payments standard operating procedures need to be strengthened	1. Add a chapter on invoice reviews required in each step of the invoice payment cycle.	March 2012
4. Training needed on invoicing roles and responsibilities throughout the contract life-cycle	1. Institute mandatory and refresher training for contracting officers, contracting officer's technical representatives, and accounting technicians.	May 2012



Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Non-Contract Payments		
1. Standard operating procedures needed	1. Develop a process and standard operating procedures for authorizing and paying non-contract payments such as lease payments and bills of lading.	June 2012
Category of Error: Acceptance and Receiving		
1. Reports and contract file maintenance needs improvement	1. Develop a standard inspection, acceptance, and receiving report for contracting officer's technical representatives and complete training on its proper completion and use.	June 2012
	2. Implement an electronic contract file maintenance system.	June 2012

Table 9. Planned Emergency Food and Shelter Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Supporting Documentation		
1. Missing Proof of Purchase	1. Develop guidance around the supporting documentation checklist to state that unless the checklist is completely satisfied, the documentation will not be accepted by EFSP.	December 2011
2. Missing Proof that Payment Still Due	1. Develop improved guidance for utility or rent assistance to clarify that the local recipient organization (LRO) must have proof that payment is still due if paid beyond 60 days after the LRO was notified of the request for assistance.	March 2012
3. Missing LRO Documentation: a. Missing required certification documents, b. Missing Proof of Payment	1. Establish a filing system to maintain required LRO certification documents, including but not limited to the following forms: (1) Local Board Certification, (2) Local Board Roster, (3) Lobbying Certification, (4) Local Board Plan, (5) Interim Report, and (6) Final Report.	December 2011
4. Missing All Supporting Documentation	1. Review the existing National Board Program requirements training for possible modification of documentation requirements and other grant management improvement opportunities.	March 2012
	2. Provide grantees with technical assistance on maintaining adequate documentation for transactions using EFSP funds.	December 2011



Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Purchase Outside Allowable Timeframe		
1. Purchase Made Outside the Period of Performance	1. Require local boards to conduct outreach activities with LROs throughout the period of performance.	December 2011
	2. Require LROs to perform a self assessment of the purchase and/or initiation dates on all supporting documentation before submission to the local board to ensure that all expenditures are within the specified period of performance of the appropriate spending phase.	March 2012
Category of Error: Spending Condition Non-compliance		
1. Spending Condition Errors	1. Develop a mandatory on-line training course to be taken and passed by all local boards and LROs awarded funding.	May 2012
2. Incorrect Rent, Mortgage or Utility Payment: a. Current Payments Made Too Early b. Allowable Assistance Payment Exceeded	1. Leverage existing LRO rent/mortgage and utility assistance letters to create standardized forms for spending and other categories where compliance problems persist with submission of LRO supporting documentation.	March 2012

Table 10. Planned National Flood Insurance Program Corrective Actions

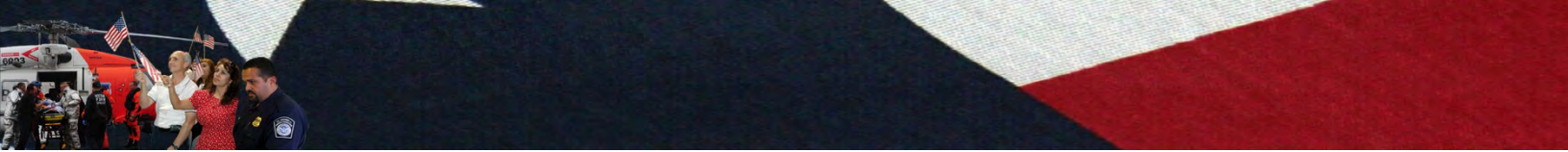
Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect Estimate / Worksheet Calculation Errors		
1. Insurance coverage incorrectly applied by adjusters. Claim estimates included items not covered under Flood insurance policy.	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	May 2012
	2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	
Category of Error: Payment Processing Errors		
1. Incorrect Application of Salvage	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences	May 2012
	2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	
	3. System Enhancements: Develop process to leverage the current transaction record reporting and processing reports and other NFIP financial and statistical data mechanisms to help insurers and flood vendors identify payment processing errors electronically.	



Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Damage Documentation		
1. Lack of supporting documentation for adjuster estimates on lump-sum items. Increased Cost Compliance claims not supported with required claim documentation.	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	May 2012
	2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	

Table 11. Planned Public Assistance (PA) Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect Entity Paid		
1. Incorrect Federal Information Processing Standards Number	1. Improve grantee project worksheet (PW) development procedures by incorporating a quality check after the initial PW is completed to confirm all information within the PW is relevant and correct prior to submitting the final version into the system of record.	October 2011
Category of Error: Unmet Work Completion Deadline		
1. Failure to Complete Work During Period of Performance	1. Increase grantee documentation review guidance and create and conduct Public Assistance payment processing training.	March 2012
Category of Error: Scope Discrepancy between Project Worksheet Scope of Work (SOW) and Supporting Documentation		
1. Discrepancies Found between PW SOW and Supporting Documentation	1. Require FEMA project specialists and Public Assistance coordinators to take training courses on proper PW data entry and development, project writing skills, and audit review requirements.	October 2011
	2. Develop reference guides and/or checklists for costs documentation reviews to improve consistency of scope reviews.	October 2011
	3. Offer grantee invoice and force account documentation review guidance or training to ensure the scope of supporting documentation falls within the scope of the PW/SA.	October 2011
Category of Error: Calculation Error between Force Account Summary Sheet and Closeout PW		
1. Mathematical Calculation Error	1. Develop guidance for grantees to eliminate use of rounding in payment calculations to improve accuracy of disbursements of grant funds to sub-grantees.	March 2012



Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Direct Administrative Costs Not Supported in Closeout PW		
1. Direct Administrative Costs Not Included in Closeout PW	1. Improve guidance and outreach to grantees on payment calculations, quality control, and overall accuracy of information when closing out a PW.	October 2011

Corrective Action Plan for ICE High-Risk Program

The corrective actions implemented by ICE for the ERO Program will strengthen documentation, invoicing, contract quality, payment quality and accuracy, discount and interest accuracy, and travel payment quality and accuracy.

Table 12. Completed ERO Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Invalid / Improper Invoice		
1. Vendor payments delayed or made incorrectly due to inadequate information	1. Discontinue the use of the invoice adjustment form. If an invoice is incorrect, the invoice must be rejected and resubmitted by the vendor.	February 2011
Category of Error: Contract Quality		
2. Improper processing of contracts and obligations; not in compliance with the Federal Acquisition Regulation	1. Align receipt and acceptance policies and procedures with federal requirements.	September 2011
Category of Error: Discount and Interest Accuracy		
3. Improper management of funds	1. Establish a policy to maximize cost-effective discounts.	May 2011
	2. Develop appropriate tools to communicate and monitor the status of invoices with discounts offered.	July 2011
	3. Conduct refresher training related to interest penalty payments and vendor discounts.	July 2011
	4. Develop monitoring and testing criteria to monitor the effectiveness of all procedural updates.	July 2011



Table 13. Planned ERO Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Missing Documentation		
1. Insufficient documentation to support and/or validate financial transactions	1. Provide payment documentation requirements and instructions to the program offices. Instructions to detail the following: (1) invoices that do not contain all invoice backup documentation must be rejected by the receiving and acceptance official, (2) compliance required with record retention guidelines according to National Archives and Records Administration (NARA), and (3) the need for program offices to maintain and have readily available all service agreements and memoranda of understanding.	December 2011
	2. Automate FY 2012 IPERA documentation collection by establishing a central SharePoint collaboration site.	March 2012
Category of Error: Invalid / Improper Invoice		
1. Vendor payments delayed or made incorrectly due to inadequate information	1. Conduct refresher training for payment technicians on elements of a proper invoice and ensure that improper invoices are rejected upon receipt.	March 2012
Category of Error: Contract Quality		
1. Improper processing of contracts and obligations; not in compliance with the Federal Acquisition Regulation	1. Implement new receipt and acceptance requirements.	March 2012
	2. Establish and provide “Subject to Availability of Funds” guidance regarding notification to vendor for funds availability, receipt of invoice, and payment of interest.	May 2012
Category of Error: Payment Quality and Accuracy		
1. Improper processing of vendor payments and disbursements	1. Conduct refresher training for contracting officer, contracting officer’s technical representative (COTR), and/or program manager to ensure review of invoices to contracted pricing, invoice alignment to correct obligations, and accurate and complete supporting documentation.	March 2012
	2. Conduct refresher training for finance centers and implement an updated checklist to incorporate the review of invoices for date (discount/penalty), correct contract, and correct obligation lines.	March 2012



Corrective Action Plan for NPPD High-Risk Program

The corrective actions implemented by NPPD and FPS will strengthen contract oversight and improve the review and processing of invoices and contract modifications.

Table 14. Planned Federal Protective Service Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Contract Oversight		
1. Contractor approving payment of invoices on behalf of the COTR	1. Remove contractors from the process of paying invoices, including terminating contractor access to Webview. Coordinate all Webview access requests through NPPD.	November 2011
	2. Provide COTRs with support to review and approve payments within Webview.	May 2012
1. Contract administration weakness	1. FPS Acquisition Division will establish a team of senior procurement officials and operational procurement staff to identify improvements to contract administration including invoicing and documentation.	December 2011
	2. FPS Acquisition Division will coordinate with program offices and contracting officers to identify and provide written delegations of authority to federal employees which facilitate an efficient invoice review and approval process.	January 2012
	3. Provide training to contracting officers, COTRs, and appropriate program officials on invoice review and contract modifications. Emphasis will be on the timely correction of errors on invoices and contract lines.	February 2012

Funds Stewardship

FEMA worked closely with primary grant recipients to ensure proper stewardship of funds at the sub-recipient levels. For example, on the Emergency Food and Shelter Program, FEMA worked closely with The United Way's National Board. As a result, the National Board issued a memo highlighting that additional rounds of funding to local boards would be dependent upon receipt of timely supporting documentation for tested sample payments. Significant additional documentation came in which supported as proper many test sample payments. FEMA also assisted states in improving the guidance they provide local entities for several state administered FEMA grant programs.



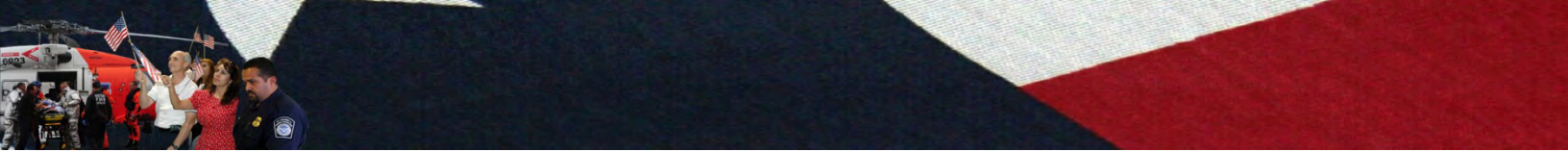
IV. Program Improper Payment Reporting

Table 15 summarizes improper payment amounts for DHS high-risk programs. Improper payment percent (IP%) and improper payment dollar (IP\$) results are provided from last year's testing of FY 2009 payments and this year's testing of FY 2010 payments. Data for projected future-year improvements is based on the timing and significance of completing corrective actions.

Table 15. Improper Payment Reduction Outlook

Improper Payment Reduction Outlook (\$ in millions)															
Program	PY Outlays	PY IP%	PY IP\$	CY Outlays	CY IP%	CY IP\$	CY+1 Outlays	CY+1 Est. IP%	CY+1 Est. IP\$	CY+2 Est. Outlays	CY+2 Est. IP%	CY+2 Est. IP\$	CY+3 Est. Outlays	CY+3 Est. IP%	CY+3 Est. IP\$
	(Based on FY 2009 Actual Data)			(Based on FY 2010 Actual Data)			(Based on FY 2011 Actual and Estimated Data)			(Based on 2012 Estimated Data)			(Based on 2013 Estimated Data)		
Border Security Fencing (CBP)	\$638	0.03%	\$0	\$251	0.01%	\$0	\$396	0.01%	\$0	\$528	0.01%	\$0	\$458	0.01%	\$0
Refund & Drawback (CBP)	\$1,436	0.20%	\$3	\$1,198	0.28%	\$3	\$1,405	0.17%	\$2	\$1,300	0.17%	\$2	\$1,300	0.17%	\$2
IHP (FEMA)	\$848	2.72%	\$23	\$679	0.31%	\$2	\$722	0.31%	\$2	\$722	0.31%	\$2	\$722	0.31%	\$2
Disaster Relief Program Vendor Payments (FEMA)	\$1,382	3.32%	\$46	\$582	2.87%	\$17	\$933	2.00%	\$19	\$933	1.50%	\$14	\$933	1.00%	\$9
NFIP (FEMA)	\$3,287	2.22%	\$73	\$1,085	1.21%	\$13	\$1,730	1.10%	\$19	\$1,730	1.00%	\$17	\$1,730	0.90%	\$16
PA (FEMA)	\$5,070	0.21%	\$11	\$3,532	0.32%	\$11	\$3,976	0.21%	\$8	\$3,976	0.21%	\$8	\$3,976	0.21%	\$8
HSGP (FEMA)	\$1,300	2.20%	\$29	\$1,516	0.34%	\$5	\$1,402	0.34%	\$5	\$1,402	0.34%	\$5	\$1,402	0.34%	\$5
AFG (FEMA)	\$429	6.32%	\$27	\$385	5.09%	\$20	\$440	4.25%	\$19	\$440	3.50%	\$15	\$440	2.50%	\$11
TSGP (FEMA)	\$119	0.09%	\$0	\$109	0.68%	\$1	\$114	0.09%	\$0	\$114	0.09%	\$0	\$114	0.09%	\$0
EFSP (FEMA)	\$86	6.18%	\$5	\$201	7.64%	\$15	\$251	5.00%	\$13	\$251	4.00%	\$10	\$251	3.50%	\$9
ERO (ICE)	\$1,320	0.53%	\$7	\$1,332	8.12%	\$108	\$1,414	7.95%	\$112	\$1,442	4.10%	\$59	\$1,471	2.00%	\$29
FPS (NPPD)	\$760	0.10%	\$1	\$811	3.27%	\$27	\$835	2.50%	\$21	\$943	2.00%	\$19	\$1,009	1.50%	\$15
Aviation Security – Payroll (TSA)	\$2,383	0.00%	\$0	\$2,458	0.01%	\$0	\$2,619	0.01%	\$0	\$2,841	0.01%	\$0	\$2,951	0.01%	\$0
ADMP (USCG)	\$2,766	0.13%	\$4	\$2,918	0.13%	\$4	\$3,006	0.13%	\$4	\$3,006	0.13%	\$4	\$3,006	0.13%	\$4
All Programs	\$21,824	1.05%	\$229	\$17,057	1.32%	\$226	\$19,243	1.17%	\$224	\$19,628	0.80%	\$157	\$19,763	0.56%	\$111

Note: For the three FEMA programs that were not tested nationally—HSGP, PA, and TSGP—the error rate from the state(s) tested was applied to the national payment population to produce the estimated error amounts listed above. Estimated outlays for FEMA programs were calculated by averaging the total disbursements for the past three fiscal years, due to the volatile nature of the programs tested. TSGP estimated outlay figures were based on the past two fiscal years that this program was tested.



Overpayments and Underpayments Details

The table that follows provides overpayment and underpayment breakouts for the Department’s high-risk programs. The table shows that 98 percent of the Department’s estimated improper payments are due to overpayments, and 2 percent are due to underpayments.

Table 16. Overpayment and Underpayment Detail on DHS Sample Test Results

Component	Program	FY 2011 Gross Total (Based on FY 2010 Actual Data)		FY 2011 Overpayment Total (Based on FY 2010 Actual Data)		FY 2011 Underpayment Total (Based on FY 2010 Actual Data)	
		Est. Error Amount (\$ millions)	Est. Error Percentage (%)	Est. Error Amount (\$ millions)	Est. Error Percentage (%)	Est. Error Amount (\$ millions)	Est. Error Percentage (%)
CBP	Border Security Fencing (CBP)	\$0	0.01%	\$0	0.01%	\$0	0.00%
	Refund & Drawback (CBP)	\$3	0.28%	\$3	0.28%	\$0	0.00%
FEMA	IHP (FEMA)	\$2	0.31%	\$0	0.00%	\$2	0.31%
	Disaster Relief Program Vendor Payments (FEMA)	\$17	2.87%	\$17	2.87%	\$0	0.00%
	NFIP (FEMA)	\$13	1.21%	\$12	1.15%	\$1	0.06%
	PA (FEMA)	\$11	0.32%	\$11	0.31%	\$0	0.01%
	HSGP (FEMA)	\$5	0.34%	\$5	0.34%	\$0	0.00%
	AFG (FEMA)	\$20	5.09%	\$20	5.09%	\$0	0.00%
	TSGP (FEMA)	\$1	0.68%	\$1	0.68%	\$0	0.00%
	EFSP (FEMA)	\$15	7.64%	\$15	7.64%	\$0	0.00%
ICE	ERO (ICE)	\$108	8.12%	\$108	8.11%	\$0	0.01%
NPPD	FPS (NPPD)	\$27	3.27%	\$27	3.27%	\$0	0.00%
TSA	Aviation Security – Payroll (TSA)	\$0	0.01%	\$0	0.00%	\$0	0.01%
USCG	ADMP (USCG)	\$4	0.13%	\$3	0.09%	\$1	0.04%
DHS	All Programs	\$226		\$222		\$4	

V. Recapture of Improper Payments

DHS completed recovery audit work for FY 2010 disbursements and continued collection activities for errors identified in prior-year recovery audits. Work was completed at CBP, FEMA, ICE (and the Components they cross-service), and U.S. Coast Guard. Given the highly productive findings from the U.S. Coast Guard’s targeted recovery audit work (details below), completing this work was given priority over completing a general recovery audit over all payments. The U.S. Coast Guard will complete a general recovery audit over FY 2010 and FY 2011 contract payments in FY 2012. This audit will also cover DNDO, TSA, and Components cross-serviced by the U.S. Coast Guard. The U.S. Secret Service will complete a recovery audit over FY 2010 and FY 2011 payments in FY 2012. FLETC performed a cost analysis which determined that a general recovery audit would not be cost effective at this time. In Table 17, which follows, current year (CY) equals FY 2010 disbursements, and prior year (PY) covers FY 2005–FY 2009 for DNDO, TSA, and U.S. Coast Guard; FY 2004–FY 2009 for CBP, ICE, MGMT, NPPD, OHA, S&T, and USCIS; and FY 2009–FY 2010 for FEMA.

The U.S. Coast Guard hired a recovery audit contractor to perform a targeted in-depth examination of telecommunications invoices. An examination of 14,000 telecommunications invoices from



FY 2005 to FY 2010 identified errors totaling \$4,144,859, of which \$64,460 has been recovered, and \$4,080,399 is undergoing collection. All of the \$4,144,859 improper payment errors were caused by overpayments (no underpayments). The low rate of recoupment of these errors reflects: (1) the fact that this was the first time the U.S. Coast Guard performed a targeted recovery audit of telecommunications payments, (2) the complexity of the invoices examined, (3) the need to centralize the collection of the overpayments within a decentralized procurement activity, and (4) the desire to complete full due diligence with the vendor community to validate the correctness of potential claims.

Telecommunications invoices were selected for a targeted recovery audit due to: (1) inconsistent billing practices and invoice format between carriers, (2) pricing complexities including multiple pages with numerous pricing elements (3) charges listed in “lump sum” amounts with discounts generally applied making it difficult to establish true price points, (4) multiple telecom companies and services billing on a single invoice, and (5) inability of staff to perform in-depth reviews of invoices due to technical proficiency and monthly payment volume.

Identified payment errors for telecommunications invoices include: (1) international and domestic rate charges in excess of published rates, (2) plan errors due to pricing not following requested General Services Administration (GSA) discounted plan, (3) inconsistent rate charges for the same service in the same geographic region, (4) charges for federal and state taxes, (5) discovery of unauthorized third-party billings (i.e., cramming), (6) unexplained increases in land line charges, and (7) zero usage charges.

Immediate benefits from this work included the dropping of long distance services from accounts where it was not required, producing an immediate cost savings of \$102,335 and the identification of numerous circuits, telephone lines, and data pipes suspected to no longer be in use. Estimated future cost savings could be in excess of two million dollars. In addition to following up on these items, the U.S. Coast Guard is evaluating procurement policy, acquisition procedures, and payment controls to fully leverage the benefits of this recovery audit contract work. An operations team consisting of specialists in telecommunications and information technology, procurement, financial management, and legal has been assembled to rectify known billing issues and to develop a corrective action plan to correct systemic process and payment errors to ensure non-recurrence going forward. The U.S. Coast Guard will apply the lessons learned from these recovery auditing activities to develop automated monitoring controls. Vendor-wide memos will be distributed requesting rate changes for all accounts with non-GSA rates. Internal certifications and ongoing training will also be provided to the designated account representatives who order telecommunications services. Language eliminating the use of third party billings will also be added to telecommunications contracts where appropriate.

FEMA conducts regular audits to assess the effectiveness of its controls, identify improper payments or risk areas, and consider new procedures to reduce risk. This continued self-assessment and vigilance significantly reduced the improper payment error rate from 14 percent following Hurricane Katrina in 2005 to less than one percent in FY 2010. In instances of improper payments, new procedures implemented in 2011 allow FEMA to request the return of any improperly awarded disaster assistance payments while maintaining each disaster survivor’s due process rights and offering opportunities to appeal, which may include the opportunity for an oral hearing.



Table 17. Payment Recapture Audit Reporting

Component	Type of Payment (contract, grant, benefit, loan, or other)	Amount Subject to Review for CY Reporting (\$ millions)	Actual Amount Reviewed and Reported (CY) (\$ millions)	Amount Identified for Recovery (CY) (\$000)	Amount Recovered (CY) (\$000)	% of Amount Recovered out of Amount Identified (CY)	Amount Outstanding (CY) (\$000)	% of Amount Outstanding out of Amount Identified (CY)	Amount Determined Not to be Collectable (CY) (\$000)	% of Amount Determined Not to be Collectable out of Amount Identified (CY)	Amounts Identified for Recovery (PYs) (\$000)	Amounts Recovered (PYs) (\$000) ¹	Cumulative Amounts Identified for Recovery (CY + PYs) (\$000)	Cumulative Amounts Recovered (CY + PYs) (\$000)	Cumulative Amounts Outstanding (CY + PYs) (\$000)	Cumulative Amounts Determined Not to be Collectable (CY + PYs) (\$000)
CBP	Contract	\$2,345	\$2,345	\$0	\$0	100%	\$0	100%	\$0	0%	\$250	\$246	\$250	\$246	\$2	\$2
DNDO ²	Contract	\$369	\$0	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$1	\$1	\$1	\$1	\$0	\$0
FEMA	Contract	\$1,067	\$1,067	\$3	\$0	0%	\$3	100%	\$0	0%	\$178	\$0	\$181	\$0	\$3	\$178
ICE	Contract	\$2,837	\$2,837	\$7	\$0	0%	\$7	100%	\$0	0%	\$1,748	\$1,607	\$1,755	\$1,607	\$45	\$103
MGMT ³	Contract	\$472	\$472	\$36	\$36	100%	\$0	0%	\$0	0%	\$174	\$172	\$210	\$208	\$2	\$0
NPPD ³	Contract	\$553	\$553	\$26	\$17	65%	\$9	35%	\$0	0%	\$190	\$190	\$216	\$207	\$9	\$0
OHA ³	Contract	\$49	\$49	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$0	\$0	\$0	\$0	\$0	\$0
S&T ³	Contract	\$433	\$433	\$1	\$0	0%	\$1	100%	\$0	0%	\$54	\$54	\$55	\$54	\$1	\$0
TSA ²	Contract	\$2,178	\$0	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$722	\$722	\$722	\$722	\$0	\$0
USCG	Contract	\$2,308	\$78	\$4,145	\$65	2%	\$4,080	98%	\$0	0%	\$107	\$91	\$4,252	\$156	\$4,096	\$0
USCIS ³	Contract	\$913	\$913	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$904	\$892	\$904	\$892	\$4	\$8
DHS Totals		\$13,524	\$8,747	\$4,218	\$118	3%	\$4,100	97%	\$0	0%	\$4,328	\$3,975	\$8,546	\$4,093	\$4,162	\$291

Notes:

1. The format for the Recovery Audit Results table published in the FY 2010 DHS Annual Financial Report included all collections accomplished in the current fiscal year in one column (Amounts Recovered CY). Reporting in the table above distinguishes between FY 2011 collections which relate to current year claims (Amount Recovered CY) from collections from prior year claims (Amounts Recovered PYs).
2. DNDO and TSA are cross-serviced by the U.S. Coast Guard.
3. MGMT, NPPD, OHA, S&T, and USCIS are cross-serviced by ICE.



The next two tables highlight the productivity of the targeted recovery audit work performed at the U.S. Coast Guard relative to general recovery audits performed elsewhere.

Table 18. Payment Recapture Audit Targets

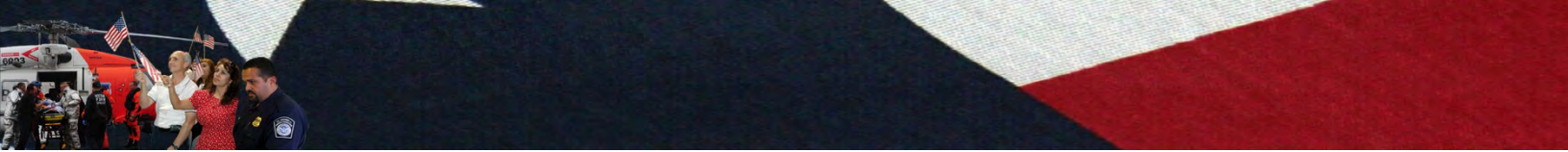
Component	Type of Payment (contract, grant, benefit, loan, or other)	CY Amount Identified (\$000)	CY Amount Recovered (\$000)	CY Recovery Rate (Amount Recovered / Amount Identified)	CY + 1 Recovery Rate Target	CY + 2 Recovery Rate Target	CY + 3 Recovery Rate Target
FEMA	Contract	\$3	\$0	0%	100%	100%	100%
ICE	Contract	\$7	\$0	0%	100%	100%	100%
MGMT	Contract	\$36	\$36	100%	100%	100%	100%
NPPD	Contract	\$26	\$17	65%	100%	100%	100%
S&T	Contract	\$1	\$0	0%	100%	100%	100%
USCG	Contract	\$4,145	\$65	2%	50%	80%	100%
DHS Totals		\$4,218	\$118	3%			

Table 19. Aging of Outstanding Overpayments

Component	Type of Payment (contract, grant, benefit, loan, or other)	CY Amount Outstanding (0 – 6 months) (\$000)	CY Amount Outstanding (6 months to 1 year) (\$000)	CY Amount Outstanding (over 1 year) (\$000)
FEMA	Contract	\$3	\$0	\$0
ICE	Contract	\$7	\$0	\$0
NPPD	Contract	\$9	\$0	\$0
S&T	Contract	\$1	\$0	\$0
USCG	Contract	\$4,080	\$0	\$0
DHS Totals		\$4,100	\$0	\$0

Table 20. Disposition of Recaptured Funds

Component	Type of Payment (contract, grant, benefit, loan, or other)	Agency Expenses to Administer the Program (\$000)	Payment Recapture Auditor Fees (\$000)	Financial Management Improvement Activities (\$000)	Original Purpose (\$000)	Office of Inspector General (\$000)	Returned to Treasury (\$000)
MGMT	Contract	\$0	\$6	\$0	\$30	\$0	\$0
NPPD	Contract	\$0	\$3	\$0	\$14	\$0	\$0
USCG	Contract	\$0	\$11	\$0	\$54	\$0	\$0
DHS Totals		\$0	\$20	\$0	\$98	\$0	\$0



The table that follows shows the importance of the Secretary’s quarterly high-dollar overpayments reporting. These reports began with January-March 2010 reporting. Recoverable errors from IPIA high-risk program testing are mainly from FEMA’s testing of the National Flood Insurance Program and U.S. Coast Guard’s testing of Active Duty Military Payroll. Post-payment review figures are from U.S. Coast Guard.

Table 21. Overpayments Recaptured Outside of Payment Recapture Audits

Source of Recovery	Amount Identified (CY) (\$000)	Amount Recovered (CY) (\$000)	Amount Identified (PY) (\$000)	Amount Recovered (PY) (\$000)	Cumulative Amount Identified (CY+PYs) (\$000)	Cumulative Amount Recovered (CY+PYs) (\$000)
High-Dollar Overpayments Reporting	\$8,183	\$7,493	\$6,063	\$5,956	\$14,246	\$13,449
IPIA High-Risk Program Testing	\$190	\$43	\$880	\$202	\$1,070	\$245
Post Payment Reviews	\$2,620	\$2,582	\$0	\$0	\$2,620	\$2,582
DHS Totals	\$10,993	\$10,118	\$6,943	\$6,158	\$17,936	\$16,276

VI. Ensuring Management Accountability

The goals and requirements of IPERA were communicated to all levels of staff throughout the Offices of the Chief Financial Officer and to relevant program office and procurement staff. The Department’s Deputy Chief Financial Officer and senior staff and FEMA’s Chief Financial Officer and senior staff have incorporated improper payment reduction targets in their annual performance plans. FEMA grant program managers have communicated to primary recipients that continued funding is contingent upon supporting the Department’s improper payments efforts.

Continuing an initiative begun in FY 2009, Secretary Napolitano includes recoupment of improper payments as an efficiency measure which is tracked quarterly. Additionally, managers are responsible for completing internal control work on payment processing as part of the Department’s OMB Circular A-123 effort.

VII. Agency Information Systems and Other Infrastructure

The Department’s agency information systems efforts are discussed under the section related to the *Federal Financial Management Improvement Act*.

VIII. Statutory or Regulatory Barriers

None.

IX. Overall Agency Efforts

The Department is striving to leverage lessons learned from the battle to reduce and recover improper payments to other operational areas. At FEMA, for example, improper payment corrective actions support improvements to grants management and better coordination between



recipients and sub-recipients. At NPPD, close cooperation between finance and procurement shops will help the Department address contract management administration weakness that does not directly lead to improper payments but raises risks. At U.S. Coast Guard, an audit of telecommunications bills supports the strengthening of acquisition practices and the identification of cost savings.



Other Key Regulatory Requirements

Prompt Payment Act

The *Prompt Payment Act* requires federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's Components submit prompt payment data as part of data gathered for the OMB CFO Council's Metric Tracking System (MTS). Periodic reviews are conducted by the DHS Components to identify potential problems. Interest penalties as a percentage of the dollar amount of invoices subject to the *Prompt Payment Act* have been measured between 0.002 percent and 0.073 percent for the period of October 2010 through September 2011, with an annual average of 0.009 percent. *Note: MTS statistics are reported with at least a six-week lag.*

Debt Collection Improvement Act (DCIA)

In compliance with the *Debt Collection Improvement Act of 1996* (DCIA), DHS manages its debt collection activities under the DHS DCIA regulation. The regulation is implemented under DHS's comprehensive debt collection policies that provide guidance to the Components on the administrative collection of debt; referring non-taxable debt; writing off non-taxable debt; reporting debts to consumer reporting agencies; assessing interest, penalties and administrative costs; and reporting receivables to the Department of the Treasury.

FY 2010 Biennial User Charges Review

The *Chief Financial Officers Act of 1990* requires each agency CFO to review, on a biennial basis, the fees, royalties, rents, and other charges imposed by the agency for services and items of value provided to specific recipients, beyond those received by the general public. The purpose of this review is to identify those agencies assessing user fees and to periodically adjust existing charges to: 1) reflect unanticipated changes in costs or market values; and 2) to review all other agency programs to determine whether fees should be assessed for government services or the use of government goods or services.

In addition, on October 28, 2009, the *FY 2010 Department of Homeland Security Appropriations Act* (Pub. L. 111-83) and accompanying House Report 111-157 was passed, requiring the Department to provide to Congress a quarterly report on actual FY 2009 user fee collections and future projections across all relevant DHS Components. Therefore, to ensure consistency in reporting, the OCFO conducted the above DHS user fee assessment based on the Component's review, validation, and confirmation of actual cash collections and user fee structures, as identified in the Department of Homeland Security User Fees Report to Congress. This review was reported by the CFO in the Department's FY 2010 Annual Financial Report. The next biennial review of user fees to be performed by DHS is scheduled to take place in FY 2012 and will be based on FY 2011 data.



Major Management Challenges Facing the Department of Homeland Security

Office of Inspector General

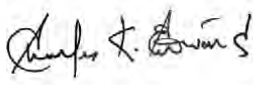
U.S. Department of Homeland Security
Washington, DC 20528



Homeland Security

November 10, 2011

MEMORANDUM FOR: The Honorable Janet Napolitano
Secretary

FROM: Charles K. Edwards 
Acting Inspector General

SUBJECT: *Major Management Challenges
Facing the Department of Homeland Security*

Attached for your information is our annual report, *Major Management Challenges Facing the Department of Homeland Security*, for inclusion in the Department of Homeland Security 2011 *Annual Financial Report*.

Should you have any questions, please call me, or your staff may contact Anne L. Richards, Assistant Inspector General for Audits, at (202) 254-4100.

Attachment



Department of Homeland Security **Office of Inspector General**

Major Management Challenges Facing the Department of Homeland Security



OIG-12-08

November 2011



Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

November 10, 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The attached report presents our fiscal year 2011 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Charles K. Edwards
Acting Inspector General



Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

Major Management Challenges Facing the Department of Homeland Security

At its establishment in 2003, the Department of Homeland Security (DHS) faced the difficult task of building a cohesive, effective, and efficient Department from 22 disparate agencies while simultaneously performing the mission for which it was created. That mission, to secure the nation against the entire range of threats that we face, is itself an arduous assignment. The Department has made progress in coalescing into an effective organization, as well as addressing its key mission areas to secure our nation's borders, increase our readiness and resiliency in the face of a terrorist threat or a natural disaster, and implement increased levels of security in our transportation systems and trade operations.

As in previous years, the Department's major challenges lie in nine broad areas, which we address below:

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



ACQUISITION MANAGEMENT

Although the Department continues to make progress in improving its acquisition management, it remains a significant challenge facing DHS, in part because of the magnitude of the number, dollar value, and complexity of its acquisition activity. Below, we identify where DHS improved its acquisition management process, as well as areas where it continues to face challenges.

Organizational Alignment and Leadership

In fiscal year (FY) 2011, DHS improved the acquisition program's organizational alignment and maintained strong executive leadership, but more needs to be done. In January, DHS reorganized the reporting structure of the procurement management and program management functions to provide a layered approach to acquisition oversight. Now the Office of the Chief Procurement Officer (OCPO) leads procurement management functions and the Under Secretary for Management leads program management functions. Components continue to maintain their own acquisition and procurement staff. At the component level, the Chief Acquisition Executive is responsible for acquisition program management and the Head of Contracting Activity is responsible for acquisition procurement. There are currently eight chief acquisition executives and nine heads of contracting activity in DHS. The chief acquisition executives and the heads of contracting activity report informally to the Under Secretary for Management and OCPO, respectively.

According to the Government Accountability Office (GAO),¹ DHS has not fully planned for or acquired the workforce needed to implement its acquisition oversight policies. A GAO report issued in February 2011 states that, DHS needs to implement its Integrated Strategy for High Risk Management and continue its efforts to (1) identify and acquire resources needed to achieve key actions and outcomes; (2) implement a program to independently monitor and validate corrective measures; and (3) show measurable, sustainable progress in implementing corrective actions and achieving key outcomes. DHS needs to demonstrate sustained progress in all of these areas to better strengthen and integrate management functions throughout the Department and its components' acquisition functions.

Policies and Processes

DHS continues to develop and strengthen its acquisition management policies and processes. However, the Department needs to further refine its policies to provide detailed guidance, and improve oversight and internal controls in some key areas. For example, the Department needs to improve internal control procedures to mitigate the inherent risks associated with purchase card use. Our review of the Department's purchase card program² found that the post-payment audit process did not ensure that component personnel were meeting minimum internal control requirements established by the Office of Management and Budget (OMB). Nor did the process effectively target high-risk transactions. Ninety-three percent of the purchase card transactions we reviewed did not fully comply with OMB requirements, and

¹ GAO-11-278, *High Risk Series - An Update*, February 2011.

² DHS-OIG, *Use of DHS Purchase Cards*, (OIG-11-101, August 2011).



the Department's purchase card manual and components' guidance were incomplete and inconsistent. Based on our audit, the Department's Office of the Chief Financial Officer has initiated corrective actions to improve internal controls over the purchase card program.³

The Department can also improve management of its use of strategic sourcing. In March 2011, we found that the Department did not have a logistics process in place to facilitate strategic sourcing of detection equipment. Strategic sourcing would require that management standardize equipment purchases for explosive, metal, and radiation detection equipment; identify common mission requirements among components; and develop standard data elements for managing the inventory accounts of detection equipment. Improving its management of detection equipment will offer the Department opportunities to streamline the acquisition process and improve efficiencies.⁴

Although the Federal Emergency Management Agency (FEMA) has developed and strengthened acquisition management policies and processes, it continues to face challenges. Weak internal controls resulted in multi-million dollar contracts with vague and questionable requirements.⁵ In addition, task monitors, agency employees responsible for managing and monitoring the contractors, had not received written guidance or training on how to evaluate contractor performance or certify billing invoices. Substantial improvements are needed in FEMA's oversight of contracts, including the prompt implementation of corrective actions.

In response to presidentially-declared disasters, FEMA's Public Assistance-Technical Assistance Contract firms (PA-TACs) provide technical assistance to state, local, and tribal governments awarded grants to fund debris removal and repair structures such as schools, medical facilities, and bridges. The *Brooks Act*⁶ requires engineering and architectural firms to be selected based on competency, qualifications, and performance, but FEMA chose between its three PA-TACs with the goal of ensuring the firms were paid equal sums over the life of their FEMA contracts. FEMA had no performance measures for its PA-TACs and failed to monitor or evaluate their performance. FEMA's contract files were not in compliance with regulations. Insufficient oversight of the contracts creates an environment ripe for waste, fraud, and abuse.⁷

Acquisition Workforce

DHS made progress in the recruitment and retention of a workforce capable of managing a complex acquisition program. The number of procurement staff has more than doubled since 2005. In addition, participation in the Acquisition Professional Career Program, which seeks to develop acquisition leaders, increased 62% from 2008 to 2010. Nevertheless, DHS continues to face workforce challenges across the Department.

³ DHS-OIG, *Improving FEMA's Disaster Purchase Card Program*, (OIG-10-91, May 2010).

⁴ DHS-OIG, *DHS Department-wide Management of Detection Equipment*, (OIG-11-47, March 2011).

⁵ DHS-OIG, *Improving FEMA's Individual Assistance, Technical Assistance Contracts*, (OIG-11-114, September 2011), and *Improvements Needed in FEMA's Management of Public Assistance-Technical Assistance Contracts*, (OIG-11-02, October 2010).

⁶ *Brooks Architect-Engineer Act*, 40 U.S.C. §1101, et seq.

⁷ DHS-OIG, *Improvements Needed in FEMA's Management of Public Assistance-Technical Assistance Contracts*, (OIG-11-02, October 2010).



According to GAO, the United States Coast Guard (Coast Guard) reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent,⁸ and had filled 832 of its 951 acquisition positions as of November 2010. Although acquisition workforce vacancies have decreased, program managers have ongoing concerns about staffing program offices. For example, the HH-65 Aircraft Program Office had only funded and filled 10 positions out of an identified need for 33 positions. Also, according to its August 2010 human-capital staffing study, program managers reported concerns with staffing adequacy in program management and technical areas. To make up for shortfalls in hiring systems engineers and other acquisition workforce positions for its major programs, the Coast Guard uses support contractors, which constituted 25 percent of its acquisition workforce as of November 2010.

FEMA continues to make progress in the recruitment and retention of a workforce capable of managing complex acquisition programs. However, significant challenges remain. Acquisition staff turnover in FEMA has exacerbated file maintenance problems and resulted in multimillion-dollar contracts not being managed effectively or consistently. One of FEMA's challenges is hiring experienced contracting officers to work at disasters. The majority of FEMA staff at a disaster site work on an on-call, intermittent basis. FEMA categorizes all its disaster assistance employees in the occupational series 301, regardless of the function the employee will perform for FEMA. As such, a Disaster Assistance job announcement will not appear in a search for open contracting officer positions, limiting FEMA's ability to attract seasoned contracting officers. Secondly, by being categorized as a 301, Disaster Assistance contracting officers will only be able to administer contracts up to \$150,000. Thirdly, the Office of Personnel Management has allowed waivers for retired annuitants who return classified as contracting officers; however, these same waivers are not available to employees classified as 301s. Consequently, Disaster Assistance employees classified as 301s are not encouraged to continue working after the first 120 days after a disaster declaration. This increases turnover, which is detrimental to smooth contract execution.⁹

FEMA has made great strides in improving its contracting officer's technical representatives (COTRs) cadre. FEMA has dedicated staff to oversee the COTR program; developed a tiered system, which ties training requirements to dollar values of contracts a COTR can monitor; and established an intranet site containing tools for COTRs' use. However, many trained COTRs have never been assigned a contract, and are unsure of their ability to be effective doing so. And, although they represent the contracting officer, the COTR's appraisal is completed by their supervisor in their program office, rather than the applicable contractor officer, thus leading to divided loyalties.¹⁰

⁸ GAO-11-480, *Coast Guard: Opportunities Exist to Further Improve Acquisition Management Capabilities*, April 2011.

⁹ DHS-OIG, *FEMA's Contracting Officer's Technical Representative Program*, (OIG-11-106, September 2011).

¹⁰ DHS-OIG, *FEMA's Contracting Officer's Technical Representative Program*, (OIG-11-106, September 2011).



Knowledge Management and Information Systems

DHS made progress in deploying an enterprise acquisition information system and tracking key acquisition data. The Department's acquisition reporting system of record, known as nPRS (next-Generation Period Reporting System), tracks components' level 1, 2, and 3 acquisition investments. It also has capabilities to store key acquisition documents, earned value management information, and risk identification. Component personnel are responsible for entering and updating information, which includes cost, budget, performance, and schedule data. However, components did not complete and report all key information in nPRS. In *DHS Oversight of Component Acquisition Programs*,¹¹ we reported that only 7 of 17 programs (41%) reported Acquisition Program Baseline required milestones. These milestones establish the acquisition cost, schedule, and performance values. Only 13 (76%) programs reviewed contained required key documentation such as a mission needs statement, acquisition plan, operational requirements document, and integrated logistics support plans.

INFORMATION TECHNOLOGY MANAGEMENT

Creating a unified information technology infrastructure for effective integration and agency-wide management of Information Technology (IT) assets and programs remains a challenge for the DHS Chief Information Officer (CIO). The CIO's successful management of IT across the Department will require the implementation of strong IT security controls, coordination of planning and investment activities across DHS components, and a commitment to ensuring privacy.

IT and Cyber Security

During our FY 2010 *Federal Information Security Management Act*¹² (FISMA) evaluation, we reported that the Department continued to improve and strengthen its security program. Specifically, the Department implemented a performance plan to improve on four key areas: Plan of Action and Milestones (POA&Ms) weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. Although the Department's efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. Management oversight of the components' implementation of the Department's policies and procedures needs improvement in order for the Department to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system certification and accreditation.

Further, over the past year, we have reported on the challenges specific components face in strengthening IT security. For example, in July 2011, we reported that the Transportation Security Administration (TSA) has implemented effective physical and logical security controls to protect its wireless network and devices.¹³ However, we identified high-risk

¹¹ DHS-OIG, *DHS Oversight of Component Acquisition Programs*, (OIG-11-71, April 2011).

¹² Title III of the *E-Government Act of 2002*, Public Law 107-347.

¹³ DHS-OIG, *Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices*, (OIG-11-99, July 2011).



vulnerabilities involving TSA's and Federal Air Marshal Service's patch and configuration controls. In September 2011, we reported that U.S. Customs and Border Protection (CBP) needs to strengthen enterprise wireless infrastructure security by remediating its open POA&Ms in a timely manner, enabling the wireless intrusion detection system to protect its network, and by performing regular vulnerability assessments to evaluate the effectiveness of wireless security.¹⁴ In March 2011, we reported on the steps the U.S. Citizenship and Immigration Services (USCIS) needs to take to protect its systems and information from the IT insider threat posed by employees and contractors.¹⁵ Specifically, USCIS needs to institute an enterprise risk management plan and incorporate insider threat risk mitigation strategies into its new business processes, institute a logging strategy to preserve system activities, and consistently enforce employee exit procedures.

In the area of cybersecurity, we reported in June 2011 that the National Protection and Programs Directorate (NPPD) has made progress in sharing cybersecurity threat information and raising cybersecurity awareness.¹⁶ However, significant work remains to address the open actions and recommendations and attain the goals outlined in *The National Strategy to Secure Cyberspace*, National Infrastructure Protection Plan, and Comprehensive National Cybersecurity Initiative. In addition, NPPD must ensure that systems personnel receive required Protected Critical Infrastructure Information training and that configuration and account access vulnerabilities are mitigated to protect the department's critical infrastructure information and sensitive data.

IT Management

Management of IT to ensure that it integrates well with other department-wide systems and federal partner agency systems and that it supports users' needs fully has been a challenge for several components. For example, the United States Coast Guard's command center and partner agency systems are not sufficiently integrated.¹⁷ These limitations had a variety of causes, including technical and cost barriers, aging infrastructure that is difficult to support, and stove-piped system development. As a result, field personnel relied on inefficient workarounds to accomplish their mission. Additionally, the IT systems developed by DHS to share information between DHS and state and local fusion centers did not support their needs fully.¹⁸ For example, the Homeland Security Information Network and the Homeland Security State and Local Community of Interest systems, both developed by DHS, are not integrated. As a result, users must maintain separate accounts, and information cannot easily be shared across the systems. Fusion center personnel also expressed concern that there were too many federal information sharing systems that were not integrated.

¹⁴ DHS-OIG, *Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure*, (OIG-11-118, September 2011).

¹⁵ DHS-OIG, *Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services (Redacted)* (OIG-11-33, January 2011).

¹⁶ DHS-OIG, *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure*, (OIG-11-89, June 2011).

¹⁷ DHS-OIG, *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG-11-108), September 2011).

¹⁸ DHS-OIG, *Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain* (OIG-11-04, October 2010).



In addition, several components involved in IT transformation activities did not have updated IT strategic plans to help guide IT investments decisions. For example, the U.S. Secret Service's IT strategic plan had not been updated since 2006 and did not reflect and guide its modernization efforts, address identified IT weaknesses, or integrate its IT with the DHS-wide enterprise infrastructure.¹⁹ In addition, FEMA's IT strategic plan was not comprehensive enough to coordinate and prioritize its modernization initiatives and IT projects.²⁰ The plan did not include clearly defined goals and objectives, nor did it address program office IT strategic goals.

DHS and its components also face challenges in upgrading their respective IT infrastructures, both locally and enterprise wide. In February 2011, we reported that CBP did not properly plan and implement the System Availability project, which was aimed at upgrading the local area networks at over 500 locations.²¹ Specifically, it did not ensure that adequate funding was available, include all at-risk sites, or develop planning documents needed to justify project requirements and cost. Subsequently, CBP ran out of funding and ended the project in February 2010. As a result, hundreds of field sites did not receive the needed upgrades and remain vulnerable to network outages.

Additionally, in September 2011, we reported that the Department has made some progress toward consolidating the existing components' infrastructures into OneNet, the Department's wide area network initiative.²² Specifically, it has established a centralized Network Operations Center/Security Operations Center incident response center and established a redundant network infrastructure and offers essential network services to its components. However, the Department still needs to establish component connections (peering) to OneNet and ensure that all components transition to the redundant trusted Internet connection.

Privacy

DHS continues to face challenges to ensure that uniform privacy procedures and controls are properly addressed and implemented throughout the lifecycle of each process, program, and information system that affects personally identified information (PII). In May 2011, we reported that USCIS demonstrated an organizational commitment to privacy compliance by appointing a privacy officer, establishing its Privacy Office, and making progress in implementing a privacy program that complies with privacy laws. However, we identified specific areas in privacy training, as well as technical and physical safeguards, to improve the protection of PII and the overall culture of privacy.²³

¹⁹ DHS-OIG, *U.S. Secret Service's Information Technology Modernization Effort (Redacted)* (OIG-11-56, March 2011).

²⁰ DHS-OIG, *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69, April 2011).

²¹ DHS-OIG, *Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project (Redacted)* (OIG-11-42, February 2011).

²² DHS-OIG, *DHS Continues to Face Challenges in the Implementation of Its OneNet Project* (OIG-11-116, September 2011).

²³ DHS-OIG, *U.S. Citizenship and Immigration Services Privacy Stewardship* (OIG-11-85, May 2011).



EMERGENCY MANAGEMENT

Although FEMA has made great strides in improving its disaster preparedness and recovery, challenges remain, including in the areas of emergency support functions, mass care and debris removal.

Emergency Support Functions

The National Response Framework is a guide to how the Nation conducts all-hazards response. FEMA is the coordinator or primary agency for eight Emergency Support Functions and is responsible for ensuring that activities for these functions are accomplished as outlined in the National Response Framework. In November 2010, we released a report evaluating FEMA's readiness to fulfill its Emergency Support Function roles and responsibilities.²⁴ The review focused on three major areas of responsibility: (1) Coordination with Emergency Support Function Stakeholders, (2) Operational Readiness, and (3) Financial Management.

We found that FEMA generally fulfilled its roles and responsibilities under the Emergency Support Functions. Specifically, the agency manages mission assignments, executes contracts, and procures goods and services for its Emergency Support Function activities. We also concluded, however, that the agency can improve its coordination with stakeholders and its operational readiness. For example, FEMA should be coordinating with stakeholders for all Emergency Support Functions. There was little evidence that support agencies were regularly included in planning meetings for Emergency Support Function 3: Public Works and Engineering, even though agency officials said that such coordination would be beneficial. The agency must coordinate these activities with all relevant federal departments and agencies, state and local officials, and private sector entities to effectively execute the Emergency Support Function mission.

FEMA also should be fully prepared to provide community assistance after a disaster. At the time of our review, it was not conducting long-term recovery exercises, and one Emergency Support Function did not have clearly defined procedures to identify and deploy needed recovery services to disaster affected communities. FEMA did include a long-term recovery component in the National Level Exercise 2011. FEMA told us that since our report, they have increased engagement with Emergency Support Function partner agencies and have reinvigorated the Emergency Support Function Leadership Group.

Mass Care and Emergency Assistance

We evaluated FEMA's progress in two Emergency Support Function sections: mass care and emergency assistance.²⁵ Mass care includes sheltering, feeding, emergency first aid, distribution of emergency items, and collecting and providing information on victims to family members. Emergency assistance is the assistance necessary to ensure that immediate

²⁴ DHS-OIG, *Assessment of Federal Emergency Management Agency's Emergency Support Function Roles and Responsibilities*, (OIG-11-08, November 2010).

²⁵ DHS-OIG, *Opportunities to Improve FEMA's Mass Care and Emergency Assistance Activities*, (OIG-11-77, April 2011).



needs beyond the scope of the traditional mass care services are addressed. These services include evacuation support, aid and services to special needs populations, reunification of families, as well as a host of other evacuation, sheltering, and other emergency services, as well as coordination of voluntary agency assistance.

FEMA continues to improve its mass care and emergency assistance program. It has coordinated more effectively with state and local governments and voluntary organizations; developed planning tools to build the mass care and emergency assistance capacities of these governments and organizations; and created an internal infrastructure to plan, coordinate, and provide direct mass care and emergency assistance, as needed.

While FEMA has taken steps to improve, additional actions are needed to ensure that the program is implemented effectively in future disasters. Mass care and emergency assistance standard operating procedures are in draft form, years after being developed. The effectiveness of developed planning tools and initiatives have not always been evaluated. Mass care and emergency assistance activities have not always been included in national and regional exercises. In addition, an opportunity exists for improved efficiency by creating automated computer interfaces between FEMA and American Red Cross National Shelter System databases. Each of these databases track sheltering information needed during a disaster. At this time, these two databases do not interface.

Debris Removal Operations

FEMA's Public Assistance program has expended more than \$8 billion over the past 11 years reimbursing applicants, primarily cities and counties, for removing debris resulting from natural disasters. In general this has been a successful effort; vast amounts of debris have been removed and disposed of, allowing communities to proceed with recovery efforts. Better planning, contracting, and oversight of debris removal operations, however, would enable these operations to be conducted in a more cost-effective manner.

Debris planning allows communities to be better prepared for a disaster by identifying debris collection and disposal sites, preparing debris removal contracts, and identifying potential debris contractors in advance of a disaster. Only a minority of states and local governments currently have such plans in place. A pilot program that operated in 2007–2008 was successful in encouraging the development of debris plans, but this momentum has been lost since the pilot program ended.

Decisions made in the first few days after a disaster strikes are critical in determining the success of a debris removal operation. Despite improved federal and state efforts to ensure that local governments are prepared for debris removal operations, they are often unprepared. FEMA debris advisers can help local governments determine what needs to be done, but qualified advisers are not always available when needed.

While FEMA has made significant strides in this area, opportunities remain for further improvement. Federal disaster response teams need to address debris expertise. Debris removal guidance is often unclear and ambiguous. Finally, an integrated performance



measurement system would provide federal and state officials and stakeholders with the data and tools to measure, analyze, and improve debris operations in a fact-based manner.

FEMA will be consolidating and updating the *Debris Monitoring Guide* and the *Debris Policy and Management Guide* into a single, comprehensive *Debris Policy and Management Guide* which will include detailed contracting guidance in FY 2012. FEMA will continue to make debris training available through the Emergency Management Institute, FEMA regional offices, and online. In addition, FEMA is currently developing a computer-based training course on debris management plan development that will be available to the public in FY 2012.

Since 2005, FEMA has worked to develop automated digital systems that will enhance FEMA's debris estimating and data collection capabilities in the field. FEMA is also developing a debris cost database to assist Public Assistance staff and applicants in determining whether a cost is reasonable. The debris cost database will also allow FEMA to analyze costs for debris operations across FEMA regions, disasters, states, and contractors. FEMA plans to implement these systems in FY 2012.

Fraud Prevention

Between January and September 2011, 10 separate billion dollar disasters have occurred in the United States.²⁶ The speed with which FEMA disburses individual and household disaster assistance results in the program's susceptibility to fraud. FEMA has established a Fraud Prevention and Investigation Branch to assist in the prevention and detection of fraud, but its operations are hindered by inadequate staffing and a lack of the latest technology tools to detect fraud. FEMA needs to improve its internal controls, provide fraud prevention training to all employees and support the Fraud Branch.²⁷

²⁶ National Climate Data Center, <http://www.ncdc.noaa.gov/oa/reports>, accessed September 13, 2011.

²⁷ DHS-OIG, *Assessment of FEMA's Fraud Prevention Efforts*, (OIG-11-84, May 2011).



GRANTS MANAGEMENT

FEMA's grants management and oversight infrastructure is challenged by the need to improve monitoring of grantees.²⁸ FEMA has taken the following steps to improve grants management and its oversight infrastructure:

- Began a multi-year effort to improve programmatic and financial monitoring. The Programmatic Grants Monitoring Improvement Initiative will expand and enhance programmatic monitoring capacity, as well as form comprehensive plans for future grants monitoring. In conjunction with this initiative, FEMA has launched a web-based system for its non-disaster grants, called ND Grants, to consolidate the entire preparedness (non-disaster) grants management lifecycle into a single system. In addition, the initiative will transition monitoring data to a web-based environment that will allow for greater ease of use, more sophisticated analytics, and greater data coordination with other reporting efforts. To enhance financial monitoring, FEMA has refined criteria for deciding which grants to monitor, standardized Regional financial monitoring activities, and expanded ongoing oversight activities to ensure early identification of issues.
- Increased regional management of grant programs to improve customer service to grantees, increase grants administration efficiencies, and build more robust regions. A recent GAO review indicates that FEMA is making progress in managing regionalization of preparedness grants.
- Established performance measures for the FY 2011 Homeland Security Grant Program and the Emergency Management Performance Grant Program, and is in the process of creating metrics for the remaining preparedness grant programs. FEMA states that internal and external management and administrative performance measures are being developed to track how well grants are being managed. However, until FEMA finalizes these measures, we are unable to evaluate their effectiveness.

FEMA is taking steps to improve its grants policies, procedures, systems, and processes, which when developed and implemented, should strengthen its grants management and oversight infrastructure. The following highlights the agency's progress in two key areas: disaster and preparedness grants management.

Disaster Grants Management

While FEMA does not directly manage subgrants, it is incumbent on FEMA to make certain that States, as grantees, understand the rules and regulations that govern disaster grants and ensure that subgrantees adhere to these. We issued a report in August 2011 that recapped the reports we issued in FY 2010 and presented some of the most common findings that lead to questioned costs, including improper contracting practices, inadequate subgrantee contract monitoring, costs not adequately supported, and ineligible work and project charges. We

²⁸ *The Post Katrina Emergency Management Reform Act of 2006* centralized most of DHS' grant programs under FEMA's Grant Programs Directorate (GPD).



also reported five instances in which grantee management could be improved. Grantees: (1) did not have procedures in place to ensure that cash advances to subgrantees were expended timely and excess funds were recovered promptly, (2) did not have a documented or standard payment processing policy or needed to strengthen controls to prevent overpayments, (3) had no procedures in place to follow up on material deficiencies reported in Single Audits, (4) were unaware of significant budget and scope increases, or (5) did not adequately monitor and report subgrantee program performance.

In FY 2011, we issued 61 subgrant audit reports with nearly \$308 million in questioned costs and over \$23 million in funding that could be deobligated or collected and be put to better use.

Preparedness Grants Management

FEMA faces challenges in mitigating redundancy and duplication among preparedness grant programs, including barriers at the legislative, departmental, and state levels. The preparedness grant application process risks being ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects. We made recommendations designed to improve the management of these grant programs, with which FEMA agreed. In FY 2010, FEMA added Operation Stonegarden to the cluster of programs comprising the Homeland Security Grant Program. For FY 2011, activities previously included in the former Buffer Zone Protection Program and Interoperable Emergency Communications Program became eligible in the Homeland Security Grant Program.

FEMA should be able to accomplish our recommendations by addressing the specific grant-related recommendations of the October 2010 report of the congressionally mandated Local, State, Tribal and Federal Preparedness Task Force. However, until FEMA finalizes implementation plans with target dates for the Task Force recommendations, we cannot adequately evaluate the corrective actions to our recommendations.

Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*, required the OIG to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the audits we have completed to date, we have determined that the states have generally done an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used. We have identified several instances of states, as grantees, insufficiently monitoring subgrantee compliance with grant terms. Further, most states could not clearly document critical improvements in preparedness as a result of grant awards. In addition, we noted a need for improvement in the areas of timeliness of grant fund obligations and expenditures, compliance with procurement and inventory requirements, and identification of long-term capability sustainment options.



FINANCIAL MANAGEMENT

In FY 2010, the Department committed to obtaining a qualified opinion on the Balance Sheet and Statement of Custodial Activity. To that end, DHS continued to improve financial management in FY 2011 and has achieved a significant milestone. For FY 2011, DHS was able to produce an auditable balance sheet and statement of custodial activity; and the independent auditors rendered a qualified opinion on those financial statements. However, challenges remain. In order to sustain or improve its opinion, the Department must continue remediating the remaining control deficiencies. Additionally, in FY 2012 the auditors could identify additional control deficiencies in areas that had not been tested previously due to the increase in audit scope to all of the financial statements. Additional deficiencies could also cause the department to lose its opinion.

Although the Department continued to remediate material weaknesses and reduce the number of conditions contributing to the material weaknesses, five of the six material conditions from FY 2010 were repeated in FY 2011. DHS made some progress in two of the material weaknesses, and accordingly, those conditions were narrowed in scope. Specifically, DHS corrected the weakness conditions related to financial management, but not the deficiencies related to financial reporting; hence, financial management and reporting was reduced to financial reporting. Additionally, the auditors noted improvement in internal controls over Actuarial Liabilities, primarily because the Coast Guard was able to assert to over \$40 billion of actuarial liabilities. The Coast Guard continues to have significant challenges in Environmental and Other Liabilities, which resulted in a material weakness for the Department during FY 2011. Further, as in previous years, the DHS Secretary has issued a statement of no assurance on the Department's internal controls over financial reporting, due to the existence of a pervasive material weakness, and limits on the scope of DHS' self assessment while focusing on remediation of control deficiencies. Consequently, the independent auditors were unable to render an opinion on DHS' internal controls over financial reporting in FY 2011.

During FY 2010, the independent auditors identified four department-wide control environment weaknesses that had a pervasive impact on the effectiveness of internal controls over consolidated financial reporting. In FY 2011, the independent auditors noted that only one of the four conditions still existed – the Department's financial information technology system infrastructure is aging and has limited functionality, which is hindering the Department's ability to implement efficient corrective actions and produce reliable financial statements. This issue is further discussed in the Information Technology Controls and Financial Systems Functionality section below.

The independent auditors noted that the DHS civilian components continued to make some progress in the remediation of IT findings that were reported in FY 2010. The Department closed approximately 31% of prior year IT findings. In FY 2011, the independent auditors issued approximately 135 findings, of which more than 65% are repeated from last year.

The remaining significant component-level challenges are primarily at the Coast Guard. In FY 2011, the Coast Guard made progress with implementing aspects of its *Financial Strategy for Transformation and Audit Readiness (FSTAR)* in the areas necessary to assert to



the auditability of its balance sheet, except for Property, Plant, & Equipment (PP&E), environmental liabilities, and related effects on other balance sheet line items. FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012.

Managerial Cost Accounting

The Department does not have the ability to provide timely cost information by major program, and strategic and performance goals as required by Office of Management and Budget Circular No. A-136, *Financial Reporting Requirements*, as amended. The Department does not have financial management systems that allow for the accumulation of costs, at the consolidated level, by major program, or allow for the accumulation of costs by responsibility segments that align directly with the major goals and outputs described in the entity's strategic and performance plans. Further, the Department has not developed a plan to implement managerial cost accounting, including necessary information systems functionality. Currently, the Department must use manual data calls to collect cost information from the various components and compile data on a consolidated basis.

The OIG conducted several audits during FY 2011 and found that a number of components did not have the ability to provide various cost data when requested. For example:

- In January 2011, we reported that CBP was unable to capture or track data related to the time officers and agents spend specifically on transportation and guard services for illegal aliens. Not having this data available prohibited CBP from having complete cost information to determine the most cost effective solution.²⁹ *U.S. Customs and Border Protection's Ground Transportation of Detainees*, OIG-11-27, January 2011.
- In March 2011, we issued a report on CBP's Efficacy of Controls Over Drug Seizures. During the course of the audit we learned that CBP was unable to estimate the cost of its drug seizure efforts.³⁰ *CBP's Efficacy of Controls Over Drug Seizures*, OIG-11-57, March 2011.
- In September 2011, we reported that the Coast Guard did not accurately capture and bill all indirect costs incurred for the Deepwater Horizon oil spill response effort. The results of the audit found that Coast Guard had adequate internal controls, policies, and procedures to accurately bill direct costs from the Deepwater Horizon oil spills, but the unprecedented size of the spill challenged its existing processes for capturing indirect costs and revealed weaknesses in these processes. The Coast Guard did not have adequate policies, procedures, and internal controls to ensure that indirect costs are verified using Coast Guard official systems of record.³¹ *United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill*, OIG-11-115, September 2011.

²⁹ DHS-OIG, *U.S. Customs and Border Protection's Ground Transportation of Detainees*, (OIG-11-27, January 2011).

³⁰ DHS-OIG, *CBP's Efficacy of Controls Over Drug Seizures*, (OIG-11-57, March 2011).

³¹ DHS OIG, *United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill*, (OIG-11-115, September 2011).



Anti-Deficiency Act Violations

The Department continues to have challenges with complying with the *Anti-Deficiency Act* (ADA). As of September 30, 2011, the Department reported six instances of potential ADA violations in various stages of review within the Department and its components.

Management at the Coast Guard continues to work toward resolving four potential ADA violations, one of which was identified during FY 2011. Those potential ADAs relate to (1) funds may have been used in advance of an approved apportionment from OMB, (2) funds used for construction and improvement projects, (3) funds that were inappropriately used for modifications to fixed price contract, and (4) the improper execution of the obligation and disbursement of funds for the lease of passenger vehicles.

Financial Statements Audit

The following six items present the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2010. Each item is divided into two categories: (1) Military – Coast Guard, and (2) Civilian – all other DHS components. These six items represent the six material weaknesses identified during the independent audit of the FY 2010 DHS consolidated balance sheet and statement of custodial activity. Five of the six weaknesses continued to exist throughout FY 2011 and were again noted in the FY 2011 Independent Auditors' Report. In FY 2011, the Fund Balance with Treasury material weakness was downgraded to a significant deficiency. Further, DHS made some progress in two of the material weaknesses, and accordingly, those conditions were narrowed in scope. Specifically, DHS corrected the weakness conditions related to financial management, but not the deficiencies related to financial reporting; hence, financial management and reporting was reduced to financial reporting. Additionally, the auditors noted improvement in internal controls over Actuarial Liabilities, primarily because Coast Guard was able to assert to over \$40 billion of actuarial liabilities. Coast Guard continues to have significant challenges in Environmental and Other Liabilities, which resulted in a material weakness for the Department during FY 2011. For a complete description of the internal control weaknesses identified in the FY 2010 audit, see OIG-11-09.³² To determine the status, we compared the material weaknesses reported by the independent auditor in FY 2010 with those identified in FY 2011.³³

Based on the consolidated result of the six financial management areas included in the report, DHS has made measurable progress overall in financial management.

³² DHS-OIG, *Independent Auditors' Report on DHS' FY 2010 Financial Statements and Internal Control over Financial Reporting*, (OIG-11-09, November 2010).

³³ DHS-OIG, *Independent Auditors' Report on DHS' FY 2011 Financial Statements and Internal Control Over Financial Reporting*, (OIG-12-07, November 2011).



Financial Reporting

Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period.

- **Military:**

In previous years, the independent auditors noted that the Coast Guard had several internal control deficiencies that led to a material weakness in financial reporting. To address the material weakness conditions, the Coast Guard developed its *Financial Strategy for Transformation and Audit Readiness*, which is a comprehensive plan to identify and correct conditions that are causing control deficiencies. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2010 included: (1) lack of sufficient financial management personnel to identify and address control weaknesses; and (2) lack of effective policies, procedures, and controls surrounding the financial reporting process.

The Coast Guard has made progress in remediating the numerous internal control weaknesses identified by the independent auditor during FY 2010 in financial reporting. The Coast Guard implemented new policies and procedures, and automated tools to improve internal controls and the reliability of its financial statements. This effort has allowed the Coast Guard to assert to the auditability of all balance sheet accounts except property, plant and equipment and environmental liabilities. However, the Coast Guard does not have properly designed, implemented, and effective policies, procedures, processes, and controls surrounding its financial reporting process. Further, the FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012. Consequently, components of the financial reporting deficiencies reported in the past remain uncorrected at September 30, 2011.

- **Civilian:**

In FY 2010, the independent auditors identified department-wide control weaknesses that have a pervasive effect on the effectiveness of internal controls over consolidated financial reporting. The auditors also found financial reporting internal control deficiencies at FEMA and TSA. Taken together, these deficiencies contributed to a departmental material weakness.

During FY 2011, the Department made progress overall in addressing the department-wide control weaknesses over consolidated financial reporting. The independent auditors noted that during FY 2011, FEMA corrected control deficiencies that contributed to the overall material weakness. Although TSA continued to make progress by hiring property accounting personnel and completing reconciliation of its balance sheet accounts, it has not fully developed its financial reporting process with sufficient policies, procedures, and internal controls to ensure reliability of certain significant financial statement balances. Further, in FY 2011, control deficiencies at USCIS



contributed to the Department's material weakness in financial reporting. The auditors noted that in FY 2011, the Department implemented a change in accounting treatment of certain user fees collected by USCIS. The change resulted in the correction of an error in the presentation of user fees as reported in previous years, and identification of a control weakness in the financial reporting process. The auditors also noted that USCIS did not have sufficient policies and procedures or documentation supporting the process used to develop adjustments to deferred revenue. These combined internal control deficiencies contributed to the Department's financial reporting material weakness in FY 2011.

Information Technology Controls and Financial Systems Functionality

IT general and application controls are essential for achieving effective and reliable reporting of financial and performance data.

- Military:

A number of the Coast Guard's challenges in financial reporting are due to the lack of an effective general ledger system. The Coast Guard currently uses multiple systems that do not comply with the requirements of the *Federal Financial Management Improvement Act*.

In previous years the independent auditors noted that one of the most significant IT issues at the Coast Guard that could affect the reliability of the financial statements related to the development, implementation, and tracking of IT scripts, and the design and implementation of configuration management policies and procedures.

During FY 2011, Coast Guard focused on improving documentation with the script change control process and implemented the final module of the script change management tool initiated in FY 2010. While the independent auditors noted that some previously identified control deficiencies were remediated, other deficiencies continued to exist. Coast Guard's core financial system configuration management process and financial system functionality remained a challenge to Coast Guard's ability to assert to all financial sheet balances during FY 2011. The auditors noted that the IT security access and configuration management controls were not operating effectively, and continued to present risks to DHS financial data confidentiality, integrity, and availability. Financial system functionality is inhibiting the Coast Guard's ability to implement and maintain internal controls supporting financial system data processing and reporting.

The independent auditors also reported that financial data in the general ledger might be compromised by automated and manual changes that are not adequately controlled. The changes are implemented through the use of an IT scripting process, which was instituted as a solution to address functionality



and data quality issues. However, the controls over the script process were not properly designed or implemented effectively.

Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls necessary to support accurate and reliable financial data. For example, existing limitations impair Coast Guard's ability to maintain adequate posting logic transaction codes to ensure that transactions are recorded in accordance with U.S. generally accepted accounting principles.

- Civilian:

During FY 2010, the independent auditor identified IT control weaknesses in five areas that continued to present risks to the confidentiality, integrity, and availability of DHS' financial data: (1) access controls, (2) configuration management, (3) security management, (4) contingency planning, and (5) segregation of duties. Additionally, the independent auditors noted that in some cases financial system functionality inhibited DHS' ability to implement and maintain or install internal controls. These combined internal control deficiencies contributed to the Department's financial management and reporting material weakness in FY 2010.

For FY 2011, DHS has made limited progress overall in correcting the IT general and applications control weaknesses identified in the FY 2010 Independent Auditors' Report. During FY 2011, DHS and its components corrected approximately 31% of the IT control weakness conditions that the auditors had identified in prior years. Coast Guard, FEMA, Federal Law Enforcement Training Center (FLETC), and ICE made the most progress in remediating the IT control weaknesses. Although conditions improved at Coast Guard, FEMA, FLETC, and ICE, conditions at CBP deteriorated during the year. The majority of new control deficiencies the independent auditors identified during the year were at CBP.

The auditors noted that at the end of FY 2011, over 135 IT control weakness conditions existed, of which more than 65% are repeat from last year. Approximately 25% of the repeat findings were for IT deficiencies that management represented were corrected during FY 2011.

The auditors noted that many of the financial systems in use at DHS components have been inherited from the legacy agencies and have not been substantially updated since DHS' inception. As a result, ongoing financial system functionality limitations are contributing to the Department's challenges in addressing systemic internal control weaknesses and strengthening the overall control environment.

The FY 2011 Independent Auditors' Report noted that the IT control weaknesses remained for the five areas and continued to present risks to the



confidentiality, integrity, and availability of DHS' financial data: (1) access controls, (2) configuration management, (3) security management, (4) contingency planning, and (5) segregation of duties.

Property, Plant, and Equipment

DHS capital assets and supplies consist of items such as property, plant, and equipment, operating materials; and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.

- Military:

The Coast Guard maintains approximately 49% of the Department's PP&E, including a large fleet of boats and vessels.

For FY 2010, the independent auditors noted that the Coast Guard had difficulty establishing its opening PP&E balances primarily because of poorly designed policies, procedures, and processes implemented, combined with ineffective internal controls. PP&E was not properly tracked or accounted for many years preceding the Coast Guard's transfer to DHS in 2003.

Furthermore, the fixed asset module of the Coast Guard's Core Accounting System (CAS) was not being updated timely for effective tracking and reporting of PP&E on an ongoing basis. As a result, the Coast Guard was unable to accurately account for its PP&E, and provide necessary information to DHS' Office of Financial Management for consolidated financial statement purposes.

In FY 2011, the Coast Guard continued to execute remediation efforts to address PP&E process and control deficiencies, specifically those deficiencies associated with vessels, small boats, aircraft, and select construction in process projects. Remediation efforts are scheduled to occur over a multi-year timeframe beyond FY 2011. Consequently, the Coast Guard has made only limited progress in this area during FY 2011.

- Civilian:

During FY 2010, CBP and TSA contributed to a departmental material weakness in PP&E. The deficiencies at TSA were more severe than at CBP.

Although TSA made some progress in remediating control deficiencies during FY 2011, including having auditable beginning internal use software balance, it was unable to fully address all of the conditions that existed in FY 2010.

Consequently, the overall severity of its internal control weakness conditions remained throughout FY 2011. Likewise, although CBP demonstrated some progress in remediating control deficiencies during FY 2011, the auditors identified control deficiencies similar to those noted in the prior year. Further,



internal control deficiencies were identified in the Office of Management that contributed to the overall DHS material weakness.

Environmental and Other Liabilities

Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including environmental, accounts payable, legal, and accrued payroll and benefits liabilities.

- Military:

The Coast Guard's environmental liabilities consist of environmental remediation, clean up, and decommissioning, and represent approximately \$973 million or 93% of total DHS environmental liabilities. Environmental liabilities are categorized as relating to shore facilities and vessels. Shore facilities include any facilities or property other than ships (e.g. buildings, fuel tanks, lighthouses, small arms firing ranges, etc).

The independent auditors noted that during FY 2011, the Coast Guard continued to implement a multi-year remediation plan to address process and control deficiencies related to environmental liabilities. As a result, the Coast Guard made limited progress in implementing policies and procedures. However, most of the control weakness conditions reported in the FY 2010 Independent Auditors' Report remained throughout FY 2011.

- Civilian:

No control deficiencies related to Environmental and Other Liabilities were identified at the civilian components in FY 2011.

Budgetary Accounting

Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.

- Military:

The Coast Guard has over 80 Treasury Account Fund Symbol (TAFS) covering a broad spectrum of budget authority, including annual, multi-year, and no-year appropriations; and several revolving, special, and trust funds. Each TAFS with separate budgetary accounts must be maintained in accordance with OMB and Treasury guidance.

Many of the conditions that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2010 remained throughout FY 2011. For example, the Coast Guard has not fully implemented policies, procedures, and internal controls over its process for validation and verification of undelivered order balances.



- Civilian:

For FY 2010, internal control weaknesses at CBP and FEMA contributed to a material weakness in budgetary accounting for the Department.

During FY 2011, the Department demonstrated moderate progress in correcting the budgetary accounting material weakness. The independent auditors noted that corrective actions CBP implemented during FY 2010 continued to be effective throughout FY 2011. Additionally, during FY 2011 FEMA continued to improve its processes and internal control over the obligation and monitoring process. However, some control deficiencies remained at FEMA. The control deficiencies at FEMA, combined with those at Coast Guard resulted in an overall material weakness in the area for the Department.

Fund Balance with Treasury

Fund Balance with Treasury (FBWT) represents accounts held at the Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency's FBWT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of various U.S. Government financial reports, and providing a more accurate measurement of budget resources.

- Military:

FBWT at the Coast Guard represents approximately 11% of total DHS FBWT. During FY 2010, the independent auditors reported a material weakness in internal control over FBWT at the Coast Guard. During FY 2011, the Coast Guard corrected several significant control deficiencies around FBWT. As a result, Coast Guard was able to assert to the completeness, existence, and accuracy of FBWT.

However, the Coast Guard continues to have FBWT control deficiencies. For example, Coast Guard does not have a process in place to provide transaction-level supporting documentation for all reconciling items. Consequently, some of the weakness conditions that were reported in FY 2010 remain throughout FY 2011. The auditors consider the remaining weaknesses to be less severe, but still important enough to require management's attention.

- Civilian:

No control deficiencies related to FBWT were identified at the civilian components in FY 2011. Corrective actions implemented in previous years continued to be effective throughout FY 2010 and FY 2011.



INFRASTRUCTURE PROTECTION

The need to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, and minimize incident consequences complicates protection efforts for all critical infrastructure and key resources and remains a great challenge for DHS.

Risk Assessment Efforts in the Dams Sector

Dams and related structures are especially important because one catastrophic failure at some locations could affect populations exceeding 100,000 and have economic consequences surpassing \$10 billion. We reviewed the Department's risk assessments effort in the Dams Sector³⁴ to determine whether the Office of Infrastructure Protection has taken steps to assess risk at the most critical dam assets, and followed up to ensure that recommendations were implemented. We found the Department lacks assurance that risk assessments were conducted and security risks associated with critical dam assets were identified and mitigated. The Department did not: (1) review all critical dam asset risk assessments conducted by other agencies, (2) conduct security reviews for 55% of the critical dam assets, or (3) ensure that corrective actions were completed to mitigate risk when security gaps were identified.

DHS was unable to complete these tasks because it does not have the authority to ensure that security partners participate in risk management activities or that dam owners undergo departmental assessments and implement corrective action. The National Infrastructure Protection Plan prescribes a partnership approach between government and the private sector to voluntarily manage risk. Underlying legislation does not give the Department the necessary authority to ensure that security partners participate in risk management activities, or that dam owners undergo departmental assessments and implement corrective action. DHS could not always obtain cooperation from its security partners and dam owners and did not always collaborate successfully. This collaborative approach can be successful only if security partners and dam owners work together to perform risk management. The Assistant Secretary, Office of Infrastructure Protection, agreed with our recommendation to determine the appropriateness of a legislative proposal to establish regulatory authority for the critical Dams Sector assets similar to the Chemical Sector. Specifically, DHS personnel need authority to review risk assessments, conduct inspections when assessments are deficient, and make recommendations for corrective actions.

BORDER SECURITY

Securing the Nation's borders from the illegal entry of aliens, contraband, terrorists and weapons of mass destruction, while welcoming all legitimate travelers and trade, continues to be a major challenge. DHS apprehends hundreds of thousands of people and seizes volumes of illicit cargo entering the country each year. DHS is responsible for securing the 7,000 miles of international borders that the United States shares with Canada and Mexico.

³⁴ DHS-OIG, *DHS Risk Assessment Efforts in the Dams Sector*, (OIG-11-110, September 2011).



Western Hemisphere Travel Initiative

To address the challenge of facilitating the entrance of legitimate travelers while securing the Nation from illegal entry of aliens and terrorists, DHS and Department of State implemented the Western Hemisphere Travel Initiative (WHTI). WHTI requires citizens of the United States, Canada, Bermuda, and Mexico arriving at air, land and sea ports of entry to present passports or other approved documents to enter the United States. CBP is not prepared to fully enforce the new document requirement at land ports of entry. CBP has acquired and deployed substantial technological tools to aid in inspecting travelers arriving at land ports of entry. However, CBP has not analyzed the impact that a substantial increase in secondary inspection workload will have on secondary inspection staffing and infrastructure during full enforcement. The reported WHTI compliance rates during the initial eight-month informed compliance period indicate noncompliant travelers arriving at the agency's 39 busiest land ports may increase the secondary inspection workloads at these ports by an average of 73% if all noncompliant travelers required secondary inspections. Also, the agency has not finalized the operating procedures its officers will use to verify the identity and citizenship of noncompliant travelers.³⁵

CBP's implementation of the WHTI document requirements have improved the agency's ability to validate the identity and citizenship of compliant air passengers, allowing officers to spend more time inspecting travelers without passports. However, there is inadequate assurance that CBP officers "verified" the identity and citizenship of all individuals who failed to provide a passport or other WHTI-compliant documentation. CBP officers did not always document the basis for their decisions to admit air passengers who were noncompliant with the new document requirements. Also, CBP officers did not always follow the agency's policy for referring all noncompliant passengers to a secondary inspection area for a more thorough review.³⁶

Information Sharing on Foreign Nationals: Overseas Screening

DHS has implemented several programs to screen foreign nationals while they are still overseas. These programs rely on biographical, biometric, and documentary information in the Department's and other federal data systems. In our FY 2011 report, *Information Sharing on Foreign Nationals: Overseas Screening (Redacted)*,³⁷ we evaluated whether levels of cooperation, resources, and technology were adequate for Department officers to assess the risks posed by foreign nationals who seek to enter the United States. We also reviewed plans to consolidate and improve information in the Department's data systems. The Department has made progress in evaluating admissibility of foreign nationals before they travel to the United States. The level of cooperation among components that conduct overseas screening is high. Headquarters support offices have long-term plans to streamline

³⁵ DHS-OIG, *Customs and Border Protection's Implementation of the Western Hemisphere Travel Initiative at Land Ports of Entry*, (OIG-11-16, November 2010).

³⁶ DHS-OIG, *Customs and Border Protection Needs To Improve Its Inspection Procedures for the Western Hemisphere Travel Initiative* (OIG-11-43, February 2011).

³⁷ DHS-OIG, *Information Sharing On Foreign Nationals: Overseas Screening (Redacted)*, (OIG-11-68, April 2011).



access to information in the Department's data systems, and improve screening and data analysis capabilities. However, DHS initiatives face serious resource and technological challenges. Information is fragmented among more than 17 data systems, and officers must conduct labor intensive, system-by-system checks to verify or eliminate each possible match to terrorist watch lists and other derogatory information.

CBP's National Targeting Center is challenged by insufficient staff and difficult working conditions. Effective small-scale screening and interdiction programs need sufficient resources to meet operational needs and congressional mandates. We made 18 recommendations to standardize the technology used to share information in Departmental data systems, enable federal officers to obtain and use the most current and complete data available, and improve information sharing procedures. Departmental components concurred with 17 of the 18 recommendations. However, for five recommendations with which components concurred, including three that would increase productivity for thousands of DHS employees, components said that they would need to request additional resources in the next federal budget cycle to implement the recommendations.

TRANSPORTATION SECURITY

TSA is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. The Nation's economy depends upon secure, yet efficient transportation security measures. Although TSA is making progress, it continues to face challenges with strengthening security for aviation, mass transit and other modes of transportation.

Passenger and Baggage Screening

TSA's screening of persons and property continues to be a vital element of the overall aviation security system. The *Aviation and Transportation Security Act*³⁸ requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our covert testing of carry-on baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not cleared for loading onto a passenger aircraft.³⁹ The same report identified needed improvements for TSA's Advanced Imaging Technology.

Airport Badging Process Oversight

TSA's responsibilities include ensuring that employees working in secured airport areas are properly vetted and badged. The agency relies on designated airport operator employees to perform the badging application process. We reported that individuals who pose a threat may obtain airport badges and gain access to secured airport areas.⁴⁰ We analyzed vetting

³⁸ Public Law 107-71, November 19, 2001.

³⁹ DHS-OIG, *Evaluation of Newly Deployed and Enhanced Technology and Practices at the Passenger Screening Checkpoint (Unclassified Summary)* (OIG-10-75, March 2010).

⁴⁰ DHS-OIG, *TSA's Oversight of the Airport Badging Process Needs Improvement (Redacted)* (OIG-11-95, July 2011).



data from airport badging offices and identified badge holder records with omissions or inaccuracies pertaining to security threat assessment status, birthdates, and birthplaces.

These problems exist because TSA has designed and implemented only limited oversight of the application process. Specifically, the agency did not (1) ensure that airport operators have quality assurance procedures for the badging application process; (2) ensure that airport operators provide training and tools to designated badge office employees; and (3) require its Transportation Security Inspectors to verify the airport data during their reviews.

Passenger Air Cargo Security

Approximately 7.6 million pounds of cargo are transported on passenger planes each day. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably “known” either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. Through covert testing, we identified vulnerabilities in the cargo screening procedures employed by air carriers and cargo screening facilities to detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.⁴¹ Although TSA has taken steps to address air cargo security vulnerabilities, our undercover audit demonstrated that the agency does not have assurance that cargo screening methods always detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.

Training

Transportation Security Officers screen passengers, carry-on baggage, and checked baggage to prevent prohibited objects from being transported on aircraft. TSA can improve its management of the training program for the screening workforce.⁴² The agency needs to develop and document standard processes to (1) use officer test results to evaluate training program results; (2) assign on-the-job training responsibilities; and (3) evaluate workforce and training needs to ensure that officers have the tools and time necessary to complete training requirements.

TSA did not establish a lead office to organize and coordinate Transportation Security Officer training until 2006. The agency issued a management directive designating the Operational and Technical Training Division responsible for the overall management of the analysis, design, development, and implementation of Transportation Security Officer training programs. However, the division did not assume an active leadership role until 2009 due to its need to maintain current training levels and respond to emerging threats. Without a documented process for updating training based on screener performance data and changes in technology or equipment, the TSA may be missing opportunities to enhance its officers’ skills and abilities.

⁴¹ DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft*. (OIG-10-119, September 2010).

⁴² DHS-OIG, *Transportation Security Administration’s Management of Its Screening Workforce Training Program Can Be Improved* (OIG-11-05, October 2010).



Rail and Mass Transit

Passenger rail stations are attractive terrorist targets because of the large number of people in a concentrated area. Amtrak provides passenger rail service for about 27 million passengers every year, using approximately 22,000 miles of rail in 46 states and the District of Columbia. We identified that grant recipients, such as Amtrak, transit agencies, and state and local authorities, coordinate risk mitigation projects at high-risk rail stations. However, Amtrak is not always using grant funds to implement mitigation strategies at the highest risk rail stations, in terms of casualties and economic impact.⁴³ Amtrak has not mitigated critical vulnerabilities reported in risk assessments. These vulnerabilities remain because TSA (1) did not require Amtrak to develop a corrective action plan addressing its highest ranked vulnerabilities; (2) approved Amtrak investment justifications for lower risk vulnerabilities; and (3) did not document roles and responsibilities for the grant award process.

The Transportation Sector Network Management, Mass Transit and Passenger Rail Division, needs to work closely with Amtrak to establish a corrective action plan that ensures decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by previous risk assessments. The Transportation Sector Network Management, Mass Transit and Passenger Rail Division needs to create and report internal procedures that describe how the agency will carry out its roles and responsibilities in the grant award process for ensuring that Amtrak and other grant recipients address the highest priority security vulnerabilities.

TRADE OPERATIONS AND SECURITY

CBP is charged with the dual mission of securing the Nation's borders, while facilitating legitimate trade and travel. While CBP continues to take action in this area, challenges remain with strengthening internal controls over revenue and protecting our Nation from security threats.

Customs Revenue

Customs revenue remains the second largest source of revenue for the U.S. government. CBP collected an estimated \$32 billion in duties, fees, and taxes (revenue) in FY 2010, an increase of 9.5% over FY 2009. In the current economic environment, it is imperative CBP ensure that participating importers comply with federal trade requirements and that government revenues are protected. In 2010 and 2011, OIG conducted revenue audits of the Importer Self Assessment program⁴⁴ and the Single Transaction Bonds process⁴⁵ and found significant issues remain with oversight of these programs. The Importer Self Assessment program was initiated in 2002 as a voluntary approach to trade compliance. It is based on the

⁴³ DHS-OIG, *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations (Redacted)* (OIG-11-93, June 2011).

⁴⁴ DHS-OIG, *Customs and Border Protection's Importer Self-Assessment Program*, (OIG-10-113, August 2010).

⁴⁵ DHS-OIG, *Information Technology Management Letter for the Federal Emergency Management Agency Component for the FY 2009 DHS Integrated Audit*, (OIG-10-92, May 2010).



premise that importers with strong internal controls achieve the highest level of compliance with federal trade laws and regulations and require less enforcement review and oversight. Our most recent review highlighted several areas where improvement can be made, including establishing and enforcing policies and procedures to document management controls and assessing risks to trade compliance.

Further, we noted that CBP needs to improve internal controls over the Single Transaction Bonds process which protects CBP from revenue loss when importers fail to fulfill their financial obligations. In 2011, the OIG conducted an audit of CBP's Single Transaction Bond program and found that from FY 2007 through FY 2010, CBP lost \$46.3 million in revenue because of inaccurate, incomplete, or missing bonds. We recommended that CBP develop a risk based approach that includes identification, assessment, and mitigation of the risk of revenue loss associated with the single transaction bonding process.

Cargo Security

Ensuring that only legitimate cargo is allowed entry into the United States while facilitating the free flow of trade remains a challenge. Based on our FY 2010 audits, *CBP's Cargo Targeting and Examinations*⁴⁶ and *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*,⁴⁷ we concluded that targeting and examination of high risk shipments continues to be a challenge for CBP. For example, CBP needs to update its guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats and conduct a risk assessment to determine which pathways pose the highest risk.

The Free and Secure Trade (FAST) program is a commercial clearance program for known low-risk shipments entering the United States from Canada and Mexico. FAST allows for expedited processing of entities that have completed background checks and fulfill certain eligibility requirements. Improvements are needed in CBP's initial enrollment process for carriers to ensure that only low-risk carriers are allowed to participate in the FAST program. Highway carriers that did not meet all Custom-Trade Partnership against Terrorism's minimum security requirements have been certified to receive FAST program benefits. Also, the CBP Vetting Center and Trade Partnership against Terrorism supply chain security specialists did not always follow established procedures when determining the initial eligibility of highway carriers.⁴⁸

Developing and maintaining a multi-layered risk based approach to trade security is a significant challenge. Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* requires DHS to screen all cargo destined for the U.S. that is loaded on or after July 1, 2012. Over the past two years, CBP and DHS have raised concerns to Congress about the feasibility of 100% screening and have advocated for continuing to use a


⁴⁶ DHS-OIG, *Cargo Targeting and Examinations*. (OIG-10-34, January 2010).

⁴⁷ DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*. (OIG-10-01, October 2009).

⁴⁸ DHS-OIG, *Improvements Needed in the Process to Certify Carriers for the Free and Secure Trade Program* (OIG-11-25, March 2011).



risk-based approach to meet the intent of mitigating high risk cargo. Regardless of whether DHS formally adopts 100% screening or continues to use its risk-based approach to trade security, DHS must ensure that it has adequate resources, infrastructure, and processes. DHS must also be able to reach agreement with the international community to resolve issues concerning corresponding resources, oversight, costs, timing, and enforcement considerations, as well as a process to resolve disagreements as they arise.



Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary Management
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

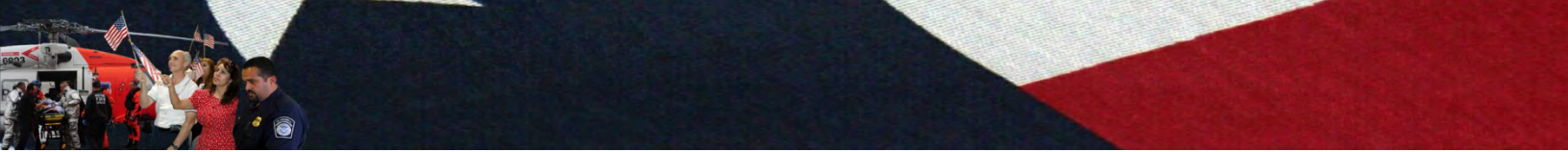
To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov, or visit our OIG websites at www.dhs.gov/oig or www.oig.dhs.gov.

OIG HOTLINE

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

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

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



Management's Response

The Reports Consolidation Act of 2000 (P.L. 106-531) requires that, annually, the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) prepare a statement summarizing the major management challenges facing the Department and an assessment of the Department's progress in addressing those challenges. For Fiscal Year (FY) 2011, the OIG has identified the Department's major challenges in nine broad areas:

- Acquisition Management
- Information Technology (IT) Management
- Emergency Management
- Grants Management
- Financial Management
- Infrastructure Protection
- Border Security
- Transportation Security
- Trade Operations and Security

DHS carries out multiple complex and highly diverse missions. While the Department continually strives to improve the efficiency and effectiveness of its programs and operations, as progress is achieved, new management challenges arise.

Overcoming major management challenges requires long-term strategies for ensuring stable operations, sustained management attention, and resources. This section of the report details the Department's efforts to address each of the aforementioned challenges and the plans it has in place to overcome specific issues highlighted by the OIG.

Challenge #1: Acquisition Management

An effective acquisition management infrastructure is essential to support the Department's mission. Effective acquisition management requires having the people, policies, and systems in place to ensure taxpayer assets are effectively and efficiently utilized. This is accomplished by having a combination of people who are experts in various disciplines, including program management, policy, operations, contracting, engineering, information technology, logistics, business and financial management, cost analysis, and testing and evaluation. Recognizing this, DHS established a core of acquisition experts at the Department to perform the appropriate governance, as well as coaching, guidance, and support to help execute programs well on a day-to-day basis. To lead this effort and enhance the Department's ability to effectively provide capability to users in support of DHS goals and objectives, the Acquisition Program Management Division (APMD) was established within the Office of the Chief Procurement Officer (OCPO) in 2007 to lead DHS in matters relating to acquisition.

According to the OIG, the magnitude of the number, dollar value, and complexity of the Department's acquisition activities keeps acquisition management among its challenges. The OIG also points out that DHS continues to make progress in this area. We agree with both assessments and continue to work to improve our acquisition management infrastructure for providing oversight



of DHS's many complex and large-dollar procurements. The OIG identified the following challenges that need to be addressed: Organizational Alignment and Leadership; Policies and Processes; Acquisition Workforce; and Knowledge Management and Information Systems.

Sub-Challenge: Organizational Alignment and Leadership

DHS agrees with the OIG's assessment that in FY 2011 the Department improved the acquisition program's organizational alignment and maintained strong executive leadership, but has room for further improvement. Specifically, there are several accomplishments we would like to highlight. For example, DHS acquisition management was reorganized to reflect a layered approach, with the Component chief acquisition executives and the heads of contracting activities reporting informally to the Under Secretary for Management (USM) and OCPO, respectively. In addition, in response to a U.S. Government Accountability Office (GAO) report, DHS has taken action to implement its Integrated Strategy for High Risk Management. Specifically, DHS has:

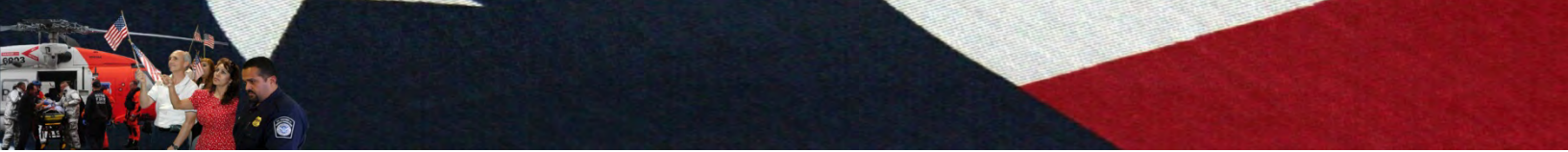
- Established the Program Accountability and Risk Management Office, reporting directly to the USM, combining the Acquisition Program Management Division and the Cost Analysis Division under one executive director;
- Completed a workforce study, the results of which have been used to augment acquisition staff for programs and Components;
- Completed a requirements definition for a decision support tool to improve business intelligence on programs (including tracking the efficacy of required actions resulting from oversight activities); and
- Begun chartering work for the implementation of the Integrated Investment Life Cycle Model (IILCM).

These actions have already established an improved acquisition management infrastructure, including much of what is needed to address GAO's concerns regarding workforce needs. DHS plans to complete implementation of IILCM as well as the first phases of the decision support tool deployment in FY 2012 in order to fully address GAO's and OIG's concerns regarding this management challenge.

Sub-Challenge: Policies and Processes

DHS continues to develop and strengthen its acquisition management policies and processes. According to the OIG, the Department needs to provide detailed guidance and improve oversight and internal controls in some areas, such as the logistics process used to facilitate strategic sourcing of detection equipment. In response, the DHS Strategic Sourcing Program Office conducted a business case analysis to determine the feasibility of procuring detection equipment under a strategic sourcing vehicle(s). The business case concludes that strategic sourcing for detection equipment can potentially eliminate duplication and reduce costs by leveraging purchase volume.

On September 8, 2011, the USM established an Executive Steering Committee (ESC) and a Commodity Working Group (CWG) for detection equipment. The purpose of this initiative is to develop a coordinated approach and apply strategic sourcing principles to the acquisition and management of detection equipment.



Moving forward, the CWG will be responsible for developing a coordinated approach to acquiring and managing detection equipment as it implements a strategic sourcing solution and completes all necessary tasks (i.e., identify requirements, perform market research, and develop sourcing strategy). The ESC will be responsible for approving the final requirements, ensuring the CWG has adequate resources, and resolving any key issues encountered by the CWG.

A DHS-wide detection equipment contract will provide a vehicle for efficient acquisition and improved commodity management. Further, leveraging buying power for detection equipment will reduce costs for DHS and its Components. DHS anticipates a strategically sourced contract vehicle to be awarded in FY 2013.

Sub-Challenge: Acquisition Workforce

DHS continues to make progress in recruiting and retaining a workforce capable of managing a complex acquisition program, as noted by the OIG, and will continue to evaluate workforce needs and make adjustments as appropriate to address this challenge. According to GAO, the U.S. Coast Guard reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent and filled 832 of its 951 acquisition positions as of November 2010. Following participation in a DHS-wide pilot, the U.S. Coast Guard was awarded a contract with Dayton Aerospace, Inc. to provide a Sustainment Acquisition Composite Model (S/ACOM) for project acquisition workforce staffing requirements. The model projects current and future year (5-year) requirements in accordance with the DHS Future Years Homeland Security Program and provides a functional breakout for all major system acquisition projects.

S/ACOM helped the U.S. Coast Guard identify and close a 100 full-time position (FTP) resource gap within its major systems acquisition workforce. Using direct/expedited hire authority for civilian recruitment and the current process for military personnel assignments, the U.S. Coast Guard has sufficient authority to reduce the 14-percent vacancy rate. The current staffing and acquisition certification level for U.S. Coast Guard major systems acquisitions is sufficient to successfully execute the programs as contained in the President's Budget Request for FY 2012. In addition, this request contains 17 new FTPs to strengthen oversight and meet the highest acquisition priorities in systems engineering, life-cycle logistics, test & evaluation, and business financial management. The U.S. Coast Guard will continue to use S/ACOM in their workforce planning efforts to project future requirements and to determine if current acquisition staffing is sufficient.

In addition, to help address a challenge identified by the OIG, FEMA recently revised its policy to allow disaster assistance employees performing contracting functions to be classified as General Schedule (GS)-1102, Contract Specialists. This will greatly improve FEMA's ability to attract and recruit experienced contracting officers with higher contracting authority to work at disaster sites. The change will also decrease turnover rates and allow for smooth contract execution.

Sub-Challenge: Knowledge Management and Information Systems

DHS agrees with the OIG that the Department has made progress in deploying an enterprise acquisition information system and tracking key acquisition data. This progress is highlighted by reports from the Department's acquisition reporting system of record (nPRS), dated October 3, 2011, showing 13 of 17 programs having approved Acquisition Program Baselines and 2 more in final routing at the Department level. In addition, Components use this system to enter and update



acquisition documentation (i.e., cost, budget, performance, and schedule data). The system shows 15 of 17 programs have key acquisition documentation from Components, while the remaining 2 programs had the documentation prepared but not yet entered. These improvements were the result of a concentrated effort by APMD/Program Accountability and Risk Management in FY 2011 to ensure critical thinking for this program had been documented.

Challenge #2: Information Technology Management

DHS continues to work to enhance the Department's information management, and DHS Components have made progress in addressing challenges with these systems identified by the OIG and in providing greater assurance that DHS-held information is protected. The Chief Information Officer (CIO) will continue to provide oversight of IT systems consolidation efforts, including Enterprise Wireless Infrastructure (EWI) security, the OneNet Project, and the DHS Data Center.

Sub-Challenge: IT and Cybersecurity

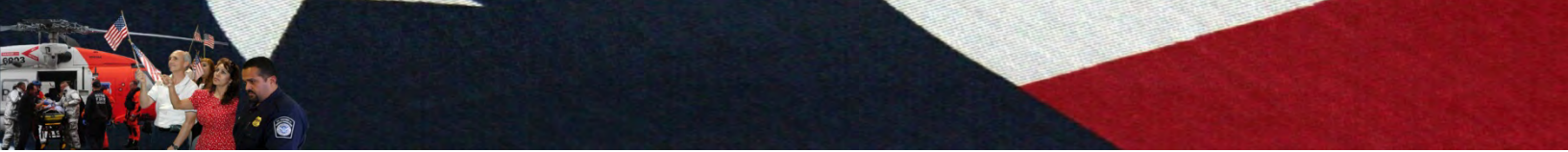
DHS agrees with the OIG that the Department has continued to improve and strengthen its security program but challenges still remain to further strengthen IT security. In January 2011, the Chief Information Security Officer (CISO) issued and implemented the *IT Security Continuous Monitoring Strategy: An Enterprise View v1.0* to meet OMB and National Institute of Standards and Technology (NIST) guidance.

U.S. Customs and Border Protection (CBP) has made considerable progress in strengthening EWI security to address a recent OIG recommendation that it needs to strengthen enterprise wireless infrastructure security by remediating its open Plan of Action and Milestones (POA&Ms). Specifically, CBP published policy and implemented guidance in 2009 for developing and implementing the CBP wireless security program. In July 2010, CBP certified and accredited EWI in accordance with processes outlined by NIST. The certification process for EWI included a review of all required documentation, such as a system security plan, risk assessment, and a system test and evaluation plan. In addition, CBP performed an independent security test and evaluation, and established wireless security configurations to protect wireless networks and devices against security vulnerabilities. Also, CBP included wireless security awareness in its annual security awareness and rules of behavior training.

CBP is addressing its open POA&Ms. To date, CBP reviewed and re-baselined the master POA&M list and schedule with the Information Systems Security Manager, to remediate which POA&Ms can be closed and to open new ones to reflect actions that are still needed to minimize potential security risks. Depending on funding approval timelines, CBP will commence with risk mitigation activities, procurement, and staffing actions.

In addition, CBP has enabled the wireless intrusion detection system but is not currently monitoring the system. CBP has a transition plan in place to monitor the system and has created a resource requirements request to obtain the necessary funding.

CBP has also set up vulnerability scans for all EWI Wireless Controllers. These scans will be conducted by CBP's wireless Information Systems Security Officer. CBP is developing a schedule



to ensure that vulnerability scans are conducted on a regular and recurring basis by December 2011.

In early February 2011, the U.S. Citizenship and Immigration Services (USCIS) Office of Security and Integrity (OSI) initiated a Risk Management Special Review to identify current risk management efforts across USCIS, gauge their effectiveness, and determine steps to be taken in order to coordinate and enhance enterprise risk management at USCIS. A charter and work plan were prepared, and OSI formed the Enterprise Risk Management Task Force. Staff members from OSI met with DHS risk management officials, attended risk management training, created a database for the project, and started a pilot risk management program within OSI. At the successful conclusion of the pilot, OSI will form a USCIS-wide task force to explore implementation of the program throughout USCIS.

Other accomplishments include appointment of a Senior Risk Executive to oversee the development of the USCIS Risk Management Office and to represent USCIS within the DHS Risk Management Office, and the completion of drafts currently under review by the Enterprise Risk Management Task Force, including:

- Management Directive that establishes authorities, responsibilities, and procedures;
- Process flow chart that outlines risk identification, mitigation, and information lines of communication; and
- White paper that outlines a general approach to establishing a risk management office and the steps necessary to establish an effective risk management process within USCIS.

In addition, USCIS is working with the Office of Transformation Coordination to establish requirements to enhance the Electronic Immigration System's (ELIS's) ability to address insider threats. DHS officials are actively engaged on the appropriate project teams to ensure additional internal risk mitigation strategies are addressed in ELIS. These requirements are currently planned for inclusion in the Release B of ELIS, which is scheduled to begin development late FY 2012.

The National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (NPPD/IP) works closely with the DHS Data Center to ensure its personnel receive protected critical infrastructure information (PCII) training. The PCII Program is an information-protection program that enhances information sharing between the private sector and the government. In addition, PCII is used by DHS and other federal, state, and local analysts to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures. All DHS Data Center personnel with access to NPPD systems that house PCII data have completed PCII training.

The DHS Data Center is responsible for ensuring the appropriate implementation of many of the security and system configuration controls associated with NPPD systems. In June 2011, the DHS CIO released an initial version of the Enterprise Common Controls, Data Center Two, Service Level Two guidance document, which is intended to supplement previous service agreements and clearly articulate which security and configuration controls are the responsibility of the DHS Data Center and how they should be implemented.



DHS, NPPD, and NPPD/IP information system security management personnel have reviewed current system security standards and documentation to achieve continued authority to operate until April 2014. In addition, when application configuration concerns are identified, they are addressed through business processes and/or software patch updates.

The National Cyber Security Division (NCSD) is the DHS entity with lead responsibility for implementing or coordinating, as appropriate, the National Strategy to Secure Cyberspace, National Infrastructure Protection Plan cybersecurity activities, and the Comprehensive National Cybersecurity Initiative. NCSD is developing a draft strategic plan that will include “performance measures that are aligned with its mission, as outlined in the Quadrennial Homeland Security and Bottom-Up reviews.” NCSD’s strategic plan is progressing through the approval process and includes a plan for developing implementation schedules for each goal within the strategic plan.

In addition, NCSD reports its performance on a quarterly basis against the measures it developed. At the same time, NCSD continuously assesses its current suite of measures and measure gaps, and then develops new measures to close identified gaps. Lastly, the Office of Cybersecurity and Communications is implementing corrective actions to address gaps identified by the OIG to ensure cybersecurity and communications programs are appropriately aligned and their overall performance is adequately assessed.

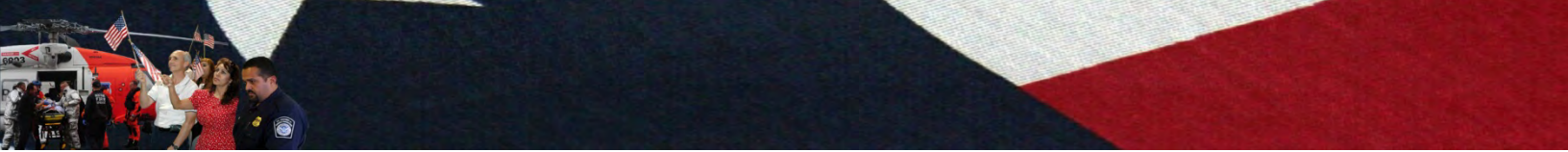
Sub-Challenge: IT Management

DHS and its Components are working to address the OIG’s recommendations to overcome challenges in upgrading their respective IT infrastructures, both locally and enterprise-wide. DHS agrees with the OIG’s findings that the Department has made progress toward consolidating the existing Components’ infrastructures into OneNet, the Department’s wide area network (WAN) initiative.

CBP continues to assess various infrastructure upgrades and is preparing a project charter that will include the business priorities provided by the different CBP operational environments when service is disrupted. In addition, CBP is developing a network infrastructure operations and maintenance effort to: ensure end-to-end network connectivity and high rates of network availability; reduce single points of failure within the CBP infrastructure; establish a continuous technology refresh lifecycle for key hardware network and software network components; and forecast technology advances and alignments to CBP strategic objectives and the lines of business of the CBP key stakeholders.

To date, CBP has completed several IT initiatives that will ensure availability of the CBP infrastructure, which include: network (WAN/local area network) infrastructure upgrades at prioritized CBP sites; WAN optimization, which allows network traffic on the data circuit to increase the overall available circuit bandwidth and network performance; upgraded cabling; End-2-End monitoring platform for greater proactive monitoring of the CBP network; and mobile communications.

Several IT projects and activities are planned and/or underway that will address availability and connectivity of the network across CBP including its various operational environments. The projects are near term (0 to 2 years), midterm (2 to 5 years), or long term (5 to 10 years). The results of all projects will, at some level, contribute to high rates of network availability. All



projects depend on funding approval and will be prioritized on the basis of budget approvals and constraints.

Sub-Challenge: Privacy

DHS agrees with the OIG that USCIS has demonstrated an organizational commitment to privacy compliance by establishing its Privacy Office, appointing a privacy officer, and making progress in implementing a privacy program that complies with privacy laws, but that the Department can do more to improve the protection of personally identifiable information (PII) and the overall culture of privacy.

The USCIS Office of Privacy has been hosting job-specific, advanced, or specialized privacy training courses. The Office of Privacy has hosted instructor-led privacy awareness training for all USCIS Headquarters employees and contractors on a monthly basis through the end of FY 2011 and is providing similar training at USCIS Regional, District, and Field offices. Further, the Office of Information Technology has incorporated privacy awareness information into the USCIS Computer Security Awareness Training and the USCIS IT Rules of Behavior. Both awareness mechanisms stipulate that all personnel must be able to identify PII and know the proper PII handling guidelines in accordance with the USCIS Office of Privacy's policies and procedures.

The USCIS Office of Privacy conducted Privacy Awareness Week in April 2011 to enhance the culture of privacy at the agency and increase employee awareness of privacy issues. It is also evaluating a series of videos addressing various aspects of privacy and expects to begin launching the videos in late November 2011.

In addition, OSI developed the USCIS Physical Security Inspection Workbook to assess security countermeasures and ensure consistent security standards and equipment are employed across USCIS. OSI completed three inspections at USCIS Headquarters facilities and piloted this workbook at seven locations in the field in FY 2011. In addition, OSI has partnered with Service Center Operations to conduct reviews of the four service centers to address any gaps in security systems and procedures that impact the protection of privacy information. OSI is evaluating the comments and results from these facility inspections and expects to finalize the workbook by the end of December 2012.

The Electronic Security Systems Nationwide Deployment Project has provided USCIS with measurable metrics to help determine whether a facility has adequate and functional security countermeasures (e.g., physical access control system, closed circuit television and intrusion detection systems). Further, in FY 2011, OSI made upgrades and improvements to these systems at both Headquarters and several regional facilities.

By the end of March 2012, the USCIS Privacy Office plans to incorporate a training page on the Office of Privacy's Intranet Web site. The training page will include links to privacy policy and guidance, training materials and presentations, Privacy-BLAST (newsletter), and upcoming training offerings and events.

The USCIS Privacy Office is finalizing a general privacy awareness training course targeted to all USCIS personnel (federal and contractor), which is expected to launch by November 30, 2011. It



also is developing specialized privacy awareness training course targeted to program or system managers and expects to have a beta version by December 2011.

To address issues regarding technical safeguards, the USCIS Office of Information Technology (OIT) has issued Public Key Infrastructure (PKI) certificates to 7,400 USCIS employees. OIT plans to continue to issue PKI certificates to all employees, ensure thumb drives are trackable property, issue a Management Directive on audit and accountability, and enhance the audit and monitoring capability of USCIS case management systems.

Challenge #3: Emergency Management

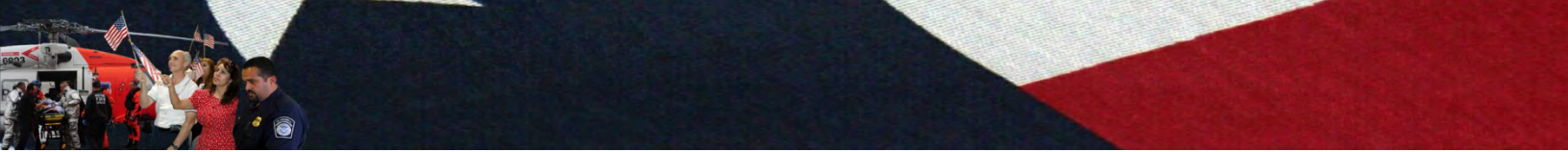
DHS agrees with the OIG that the Federal Emergency Management Agency (FEMA) has made great strides in improving its disaster preparedness and recovery. FEMA continues to work to improve, particularly in the areas identified by OIG as challenges. Specifically, DHS is working to make improvements in the emergency support function; implement and evaluate mass care and emergency standard operating procedures, tools, and initiatives; and provide debris removal expertise and guidance.

Sub-Challenge: Emergency Support Function

OIG stated that although FEMA generally fulfilled its roles and responsibilities under the Emergency Support Functions, the agency can improve its coordination with stakeholders and its operational readiness. FEMA is currently engaged in working-group activities with stakeholders to address this challenge. In October 2010, FEMA's Office of Response and Recovery launched an effort to reinvigorate the Emergency Support Function Leadership Group (ESFLG), the senior-level entity that coordinates responsibilities, resolves operational and preparedness issues, and provides planning guidance and oversight for interagency response and recovery activities. The goal of this effort—and the mission of the ESFLG—is to improve the effectiveness of coordinated federal response and recovery activities by engaging interagency leadership through a forum that fosters the exchange of information, planning, and decision-making.

ESFLG membership includes senior officials who can speak authoritatively on behalf of their respective organizations, including representatives from each of the 15 emergency support functions (ESFs). ESFLG meetings now serve as a vehicle to address issues that directly affect the roles and responsibilities of the ESFs as described in the National Response Framework and its annexes. Also in 2010, the revived ESFLG group managed FEMA's Whole Community planning effort—a worst-case, catastrophic disaster scenario affecting 7 million people and 25,000 square miles. Through its working group structure, the ESFLG identified 13 core capabilities and supporting objectives required for a rapid and effective response. The working groups then developed courses of action to close capability deltas in support of each capability. These capabilities were also tested through the participation of ESF members during National Level Exercise 2011: New Madrid Earthquake.

Building on the ESFLG's Whole Community efforts and in response to Presidential Policy Directive #8 (PPD-8), FEMA is leading the development of a Federal Interagency All-Hazards Response Plan, to include scenario-specific annexes that integrate prior earthquake, hurricane, and catastrophic planning efforts. Employing the Whole Community framework and the ESFLG



throughout PPD-8 efforts, FEMA seeks to integrate non-traditional response strategies required for catastrophic disasters. The final plan will comprehensively address coordinated federal support to regional, state, tribal, and local entities for all-hazard responses.

Sub-Challenge: Mass Care and Emergency Assistance

FEMA is working to address OIG recommendations to implement and evaluate mass care and emergency standard operating procedures, tools, and initiatives by increasing the use of these items at exercises. For example, Mass Care activities were exercised at the National Level Exercise 2011. As part of the scenario, Mass Care services were coordinated and provided to 4 million people and 1.5 million pets in seven affected states. Mass Care task forces were deployed to support the survivors and affected states and individual assistance/technical assistance contractors were activated and mobilized to support survivors. All Mass Care tools, including contractors, agreements with other agencies and organizations, and other Mass Care partners were coordinated and used.

In addition, states are beginning to use some of the Mass Care tools. For example, in 2010, the Multi Agency Feeding Template and Task Force documents were used in Florida, and the National Mass Evacuation Tracking System was used in Maryland; in 2011, the Household Pets Task Force was used in Maine, and the interface of the Web-enabled Emergency Operations Centers was tested in Arkansas as part of the National Level Exercise 11.

FEMA and the American Red Cross are also working together to complete the interface of the two National Shelter System databases. Both agencies are working on an agreement and protocol that will facilitate the exchange. A software modification that will allow for both programs to exchange data has been completed.

Sub-Challenge: Debris Removal Operations

DHS agrees with the OIG that FEMA's public assistance program has, in general, been a successful effort; vast amounts of debris have been removed and disposed of, allowing communities to proceed toward recovery unencumbered. FEMA is working to address its recommendations to improve planning, contracting, and oversight of debris operations to increase the cost-effectiveness of these operations.

While FEMA provides support for debris removal, including through reimbursements, state and local jurisdictions are ultimately responsible for debris removal.

FEMA agrees with the OIG on the benefits of the Public Assistance Pilot Program, specifically with regard to the initiative to provide an increased federal cost share for applicants with debris management plans. The authority provided by Congress to implement the pilot ended on December 31, 2008. After the pilot, FEMA assessed the pilot program and submitted a report to Congress. On the basis of those findings, FEMA is developing regulatory action to permanently implement the initiatives of the pilot.



Challenge #4: Grants Management

FEMA awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. FEMA is continuously working to enhance its grant management to include risk management principles and performance measures in order to determine how the preparedness grants have improved preparedness capabilities across the Nation.

Sub-Challenge: Disaster Grants Management

FEMA's progress includes implementing a long-term approach to enhance financial monitoring within the regions. This approach implements risk management principles to direct scarce monitoring resources to grantees and programs with the most need. As part of a multi-year process, FEMA has refined criteria for deciding which grants to monitor, standardized Regional Financial monitoring activities, and expanded ongoing oversight activities to ensure early identification of issues. This approach builds on the established monitoring approach and will drive FEMA toward continuously advancing its grants management capability.

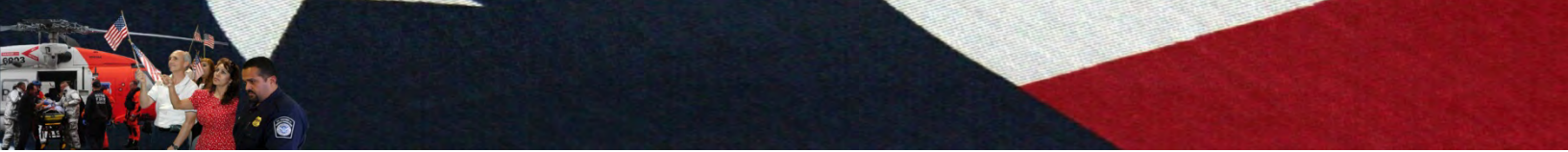
Sub-Challenge: Preparedness Grants Management

FEMA has undertaken two initiatives to establish performance measures for the Preparedness Grant Programs. The Grant Programs Directorate is developing both internal and external management and administrative performance measures to track how well the grants are managed. In addition, the National Preparedness Division is building upon the performance metrics established in the Homeland Security Grant Program (HSGP) and Emergency Management Performance Grant and is creating metrics for the remaining preparedness grant programs. When finalized and combined, these two efforts to develop performance measures will allow FEMA to better manage and analyze the preparedness grant programs. Ultimately, these measures will help to determine how the preparedness grants have improved preparedness capabilities across the Nation.

FEMA continues to work with Congress, DHS Headquarters, and state grant administrators to consolidate grant programs in which activities are allowable under multiple grants. In the FY 2010 HSGP's Program Guidance, a fifth program, Operation Stone Garden, was added into the cluster of programs comprising HSGP. This was done to help streamline the application and award process. In FY 2011, the Buffer Zone Protection Program and the Interoperable Emergency Communication Program were no longer funded. Activities previously allowable under those programs are now eligible under the HSGP and Urban Area Security Initiative Program. Moving forward, FEMA will continue to address redundancies and identify opportunities to streamline grant programs where possible.

Challenge #5: Financial Management

DHS is dedicated to demonstrating good stewardship of taxpayer dollars. In January 2011, Secretary Napolitano committed to the goal of receiving a qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity in FY 2011. This level of confidence and support from our Secretary spoke volumes to all levels of financial management



throughout the Department and strongly reinforced all of our efforts to improve financial management at DHS.

From FY 2006–2011, DHS has reduced the number of audit qualifications from 10 to 1, Department-wide material weaknesses in internal controls over financial reporting from 10 to 5, and the number of Component conditions contributing to material weaknesses from 25 to 7. Although five material weaknesses remain, in most cases, the Department lessened the severity of the conditions, and corrected its material weakness condition in Actuarial Liabilities.

In FY 2011, the Department obtained a qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity. This means that for the first time since FY 2003, we can report to the public that most of the line items on the Department balance sheet are materially correct. We still face challenges, but we made significant progress in strengthening internal controls and implementing corrective actions within several key financial management areas. In FY 2011, the Department:

- Developed a more-robust risk management process, meeting with Components frequently to mitigate high-risk areas and to prevent new material weaknesses. We also developed a new technical accounting issues resolution process, wherein Components can communicate issues and work with the Department to determine the best path forward.
- Addressed financial management and business process challenges and shared best practices and lessons learned by identifying subject matter experts in critical risk areas and leveraging their expertise through cross-Component working groups. In addition, DHS updated its “Component Requirements Guide,” which contains approximately 40 standard financial reporting processes and provides guidance for implementing controls and reporting financial data.
- Analyzed the skill sets of essential financial management personnel and developed a plan to improve core competencies in key financial management areas. Implemented a new training program that in FY 2012 will offer courses to the financial management community in subjects ranging from appropriations law and federal accounting fundamentals to budget formulation/execution and the U.S. Standard General Ledger.
- Worked closely with Components to plan responses to IT notices of findings and recommendations, with a focus on FEMA and U.S. Coast Guard scripting issues. Because of a strong FY 2011 IT remediation process, we have reduced the severity of some areas of material weakness.
- Continued to refine and update the Financial Management Policy Manual to provide all DHS employees with standard processes to follow for budgetary policy, financial reporting, financial assistance, and travel and bank card management.

The gains made in financial management at DHS over the past few years are due to the hard work of dedicated employees at the DHS Office of the Chief Financial Officer and Components across the Department. We have put in place policies, processes, and structures to help ensure consistent operations for each of our financial accounting centers and financial management offices within DHS Components. Improvements made by the Components include corrective actions that increased the Department’s auditable balance sheet balances to approximately 90 percent in FY 2011.



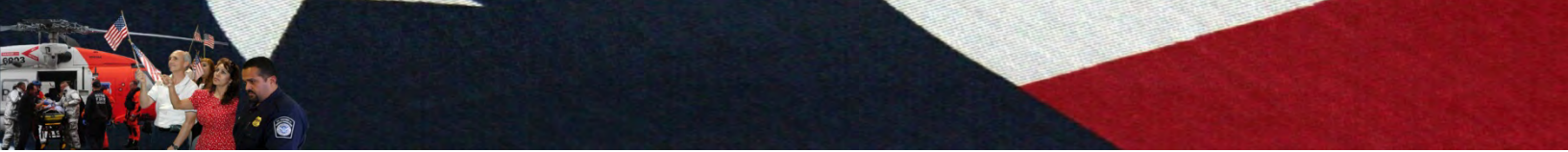
- Showing great commitment from senior leadership, the Commandant of the U.S. Coast Guard issued a memo to the U.S. Coast Guard community stressing the importance of implementing corrective actions in order to achieve success with the audit in FY 2011. By executing corrective action plans, implementing new processes, and monitoring risk throughout the fiscal year, the U.S. Coast Guard has been able to reach major milestones, making it possible for the Department to attain a balance sheet opinion in FY 2011.
- In FY 2007, the U.S. Coast Guard had disclaimer conditions on all balances. Since then, the U.S. Coast Guard has reduced its disclaimer conditions each year. This year, the U.S. Coast Guard asserted to all balance sheet items but Property, Plant, and Equipment and the associated impact on environmental liabilities and cumulative results of operations, representing a total of \$57.5 billion, or more than 80 percent of its balance sheet.
- Most significantly, the U.S. Coast Guard corrected a longstanding entity level control deficiency. This success is due to the Commandant's leadership in setting strong tone at the top and to delegating responsibility for internal control from senior management to all financial management staff levels and across business lines.
- In FY 2011, the Department's Financial Reporting material weakness was narrowed in scope because the U.S. Coast Guard implemented processes and procedures to support its financial statement balances. The U.S. Coast Guard also reduced the scope of its Financial Systems material weakness through corrective actions to improve computer scripts that impacted the accuracy of financial statements and consolidated the scope of its Environmental and Other Liabilities material weakness through elimination of another liability condition related to more than \$40 billion in medical retirement benefits.
- FLETC corrected its control deficiency in IT Controls and System Functionality; FEMA corrected its control deficiency in Financial Reporting; and CBP corrected control deficiencies in Budgetary Accounting and Entity-Level Controls. ICE reduced the severity of its control deficiency in IT Controls and System Functionality.

These successes have positioned DHS to be able to expand the audit to all of the financial statements in FY 2012. By taking a deeper dive into the financial statements, we will identify additional areas for corrective action, taking us further down the road toward a clean opinion on all financial statements.

While we have made progress, we recognize that significant internal control challenges remain. The Department's Deputy Chief Financial Officer will remain actively engaged with senior management and staff at each Component, overseeing corrective actions to ensure continued progress across the Department. The Department has several initiatives under way and planned to remediate internal control challenges.

Sub-Challenge: Managerial Cost Accounting

The Department is determining best way to use and deploy managerial cost accounting (MCA) across the enterprise. We have chartered a cross-Component working group to assist Components in costing methodologies and developing a methodology to approximate full cost, as required by SFFAS No. 4, Managerial Cost Accounting. This group is studying the extent to which DHS is currently using MCA, with the goal of identifying best practices and defining Component requirements for implementation and reporting.



DHS is working to develop a consistent approach across Components for determining the full costs of program and missions at the individual program/mission activity level. Our goal is to be able to accumulate and consolidate these costs to align directly with the major goals and outputs described in the DHS strategic and performance plans (QHSR goals), and eventually enable Statement of Net Cost to be presented by major program/strategic goal in compliance with OMB Circular A-136.

In addition, DHS will continue to develop its strategy for deploying MCA Department-wide. This strategy will take some time to execute because full implementation of SFFAS No. 4 is highly dependent on financial systems. The Department is modernizing its core financial systems, implementing a common accounting structure, and developing data standards and business intelligence tools to collect and crosswalk cost data at program/project/activity level across Department Components.

DHS will ensure Mission Action Plans at key Components include long-term corrective actions and milestones related to the compliance with SFFAS No. 4 and the ability to report full costs at individual program/mission activity level that align directly with the Department's major programs/strategic goals.

Sub-Challenge: Antideficiency Act

In FY 2011, the Department continued to implement its plan to improve compliance with the *Antideficiency Act* (ADA). This multi-year plan includes policy reviews, Department-wide training, and internal control test work to prevent ADA violations.

- In FY 2010, we completed a crosswalk of Component administrative control of funds policies to the Department-wide policy and initiated revisions to strengthen Department-wide funds controls.
- In FY 2011, we made significant progress ensuring appropriate controls are in place to prevent violations. As part of A-123 testing, the Department assessed Component-level internal controls over the Budget Resource Monitoring process to ensure controls are in place to prevent future ADA violations.
- In FY 2011, we offered several introductory and refresher courses in appropriations law, and we developed an online course scheduled for launch through Department and Component learning systems in the first quarter of FY 2012.

Sub-Challenge: Financial Statements Audit

We recognize that maturing our Department is a collective effort, and we continue to implement initiatives to strengthen and mature the Department across many areas. The Department is preparing to move beyond the Balance Sheet to the other financial statements and to prepare for the Internal Controls Over Financial Reporting audit. We are working with Components to develop risk registers for the statements of budgetary resources, net cost, and custodial activity. We will continue to meet regularly with Components through the Financial Management Working Group, issue-specific working groups, and regular risk-management and audit status meetings to assess their progress executing corrective action plans.

In support of our goal of continued progress toward a clean audit opinion, the Department will:



- Continue targeted risk assessments to identify and remediate weaknesses in accounting and financial reporting.
- Partner with Components to design and implement corrective actions to prepare all financial statements for audit, to remediate weaknesses, and to ensure continued progress in FY 2012 and beyond.
- Expand pilot efforts to have the independent auditor use management’s internal control over financial reporting work, which will build additional audit efficiencies.

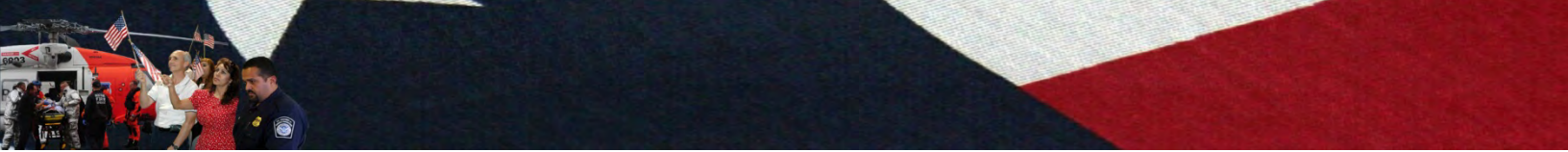
Modernize core financial management systems; establish standard, key business processes and internal controls; and implement a standard line of accounting across financial systems to ensure DHS sustains its audit progress. Progress that relies on manual processes may not be sustainable without such system improvements and standard processes.

Challenge #6: Infrastructure Protection

DHS works closely with federal partners and the private sector to deter threats, mitigate vulnerabilities, and minimize incident consequences for all Critical Infrastructure and Key Resources (CIKR). The OIG states that the need to coordinate with and rely on federal partners and the private sector presents a challenge for the Department but also an opportunity for DHS to engage people across the country in the protection and resilience of the nation’s infrastructure. DHS continues to support the voluntary framework developed in response to Homeland Security Presidential Directive 7, and the support of voluntary stakeholders has helped the Department with its achievements thus far. Although challenges remain, DHS continues to make significant progress to protect the nation’s CIKR. For example, NPPD/IP launched a strategic effort called the Critical Infrastructure Risk Management Enhancement Initiative, which will strengthen critical infrastructure protection and resilience across all sectors and regions. Its goal is to ensure that National Infrastructure Protection Plan critical infrastructure protection and resilience activities achieve outcomes that are developed on the basis of the most pressing risks and our effectiveness in managing those risks.

Sub-Challenge: Risk Assessment Efforts in the Dam Sector

DHS has identified, consistent with the National Infrastructure Protection Plan, the Nation’s most critical systems within the Dams Sector and has developed a risk assessment tool that combines all three functions of risk: threat, vulnerability, and consequence. While DHS does not have regulatory authority over the Dams Sector, it does provide public and private sector partners with education and training opportunities that offer guidance on protective measures and crisis management in addition to conducting vulnerability assessments that identify potential security improvements. Specifically, NPPD/IP collaborates with federal, state, local, and private sector partners on many initiatives and provides a wealth of information such as a cybersecurity roadmap to secure control systems; guidelines and training on security awareness, protective measures, and crisis management; an exercise program to enhance regional disaster resilience (Dams Sector Exercise Series); and vulnerability assessment products that identify potential areas for improvement and suggest protective measures that could be implemented on a voluntary basis. In addition, NPPD is working with stakeholders from industry and government to determine whether a legislative proposal should be made to address any critical gaps, addressing an OIG recommendation.



Challenge #7: Border Security

In March 2009, the Obama Administration launched the Southwest Border Initiative to bring focus and intensity to Southwest Border security, coupled with a reinvigorated, smart, and effective approach to enforcing immigration laws in the interior of our country. DHS is now more than two years into this strategy, and based on previous benchmarks set by Congress, it is clear that this approach is working.

Under the initiative, CBP has increased the number of Border Patrol agents deployed to the Southwest Border to more than 18,000, which is more than twice the number stationed in the region in 2004. In addition, DHS has doubled personnel assigned to Border Enforcement Security Task Forces, which work to dismantle criminal organizations along the border. The number of ICE intelligence analysts along the border focused on cartel violence has also increased. In all, a quarter of ICE's personnel are now in the region, the most ever. In addition, the number of border liaison officers assigned to work with their Mexican counterparts has tripled, and CBP is now screening all southbound rail traffic and a random number of other vehicles for illegal weapons and cash that are helping fuel the cartel violence in Mexico.

Sub-Challenge: Western Hemisphere Travel Initiative

In 2009, DHS implemented the Western Hemisphere Travel Initiative (WHTI), a program that strengthens border security for land and sea travel to the United States, while facilitating legitimate travel and trade by requiring that U.S., Mexican, and Canadian citizens present a passport or other secure travel document¹ that denotes identity and citizenship when crossing the border. Prior to the implementation of WHTI, there was no documentary requirement for U.S. or Canadian citizens to enter the United States from within the Western Hemisphere; travelers could present any of numerous documents or simply make an oral declaration without presenting any documentation. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases. Today, due to WHTI, the national query rate is over 97 percent.

To support WHTI, DHS has worked with U.S. governors and Canadian government officials to develop state and provincial Enhanced Driver's Licenses (EDLs) that denote identity and citizenship for frequent border crossers, and with the Department of State to develop a wallet-sized U.S. Passport Card. Both documents, as well as others developed for WHTI, can be electronically verified with the issuing agency at the port of entry. CBP and Canada Border Services Agency also worked to expand enrollment in the NEXUS trusted traveler program. The United States has deployed Radio Frequency Identification technology readers at ports that cover 99 percent of inbound vehicle traffic at the Northern Border and allow the documents to be read as the traveler is approaching the inspection booth.

CBP is also working with tribes across the country on the development of Enhanced Tribal Cards (ETCs). To date, CBP has signed Memoranda of Agreement for the development of ETCs with the Kootenai Tribe of Idaho, the Pascua Yaqui of Arizona, the Tohono O'odham of Arizona, the Seneca Nation of New York, the Coquille of Idaho, and the Hydaburg of Alaska.

¹ WHTI-compliant documents include passports, U.S. passport cards, military identification cards, trusted traveler cards, Enhanced Driver's Licenses, and Enhanced Tribal Cards.



Sub-Challenge: Information Sharing on Foreign Nationals: Overseas Screening

To enable officers and analysts to use a single sign-on for DHS systems used for screening foreign nationals, the DHS CIO developed the Identity, Credential, and Access Management Segment Architecture (version 1.0, March 31, 2010) and Information Sharing Segment Architecture (version 2.1, May 15, 2009), which identifies the requirement for single sign-on across multiple internal and external systems, including screening systems.

Additional resources are being developed to establish a portal on the secure Homeland Security Information Network (HSIN) through which authorized DHS users can log on to DHS Web-based databases to access information on foreign nationals. The DHS OCIO Information Sharing and Exchange Division is working with the Office of Operations (OPS) and I&A to build this functionality into the HSIN 3.0 rollout, scheduled for initial operating capability in the third quarter of FY 2012. Until then, OCIO is also working with OPS HSIN and I&A to put in place an interim capability.

In response to staffing issues identified by OIG, CBP National Targeting Center-Passenger (NTC-P) has identified the need for 55–75 new permanent CBP officer FTP and new, permanent managerial, support, and administrative FTP to support the additional staff. The 55–75 new positions are needed to adequately staff new or enhanced targeting programs, including pre-departure screening, Advanced Targeting Team initiatives, outbound targeting, Visa re-vetting, and expanded Immigration Advisory Program operations. The officers would be spread across three shifts, to cover a 24-hour period. The allocation of officers to specific shifts and targeting programs is continually evaluated. The President's FY 2012 budget request includes funding for multiple enhancements to the NTC-P, including for the hiring of additional staff. As of September 30, 2011, 179 officers are on full-time or temporary duty. A full complement of staff should be achieved by FY 2013.

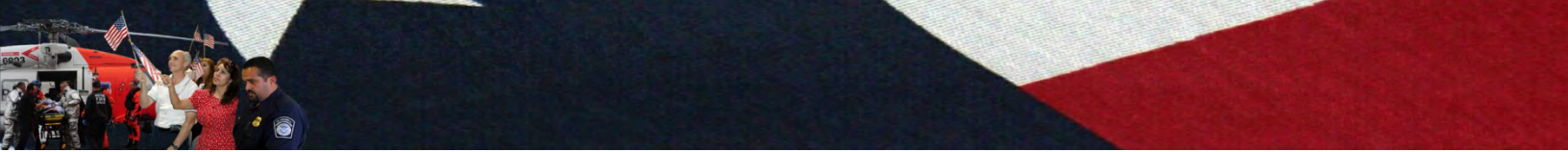
The NTC-P has implemented a variety of changes to promote staff retention, including: improvements to the hiring process and postings of vacancy announcements; implementation of employee recognition and communications initiatives; establishment of permanent shifts with rotating long weekends; establishment of a permanent training team; periodic rotations through multiple programs; and participation in the Student Career Experience Program, which provides student interns with a paid work experience that may make them eligible for permanent employment upon graduation from their academic institution.

Challenge #8: Transportation Security

According to the OIG, TSA is making progress in meeting the challenges of transportation security. However, it remains a challenge for TSA to establish effective security strategies while facilitating the legitimate flow of passengers and cargo.

Sub-Challenge: Passenger and Baggage Screening

TSA appreciates the OIG's work to identify opportunities to further enhance TSA's checkpoint program. TSA continuously enhances its screening technologies and procedures to address evolving threats to our Nation's transportation systems. The best defense against threats to our



transportation systems remains a risk-based, layered security approach that uses a range of measures, both seen and unseen. After analyzing the latest intelligence and studying available technologies and other processes, TSA determined that Advanced Imaging Technology (AIT) is the most effective method to detect metallic and non-metallic threat items concealed on passengers. In addition, TSA is in the process of upgrading its AIT units with Automatic Target Recognition. This will enhance AIT units' detection capability by increasing the throughput and corresponding percentage of passengers screened by this technology while also further enhancing the privacy protections in place for AIT screening.

TSA has initiated the deployment of the Advanced Technology (AT)-2 units, which will be used to screen passengers' carry-on items. The AT-2 systems are equipped with algorithms that are intended to assist the operator with automatic detection of prohibited items and threats. This platform also provides TSA a baseline of performance, upon which future enhancements can be accomplished. Finally, TSA is procuring Credential Authentication Technology (CAT)/Boarding Pass Scanning Systems (BPSS), which Transportation Security Officers (TSOs) will use to validate and verify passengers' identification and boarding passes, increasing security at the checkpoints. CAT/BPSS will automatically verify both passenger identification documents and boarding passes, which will help facilitate identity-based screening while making the process more effective and efficient.

CAT/BPSS will eventually replace the current manual "lights and loupes" used by security officers to verify document authenticity. TSA anticipates the new technology will enhance security and increase efficiency by automatically verifying passenger identification and boarding passes. It will be incorporated into TSA's passenger prescreening pilot that is slated to begin at four airports this fall. This aligns with TSA's latest efforts to enhance the passenger screening experience by moving toward a more risk-based, intelligence-driven counter-terrorism agency.

TSA began testing travel document authentication technology at its Transportation Security Integration Facility in July 2011. Earlier versions of this technology were tested at Ronald Reagan Washington National (DCA) and Baltimore/Washington International Thurgood Marshall (BWI) airports in 2009.

As with all technologies, TSA will continue to push industry to higher performance requirements in an effort to increase detection and accuracy while also improving screening operations efficiency. TSA is already conducting work in a number of areas included in the OIG's recommendations. In addition, TSA is formulating plans to implement the other recommendations in the report.

Sub-Challenge: Airport Badging Oversight

TSA is responsible for implementing a process to ensure employees working in secured airport areas are properly vetted and badged, and must oversee the designated airport-operator employees who perform the badging application process. TSA ensures that airport operators have quality assurance procedures for the badging application process by implementing the requirements in Sections III–V of Security Directive 1542-04-08G, *Security Threat Assessment and Reporting Requirements Related to Individuals with Airport-Issued Identification Media*, dated May 28, 2009. TSA also ensures that airport operators provide training and tools to designated badge office employees by implementing the requirements in Attachment B, Section II of Security Directive 1542-04-08G. Transportation Security Inspectors are required to verify the airport data



during their inspections as required in the Domestic Airport Inspection, Prompt Section 14: Security Directive 1542-04-08 Series. This is, at a minimum, a yearly inspection requirement.

Sub-Challenge: Passenger Air Cargo Security

Prior to 9/11, no federal security requirements existed for cargo screening. Now, 100 percent of all cargo transported on passenger aircraft that depart U.S. airports is screened commensurate with screening of passenger checked baggage. This was accomplished largely through the Certified Cargo Screening Program, which permits entities that have undergone rigorous inspection and certification processes throughout the air cargo supply chain to screen cargo.

In December 2010, TSA implemented requirements for 100 percent screening of high-risk cargo on international flights bound for the United States. Following this, Secretary Napolitano and TSA Administrator Pistole solicited feedback from passenger carriers on their ability to screen 100 percent of all air cargo on international inbound passenger aircraft. The Department evaluated formal industry comment to this proposal and continues to finalize its strategy and timeline for implementing the 100 percent international inbound cargo screening requirement. As part of this effort, TSA will work with industry to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process, which certifies foreign aviation security programs that are commensurate with TSA standards.

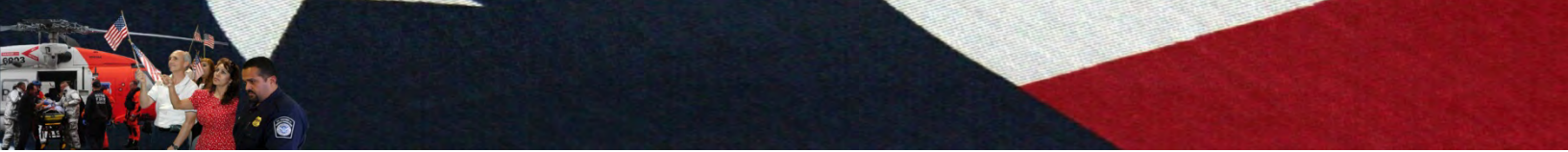
In addition, In January 2011, Secretary Napolitano announced a new partnership with the World Customs Organization (WCO) to enlist other nations, international bodies, and the private sector in increasing the security of the global supply chain—outlining a series of new initiatives to make the system stronger, smarter, and more resilient.

As part of the effort to strengthen the global supply chain, ICE, in coordination with the WCO, launched Operation Global Shield in 2010, a multilateral law enforcement effort aimed at combating the illicit cross-border diversion and trafficking of precursor chemicals for making improvised explosive devices (IED) by monitoring their cross-border movements. In March 2011, the WCO voted to make Project Global Shield a permanent program.

In addition, the Customs Trade Partnership Against Terrorism (C-TPAT), a voluntary public-private sector partnership program, strengthens cargo security throughout the international supply chain by working closely with importers, carriers, consolidators, licensed customs brokers, and manufacturers. The C-TPAT program—launched in November 2001 with seven participating companies—evaluates trusted shippers through security checks and on-site evaluations. As of October 2011, C-TPAT has 10,189 certified partners worldwide and has conducted 18,872 on-site validations of manufacturing and logistics facilities in 97 countries, representing some of the highest risk areas of the world.

Sub-Challenge: Training

TSA's Operational and Technical (OTT) Training Division, within the Office of Security Operations, provided information on several activities already under way that address the challenge the OIG highlighted regarding training of TSA's screening workforce. OTT has established an integration process team (IPT) to review and analyze current documented and undocumented OTT business practices and processes. OTT currently uses events or inputs, such as Aviation Security



Assessment Program test results, internal [TSA] and external [OIG and GAO] covert test results, new threat and/or intelligence/threat information, and changes to procedures as catalysts to update existing or design new training materials. The deliverable from this IPT is a document that includes regulated and repeatable milestone-driven processes and procedures to ensure currency, effectiveness, and efficiency of training curriculum.

TSA's efforts to formalize the On-the-Job Training Instructor (OJTI) program are enhancing the level of training of the screening workforce. DHS OIG was provided an update stating that OTT conducted an OJTI Operational Tryout (OTO) at Seattle airport (SEA) to pilot a structured training curriculum for the TSOs who will serve as OJTIs. This included mandatory courses on mentoring and providing effective feedback. On the basis of initial feedback during the OTO in SEA, changes were made to the curriculum, a second OTO was conducted, and the new model was highly successful. Expansion of the program is beginning in the first quarter of FY 2012.

The DHS OIG also recommended that TSA determine if modifications to its allocation of training computers in the field are adequate. TSA completed an initial review of the current allocation of training computers and must continue that review because it is clear that simply establishing a TSO-to-training computer ratio for all airports would not be an appropriate solution. Office/training space, training room locations, and maximum number of officers that can be removed from the operations for training at any given time all must be factored in to ensure each airport has an appropriate training computer allocation.

OTT will continue its work to finalize the documentation that will capture OTT business practices and processes to ensure the currency, effectiveness, and efficiency of the training curriculum. National rollout of the formalized training program for OJT instructors will be conducted throughout FY 2012.

The review of training-computer allocations will continue throughout FY 2012, and adjustments may be made to individual airport inventories if they have a demonstrated need and can accommodate the additional equipment.

TSA believes that progress has been and continues to be made as TSA continues to build its training portfolio, with the desired outcome of improving performance and developing its workforce.

In FY 2012, OTT anticipates having documents that describe the processes used to identify needs for updating training materials and/or to develop new materials on the basis of information from various sources. TSA will continue to define changes needed to support a training program that is both comprehensive and adapts to address evolving threats.

Sub-Challenge: Rail and Mass Transit

The final report for OIG-11-93, "DHS Grants Used for Mitigating Risks to Amtrak Rail Stations," was issued in June 2011. The 90-day response was submitted in September 2011. The language cited in the Management Challenges report does not reflect the recommendations from OIG-11-93. TSA is addressing the recommendations from the OIG-11-93 report, as follows and as previously submitted to the OIG.



OIG-11-93 Recommendation 1—Require the Transportation Sector Network Management, Mass Transit and Passenger Rail Division, to work closely with Amtrak to establish a corrective action plan that ensures decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by previous risk assessments. The plan should include:

- *Preliminary strategies and designs specifying the identification and commitment of all interested parties, to be presented during the grant application process to facilitate prompt mitigation efforts,*
- *Details on the amount of funding needed to address the most critical vulnerabilities, and*
- *Milestones for the timely approval of mitigation projects.*

TSA, in coordination with FEMA, is actively coordinating with Amtrak to address all items. TSA has completed a Baseline Assessment for Security Enhancement (BASE) review for the Northeast Corridor, and the preliminary results are being compiled and analyzed. Amtrak and DHS met on September 12, 2011, to discuss several items, including how the FY 2011 Amtrak grant funds can be used to address items from the BASE results and how corrective action plans will be developed for security projects that are currently either partially funded or not funded.

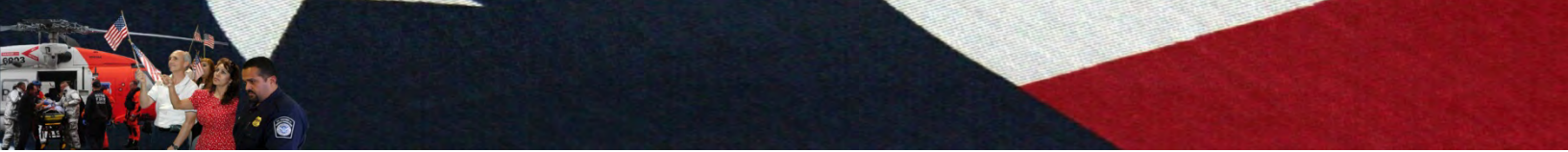
Actions planned to address Recommendation 1 within the next year:

- Members of the Mass Transit and Passenger Rail Security Division (MTPRS) will work with TSA/Office of Security Operations, Compliance, through the Northeast Regional Security Inspectors, to complete the second regional BASE assessment for Amtrak.
- Although a formal security plan cannot be finalized before the security plan regulation is issued, TSA will continue to work with Amtrak in the interim to develop action plans and security projects that address vulnerabilities identified through other completed assessments and plans.

Actions planned to address Recommendation 1 within the next 2–3 years:

- Members of MTPRS will work with TSA/Office of Security Operations, Compliance, through the Northeast Regional Security Inspectors, to complete the third and final regional BASE assessment per year, completing the 3-year system-wide assessment.
- The system-wide BASE assessment will be used with the foundation Amtrak already built through its prioritization “quilt.” The quilt summarizes in spreadsheet format the results of Amtrak’s system-wide risk assessments; provides a snapshot of critical assets identified in the risk assessments; and includes the status of on-going mitigation projects, including relevant funding sources. The quilt is a living document and is updated as necessary with current information. This quilt will set the baseline to inform a comprehensive security plan that will include strategies, designs, and cost-mitigation efforts.
- TSA will develop and include, as part of its internal procedures (per Recommendation 2), performance metrics to ensure the timely approval of Amtrak security projects.

OIG-11-93 Recommendation 2—Ensure the Transportation Sector Network Management, Mass Transit and Passenger Rail Division, creates and reports internal procedures that describe how the agency will carry out its roles and responsibilities in the grant award process for ensuring that Amtrak and other grant recipients address the highest-priority security vulnerabilities.



FEMA and TSA have set forth how each agency will carry out its roles and responsibilities in the grants award process in a memorandum of agreement that was signed by both agency Administrators in March 2011. An updated memorandum of understanding was also signed June 30, 2011, between TSA, FEMA, and the U.S. Department of Transportation/Federal Railroad Administration regarding how Amtrak funding would be administered and identifying, at a high level, each agency's role in the award process.

Actions planned to address Recommendation 2 within the next year:

- TSA will develop its own internal processes document, which it will share with FEMA, to document how TSA will internally carry out its roles and responsibilities.
- The internal processes will be validated during the FY 2012 grants cycle.

Actions planned to address Recommendation 2 within the next 2–3 years:

- TSA will review the documented processes as performed during the FY 2012 grants cycle and make updates and improvements based on lessons learned.
- Any updates to the internal processes will be shared with FEMA.

TSA is actively working on issuing a security plan regulation, which would cover Amtrak, as required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. 110-53). Once complete, this regulation will serve as the basis for DHS's coordination with Amtrak in developing DHS's system-wide security plan. A formal security plan cannot be finalized with Amtrak until such time. As stated in Recommendation 1, future-year appropriations to implement the "fund[ing of] Amtrak rail station remediation projects" is uncertain.

Challenge #9: Trade Operations and Security

CBP has made progress on the challenges identified by the OIG regarding completion of assessments of risk and the need for standard procedures and guidance for Importer Self Assessment (ISA) program participants.

Sub-Challenge: CBP Revenue

CBP provided a risk matrix and risk analysis for the ISA program. The risk matrix provided guidance for the assessment of risk based on the likelihood of occurrence and impact of the risk, if it occurred. The risk analysis identified 10 risk factors, the probability of occurrence and severity of the risk, and mitigating controls. This risk analysis demonstrates that CBP analyzed the individual risks to trade compliance associated with policies for accepting importers into the ISA program and identified appropriate mitigating activities for each risk. Further, CBP identified the source of the mitigating activities, such as the ISA Handbook, ISA SOP, etc. OIG has indicated that CBP's corrective action satisfied the intent of the recommendation, which was closed on July 18, 2011.

CBP provided support that it has removed ISA program oversight responsibilities from port account managers and assigned those importer accounts to national account managers. OIG has indicated that CBP's corrective action satisfied this recommendation, which was closed on November 18, 2010.



ISA SOP #2011-001 requires that national account managers review the information in the importer's annual notification letters including the findings from the periodic testing. In addition, ISA SOP #2011-001 requires the national account managers to complete an ISA account risk summary, which includes the evaluation of risk associated with importer self-testing results and actions taken. OIG has indicated that CBP's corrective action satisfied the intent of the recommendation, which was closed on July 18, 2011.

CBP decided that in lieu of updating the National Account Manager Guidebook, it will implement Account Management's SOP for ISA Accounts. The purpose of the SOP is to provide guidance and instruction to national account managers on assessing and reviewing ISA applicants and to promote uniform oversight of ISA program participants. The SOP addresses the challenges of the ISA program from an account management perspective and will be the authoritative document that national account managers follow for ISA account management purposes. The SOP has been reviewed by CBP stakeholders and is awaiting final approval. Once CBP obtains final approval, the SOP will be disseminated for implementation.

In addition to Account Management's SOP for ISA Accounts, additional formal procedural guidance is provided in ISA SOP #2011-001 issued by the Partnership Programs Branch to ensure consistent and effective implementation of the program.

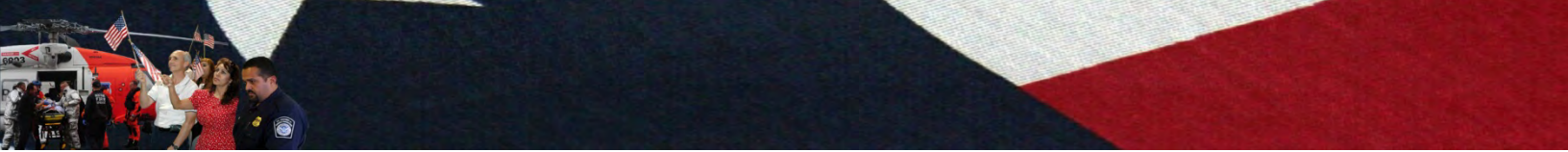
To address the OIG recommendation, CBP has incorporated the requirement for bond automation into the Automated Commercial Environment Cargo Release Concept of Operations (ConOps). The ConOps is currently under senior leadership review. CBP is confirming the high-level requirements. The deployment date of Single Transaction Bonds will not be available until CBP completes the acquisitions and procures a development contract. The acquisition date is estimated to occur in the second quarter of FY 2012. The estimated completion date is March 31, 2012.

Sub-Challenge: Cargo Security

CBP updated the Anti-Terrorism Contraband Enforcement Team National Directive to address terrorism threats and outline minimum procedures for CBP officers to follow when performing anti-terrorism examinations, including specific procedures for inspecting for chemical, biological, nuclear, and radioactive threats. The directive is awaiting final approval.

As mentioned earlier, the C-TPAT, a voluntary public-private sector partnership program, strengthens cargo security throughout the international supply chain by working closely with importers, carriers, consolidators, licensed customs brokers, and manufacturers. The C-TPAT program—launched in November 2001 with seven participating companies—evaluates trusted shippers through security checks and on-site evaluations. As of October 2011, C-TPAT has 10,189 certified partners worldwide and has conducted 18,872 on-site validations of manufacturing and logistics facilities in 97 countries, representing some of the highest risk areas of the world.

To address an OIG recommendation, C-TPAT has updated the Web-based partner security profile to include additional security questions and has conducted refresher training for supply chain security specialists (SCSSs) regarding review of the security profile and vetting procedures; the latter was done in conjunction with the CBP Vetting Center. The program conducts quarterly random management reviews of newly certified security profiles for highway carriers to ensure the accuracy and consistency of the decisions made by the SCSS.



CBP is participating in DHS initiatives focused on biological and chemical threats to the United States and is working to update and develop new rule indicators in the inbound cargo CBP Automated Targeting System (ATS-N) to target high-risk shipments. To supplement its expertise and experience in these areas, CBP will draw on the knowledge of DHS bio-terror subject-matter experts as well as the knowledge of members of the intelligence community. Through participation in these initiatives and through the use of their recommendations, CBP will be well-positioned to identify pathways that pose the highest risk of biological and chemical weapons entering the country. This will support the acquisition and deployment of biological and chemical detection equipment and will ensure that the appropriate guidance and training is provided to CBP personnel. This thoroughly coordinated initiative and its accomplishments are described below.

In 2010, CBP personnel from the Office of Field Operations (OFO), Agriculture Programs and Trade Liaison (APTL) and the Office of Intelligence and Investigative Liaison (OIIL) held a series of meetings with subject-matter experts from the Biodefense Knowledge Center (BKC), Lawrence Livermore National Laboratory (LLNL), to discuss the determination of risk, conduct studies, and create intelligence requirements for the identification and interdiction of possible biological and chemical terrorist material by the biodefense community.

OFO and OIIL briefed BKC personnel on the Automated Targeting System in relation to targeting high-risk cargo shipments, including the use of rules and weight sets for identifying high-risk cargo. OIIL also provided a review of current ATS rules used to identify cargo with the highest risk for possible biological or chemical terrorist material.

After receiving analysis from subject-matter experts, BKC reviewed current ATS rules for the cargo shipment threat area and provided OIIL with recommendations for the enhancement of the lists utilized for targeting. BKC also developed lists pertaining to known scientists and facilities for possible application in ATS targeting rules.

Three rules summits were held throughout 2010. These summits led to the creation of preliminary rule concepts for targeting high-risk biological and chemical threats in the inbound cargo stream and the development of a number of rule modifications, including the creation of several new rules bundles, blocking of common pathogen description acronyms to eliminate false matches of manifest descriptions, marks and numbers, and updating of facility lists.

APTL is currently in a testing period for the ABTC2 Weight Set to target inbound cargo. After testing is completed, OIIL and TASPO will complete an analysis of rule firings during the test period for APTL review and approval. OIIL will support APTL development of an SOP and field training plan for national deployment of the ABTC2 Weight Set.

Additional planned efforts include OFO designing a pilot rollout of the Weight Set and creating the policy for targeting shipments for biological and chemical threats and evaluate the Weight Set prior to national deployment. OIIL will continue to support OFO via ATS rules and Weight Set work for the nationwide implementation of the Ag/Bio Weight Set. The estimated completion date is December 31, 2011.



Concluding Comment

The Department concurs with the OIG's assessment that

...the Department has made progress in coalescing into an effective organization, as well as addressing its key mission areas to secure our nation's borders, increase our readiness and resiliency in the face of a terrorist threat or a natural disaster, and implement increased levels of security in our transportation systems and trade operations.

We appreciate the perspectives offered by the OIG in its management challenges report and will use them to assist the Department in developing our future plans for addressing these important areas.



Acronym List



Acronyms

ADA – Anti-Deficiency Act	CRCL – Civil Rights and Civil Liberties
ADMP – Active Duty Military Payroll	CSRS – Civil Service Retirement System
AFG – Assistance to Firefighters Grants	C-TPAT - Customs Trade Partnership Against Terrorism
AFR – Annual Financial Report	CWG – Commodity Working Group
AIT – Advanced Imaging Technology	CY – Current Year
APMD – Acquisition Program Management Division	DADLP – Disaster Assistance Direct Loan Program
APTL – Agriculture Programs and Trade Liaison	DC – District of Columbia
ARRA – American Recovery and Reinvestment Act	DHS – U.S. Department of Homeland Security
AT – Advanced Technology	DHS FAA – Department of Homeland Security Financial Accountability Act
ATA – American Trucking Association	DIEMS – Date of Initial Entry into Military Service
BKC – Biodefense Knowledge Center	DNDO – Domestic Nuclear Detection Office
BP – British Petroleum	DOC – Department of Commerce
BPD – Bureau of Public Debt	DOD – Department of Defense
BPSS – Boarding Pass Scanning Systems	DOL – Department of Labor
BUR – Bottom-Up Review	DRO – Detention and Removal Operations
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance	EDL – Enhanced Driver’s License
CAT – Credential Authentication Technology	EDS – Explosive Detection System
CBP – U.S. Customs and Border Protection	EFSP – Emergency Food and Shelter Program
CBRN – Chemical, Biological, Radiological, and Nuclear	ELIS – Electronic Immigration System
CDL – Community Disaster Loan	EMI – Emergency Management Institute
CDP – Center for Domestic Preparedness	ER – Efficiency Review
CFO – Chief Financial Officer	ESC – Executive Steering Committee
CFR – Code of Federal Regulations	ESF – Emergency Support Functions
CIKR – Critical Infrastructure and Key Resources	ESFLG – Emergency Support Function Leadership Group
CIO – Chief Information Officer	ETC – Enhanced Tribal Card
CIRT – Controlled Impact Rescue Tool	ETD – Explosive Trace Detection
CISO – Chief Information Security Officer	EWI – Enterprise Wireless Infrastructure
COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985	FAR – Federal Acquisition Regulation
COTR – Contract Officer’s Technical Representative	FBI – Federal Bureau of Investigation
COTS – Commercial Off-the-Shelf	FBwT – Fund Balance with Treasury
	FCRA – Federal Credit Reform Act of 1990
	FECA – Federal Employees Compensation Act



- FEMA – Federal Emergency Management Agency
- FERS – Federal Employees Retirement System
- FFMIA – Federal Financial Management Improvement Act of 1996
- FISMA – Federal Information Security Management Act
- FLETC – Federal Law Enforcement Training Center
- FMFIA – Federal Managers’ Financial Integrity Act
- FOSC – Federal On-scene Coordinators
- FPS – Federal Protective Service
- FTP – Full-time Position
- FY – Fiscal Year
- GAAP – Generally Accepted Accounting Principles
- GAO – Government Accountability Office
- GCCF – Gulf Coast Claims Facility
- GETS – Government Emergency Telecommunications Service
- GSA – General Services Administration
- GSP – Generalized System of Preferences
- HSA – Homeland Security Act of 2002
- HSGP – Homeland Security Grant Program
- HSIN – Homeland Security Information Network
- HSPD – Homeland Security Presidential Directive
- HS-STEM – Homeland Security Science, Technology, Engineering, and Mathematics
- ICCB – Internal Control Coordination Board
- ICE – U.S. Immigration and Customs Enforcement
- IDI – Injured Domestic Industries
- IED – Improvised Explosive Device
- IEFA – Immigration Examination Fee Account
- IHP – Individuals and Household Programs
- IILCM – Integrated Investment Life Cycle Model
- INA – Immigration Nationality Act
- IP – Improper Payment
- IPERA – Improper Payments Elimination and Recovery Act
- IPIA – Improper Payments Information Act of 2002
- ISA – Importer Self Assessment
- ISO – Immigration Services Officer
- IT – Information Technology
- LLNL – Lawrence Livermore National Laboratory
- LOI – Letters of Intent
- MCA – Managerial Cost Accounting
- MCO – Mission Critical Occupation
- MD&A – Management’s Discussion and Analysis
- MERHCF – Medicare-Eligible Retiree Health Care Fund
- MGMT – Management Directorate
- MHS – Military Health System
- MOA – Memorandum of Agreement
- MRS – Military Retirement System
- MTS – Metric Tracking System
- ND – Non-Disaster
- NFIP – National Flood Insurance Program
- NIST – National Institute of Standards and Technology
- NPFC – National Pollution Funds Center
- NPPD – National Protection and Programs Directorate
- nPRS – Next-Generation Period Reporting System
- NSA – National Security Agency
- NTAS – National Terrorism Advisory System
- NTC-P – National Targeting Center-Passenger
- OCAO – Office of the Chief Administrative Officer
- OCFO – Office of the Chief Financial Officer
- OCIO – Office of the Chief Information Officer
- OCPO – Office of the Chief Procurement Officer



- OFO – Office of Field Operations
- OHA – Office of Health Affairs
- OIG – Office of Inspector General
- OIIL – Office of Intelligence and Investigative Liaison
- OJT – On-the-Job Training
- OJTI – On-the-Job Training Instructor
- OMB – Office of Management and Budget
- OM&S – Operating Materials and Supplies
- OPA – Oil Pollution Act of 1990
- OPEB – Other Post Retirement Benefits
- OPM – Office of Personnel Management
- OPS – Office of Operations
- ORB – Other Retirement Benefits
- OSI – Office of Security and Integrity
- OSLTF – Oil Spill Liability Trust Fund
- OTO – Operational Tryout
- OTT – Operational and Technical Training Division
- PA – Public Assistance
- PA&E – Program Analysis and Evaluation
- PCS – Permanent-Change-of-Station
- PII – Personally Identifiable Information
- PM – Program Manager
- POA&M – Plan of Action and Milestones
- PPD – Presidential Policy Directive
- PP&E – Property, Plant, and Equipment
- Pub. L. – Public Law
- PY – Prior Year
- QHSR – Quadrennial Homeland Security Review
- Recovery Act – The American Recovery and Reinvestment Act of 2009
- RSSI – Required Supplementary Stewardship Information
- S/ACOM – Sustainment Acquisition Composite Model
- SAT – Senior Assessment Team
- SBI^{net} – Secure Border Initiative Network
- SBR – Statement of Budgetary Resources
- SCDL – Special Community Disaster Loan
- SCSS – Supply Chain Security Specialists
- SFFAS – Statement of Federal Financial Accounting Standards
- SFRBTF – Sport Fish Restoration Boating Trust Fund
- SMC – Senior Management Council
- S&T – Science and Technology Directorate
- TAFS – Treasury Account Fund Symbol
- TASC – Transformation and Systems Consolidation
- TCM – Trade Compliance Measurement
- TSA – Transportation Security Administration
- TSGP – Transit Security Grants Program
- TSO – Transportation Security Officers
- U.S. – United States
- U.S.C. – United States Code
- US-CERT - United States Computer Emergency Readiness Team
- USCG – U.S. Coast Guard
- USCIS – U. S. Citizenship and Immigration Services
- USM – Under Secretary for Management
- USSS – U.S. Secret Service
- VA – Veterans Affairs
- IBE – Validation Instrument for Business Enterprises
- WAN – Wide Area Network
- WHTI – Western Hemisphere Travel Initiative
- WYO – Write Your Own





Homeland
Security



Homeland
Security