DHS Annual Financial Report

Fiscal Year 2007

Homeland Security

Pursuant to OMB Circular A-136, this year's Finance and Performance reporting is following an Office of Management and Budget (OMB) Pilot Program for Alternative Approaches to Performance and Accountability Reporting. The pilot is an alternative to the consolidated Performance and Accountability Report (PAR) published in previous years. DHS anticipates this approach will improve its performance reporting by presenting performance information in a more accessible and informative format, and that performance information will be more complete given additional time to collect actual year-end performance data. Additionally, the pilot approach will ensure performance results and plans are integrated with the President's Budget.

The pilot consists of three separate reports:

- **DHS Annual Financial Report (AFR)**. The AFR (this report) consists of the Secretary's Message, Management's Discussion and Analysis, Financial Statements and Notes, the Audit Report, Major Management Challenges, and other required information. The AFR was published on 15 November 2007, and is available at the DHS website.

- **DHS Annual Performance Report (APR)**. The APR contains more detailed performance information as required by the Government Performance and Results Act (GPRA). The APR will report fiscal year (FY) 2007 results and will include the DHS performance plan for FY 2009. The APR will be transmitted with the Congressional Budget Justification (CBJ) on 4 February 2008 and posted on the DHS website within 10 days of submittal with the CBJ.

- **DHS Highlights Report**. The Highlights report summarizing key performance and financial information. It will be available by 1 February 2008, and will also be posted on the DHS website.

The Department of Homeland Security's FY 2007 Annual Financial Report
is available at the following website:
http://www.dhs.gov/xabout

For more information or to obtain additional copies, contact:

Department of Homeland Security
Office of the Chief Financial Officer
Program Analysis and Evaluation (PA&E)
245 Murray Lane SW
Mailstop 0200
Washington, DC 20528

par@dhs.gov
(202) 447-0333

Table of Contents

Message from the Secretary

November 15, 2007

I am pleased to provide the Department of Homeland Security's (DHS) Annual Financial Report (AFR) for fiscal year (FY) 2007. The report documents progress toward protecting the American people from terrorist attacks and natural threats and ensuring our Nation is prepared for any disaster that may befall this country. The report also demonstrates the effects of our hard work to ensure taxpayer dollars are accurately accounted for and effectively and efficiently used.

This year, we have made significant progress improving Department-wide internal controls for financial reporting. For the first time, I am able to provide assurances that internal control over financial reporting is designed effectively, with the exception of the material weaknesses listed in my Assurance Statements. Additionally, the report's performance measures are complete and reliable, and will be discussed in the forthcoming Annual Performance Report. The AFR is an alternative approach to the consolidated Performance and Accountability Report (PAR) published in previous years.

In FY 2007, the Department had roughly $57 billion in new budget authority. I set forth the following goals to focus our resources and efforts:

- Protect our Nation from dangerous people;
- Protect our Nation from dangerous goods;
- Protect critical infrastructure;
- Build a nimble, effective emergency response system and a culture of preparedness; and
- Strengthen and unify DHS operations and management.

The following highlights some of our achievements in meeting our goals as of the close of FY 2007:

- Added 2,574 Border Patrol agents, totaling 14,923 agents as of September 30, 2007. We are well on our way to meeting our goal of doubling the number of border patrol agents on the border.
- Effectively controlled 599 miles of border, an annual increase of 150 miles, through personnel, fencing, additional infrastructure, and technology integration.
- Removed 226,677 illegal aliens from the United States after a final order for removal was issued.
- Processed more than 6 million immigration applications and over half a million new citizens were naturalized.
- Screened 95 percent of all cargo entering the U.S. through radiation portal devices.
- Screened 86 percent of shipping containers at foreign ports before they were shipped to the United States through the Container Security Initiative (CSI), up from 48 percent in FY 2004. CSI is now deployed at 58 foreign ports.

- Achieved 100 percent safe arrival and departure for Secret Service protectees at more than 6,100 travel stops.
- Responded to 37,213 cyber security incidents, an increase of more than 50 percent over the previous year. The increase is due not only to more attacks on public and private networks, but also to increased situational awareness levels and reporting rates.
- Trained over 60,000 individuals by the Federal Law Enforcement Training Center, providing them skills needed to perform law enforcement duties to help secure our Nation.
- Confirmed that two-thirds of emergency response agencies use interoperable communications through the National Interoperability Baseline Survey – a nationwide survey of first responders and law enforcement that assessed progress in achieving interoperable communications.
- Upgraded the strategic stockpiles of emergency food and equipment.
- Activated an iDirect teleport to support deployed field teams with Internet, Voice over Internet Protocol, Video Teleconference, and streaming video capability.
- Dramatically improved internal controls over financial reporting and reduced the number of financial material weakness conditions, improving the Department's ability to report accurate and timely financial information.

We must continue our work to improve systems and information sharing to stay ahead of the terrorists, and others who wish us harm, as they will never relent. We must protect our borders to keep dangerous people and things from entering our country, and we must have plans in place to protect our critical infrastructure in case something would occur. We must continue our work to ensure that we can respond to and recover from natural disasters. In 2007, we invested significant time and effort to implement the requirements of the Post-Katrina Emergency Management Reform Act to focus our efforts on the greatest risks, to be nimble in our response to changing threats, and to be disciplined in our use of resources as we build a Department ready to meet future challenges. In all instances, we must draw upon the strength of our network of partners and assets, functioning as seamlessly as possible with State and local leadership, first responders, the private sector, our international partners, and, most certainly, the public.

It is no accident that we have not suffered a major terrorist attack on U.S. soil since September 11, 2001. It is the result of the President's leadership, congressional support, and the strident efforts and constant vigilance of hundreds of thousands of men and women –including the 208,000 employees of the Department of Homeland Security – who are working tirelessly both at home and overseas to protect our country. The Department will continue to effectively carry out its critical missions and will leave a strong legacy for the future.

Together we will make our Nation a safer place to live and thrive as a free and democratic people.

Sincerely,

Michael Chertoff

Message from the Chief Financial Officer

November 15, 2007

The Annual Financial Report (AFR) is our principal financial statement of accountability to the President, Congress and the American public, documenting the Department's progress in financial management and stewardship of taxpayer dollars. The FY 2007 audit is complete and I am encouraged by the results.

In every measure the audit shows that financial management at DHS has improved dramatically. Consider these highlights:

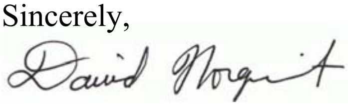
- We increased from four to seven, the number of organizations that do not contribute to a material weakness. This now includes Customs and Border Protection, Immigration and Customs Enforcement (ICE), Federal Law Enforcement Training Center, U.S. Citizenship and Immigration Services, U.S. Secret Service, US-VISIT, and Science and Technology;
- We reduced from 25 to 16, the number of Component conditions that contributed to our FY 2007 material weaknesses;
- We reduced Department-wide audit disclaimer conditions by 40 percent. The Transportation Security Administration no longer contributes to qualifications in the auditor's report; and
- Under the Chief Information Officer's leadership, the number of Components contributing to the Department-level information systems security material weakness went from six to three.

The FY 2007 audit shows our corrective actions are working. Earlier this year, we released the Internal Controls Over Financial Reporting (ICOFR) Playbook outlining our plan to resolve material weaknesses and build management assurances. I am particularly encouraged with how the corrective actions process has been sustained. Last year, ICE eliminated the majority of its material weaknesses and this year they maintained this success, a noteworthy achievement.

Audit challenges remain, albeit in much more focused areas. The U.S. Coast Guard and the Federal Emergency Management Agency (FEMA) account for 80 percent of the Department's remaining Component material weaknesses conditions. The U.S. Coast Guard's problems are particularly complex, but they have spent 2007 assembling the plan and staffing to tackle them.

Financial management at DHS has come a long way. I continue to be inspired by the extraordinary efforts of the Department's dedicated staff at Headquarters, in the Components, and in the finance centers at Indianapolis, Dallas, Burlington, Glynco, Chesapeake, and Mt. Weather. Our progress would not have been possible without their hard work and the strong support of the Secretary.

Sincerely,



David Norquist
Chief Financial Officer

Foreign Port "Rad/Nuke" Detection Underway

Situation

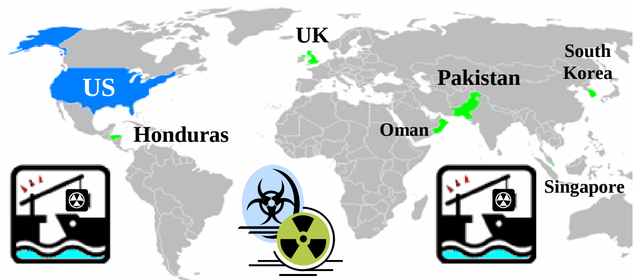
- Terrorists could use global shipping networks to send nuclear or radiological materials to the U.S.
- Early detection of materials is critical.
- Cooperation with foreign allies is imperative to scan containers before they depart for U.S. sea ports.
- Dec 7, 2006: Secure Freight Initiative (SFI) underway.

Action

- Mar 31, 2007 & Apr 2, 2007: DHS and the Department of Energy (DOE) announce detection is underway in Pakistan and Honduras.
- U.S. nuclear security and detection expertise used.
- Shipping containers scanned for nuclear and radiological materials before ships depart for U.S.
- Three "Phase I" SFI ports underway.

Result

- Data gathered from detectors is sent in near real time to CBP officers in foreign ports and to U.S.
- Data adds to risk assessment tools to improve analysis, targeting, and scrutiny of all containers.
- All alarms from detectors are resolved locally.
- If alarms not resolved, policy is "Do Not Load".



SFI "Phase I" Ports: Port Qasim, Pakistan; Puerto Cortes, Honduras; Southampton, United Kingdom; Salalah, Oman; Port of Singapore; Port Busan, South Korea

DHS Aids Rescue Efforts in Minnesota Bridge Collapse

Situation

- Aug 1, 2007: An eight-lane bridge collapses into the Mississippi River in Minneapolis, MN.
- Many victims are on the bridge and in the water.
- Bridge is a main artery of traffic for the Twin Cities.
- Collapse appears to be the result of structural deficiencies, not terrorism.
- Response: Over 75 Federal, State, & local agencies.

Action

- DHS's FEMA & USCG reach out to MN immediately.
- DHS assists State and local authorities in communications efforts.
- FEMA activates its Regional Response Coordination Center; lends logistical support to first responders.
- USCG deploys personnel and assets to assist in rescue operation; FBI & Navy divers added.

Result

- Efforts bolstered by the enhanced radio system made possible by Federal homeland security grants.
- Six ambulance services transport 55 victims within 1 hour and 53 minutes of the first call.
- Tragic incident demonstrates effectiveness of efforts put forth in prior years by DHS in devising plans to help governmental entities work together after terrorist attacks and natural catastrophes.

SUCCESS STORIES

U.S. Records Largest Maritime Cocaine Seizure

Situation

- Joint U.S. task force monitors and detects drugs.
- Intelligence plus strong interagency coordination among multiple agencies.
- Panama promptly responds to registry inquiry.
- International cooperation is the key to success.

Action

- Mar 18, 2007: Marine vessel Gatun is boarded.
- USCG cutter Sherman interdicts the Gatun under the cover of night.
- Supported by USCG cutter Hamilton & C-130 airship.
- USCG overcomes significant mechanical challenges.

Result

- Over 38,000 lbs of cocaine is seized on high seas.
- Value of cocaine: worth over $450 million.
- 14 crew detained, 11 sent to United States for trial: pled guilty.
- Three crew of Gatun turned over to Panama.
- Cocaine: 197,391 lbs seized in 1^{st} quarter FY 2007 vs. 148,514 lbs seized in 1^{st} quarter FY 2006.

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 pilot approach to performance and accountability reporting.

Mission and Organization

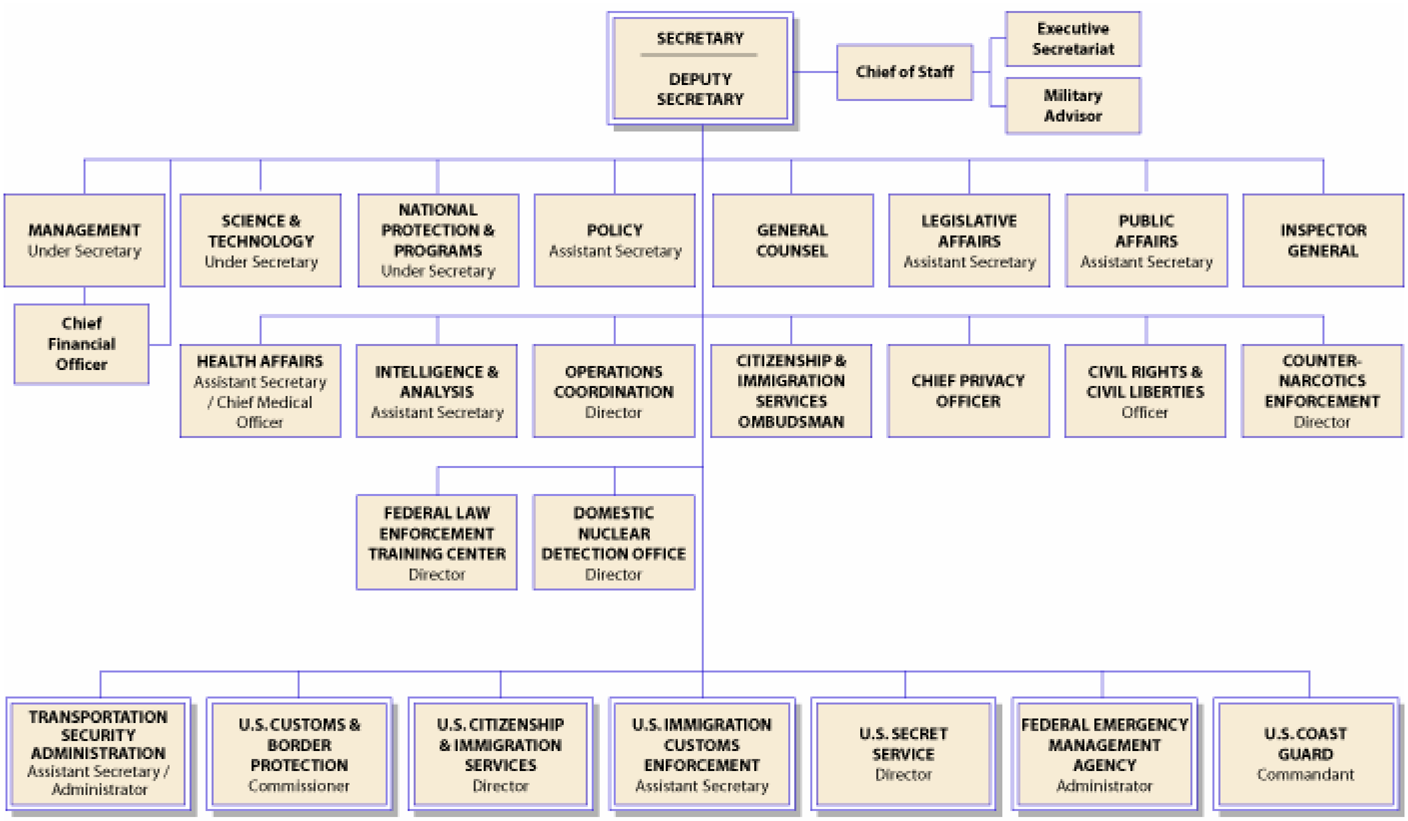
Our Mission

We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce.

Our Organization

Homeland Security leverages resources within Federal, State, and local governments, coordinating the transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the Federal, State, and local level have homeland security responsibilities. The comprehensive national strategy seeks to develop a complementary system connecting all levels of government without duplicating effort. Homeland Security is truly a "national mission." For more information visit our website at http://www.dhs.gov/xabout/structure.

Figure 1. DHS Organizational Chart

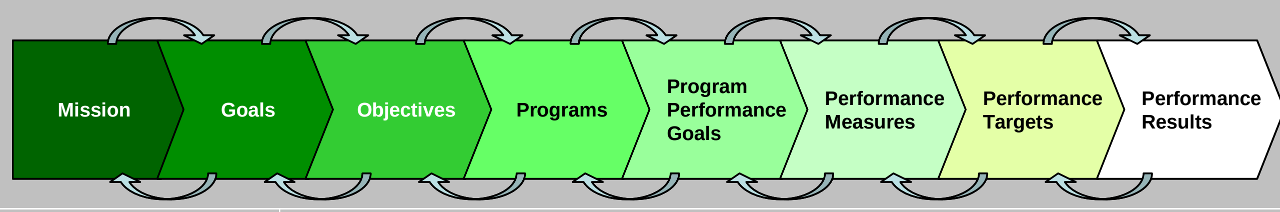


Performance Overview

Performance Management Framework

DHS is committed to strengthening our ability to report on performance results in achieving our goals and delivering value to the American public. Figure 2 presents the DHS performance management framework used to tie Department-wide goals and objectives to mission-oriented programs, and their associated program performance goals and performance measures. Terms used in the framework are defined in Figure 2. Following the framework, performance achievements and two key performance measures are presented for each Department-wide goal. More information on performance results may be found in the forthcoming DHS Highlights Report and DHS Annual Performance Report that will be published in conjunction with the Congressional Budget Justification.

Figure 2. DHS Performance Management Framework

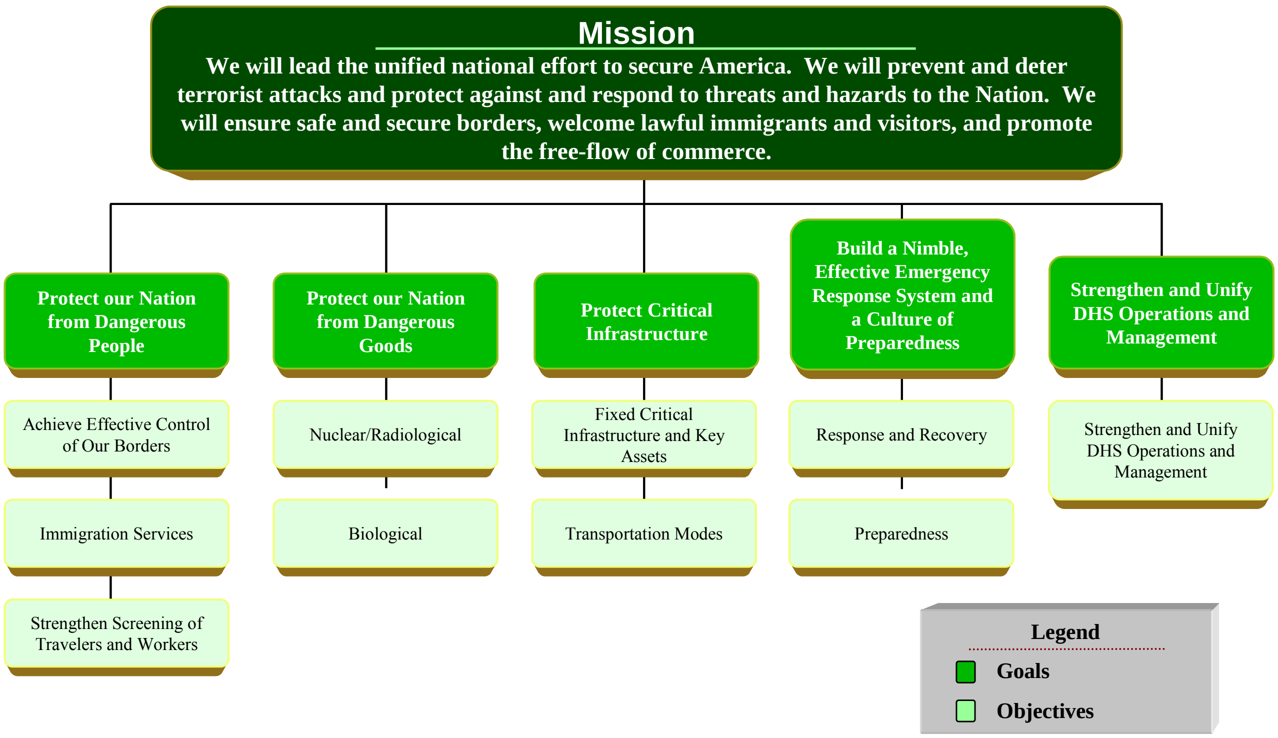


Mission:	Describes at the highest level what the Department aims to achieve.
Goal:	A goal is a statement of aim or purpose included in the Department's strategic plan. In the DHS Annual Performance Plan, goals are the overarching structure used to group multiple Department objectives and their associated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

Goals and Objectives

In FY 2007, we at the Department of Homeland Security structured our work around our Goals and Objectives. This plan consists of five goals and ten objectives as shown in the diagram below.

Figure 3. DHS Mission, Goals, and Objectives



The table below describes the outcomes that DHS strives to achieve through our Goals and Objectives.

Table 1. DHS Goal and Objectives

Goal 1. Protect our Nation from Dangerous People
Objective 1.1: Achieve Effective Control of Our Borders
Achieves outcome of: Reducing the risk of potential terrorists, instruments of terrorism, or other unlawful activities from entering the United States through our borders.
Objective 1.2: Immigration Services
Achieves outcome of: Ensuring lawful immigrants and visitors are welcomed and they receive timely and correct immigration information and benefits.
Objective 1.3: Strengthen Screening of Travelers and Workers
Achieves outcome of: Reducing the risk of potential terrorists, instruments of terrorism, or other unlawful activities from threatening our transportation systems.

Goal 2. Protect our Nation from Dangerous Goods

Objective 2.1: Nuclear/Radiological

Achieves outcome of: Reducing the risk of a nuclear or radiological attack in the United States.

Objective 2.2: Biological

Achieves outcome of: Reducing the risk of a biological attack in the United States.

Goal 3. Protect Critical Infrastructure

Objective 3.1: Fixed Critical Infrastructure and Key Assets

Achieves outcome of: Ensuring the protection and resiliency of the Nation's fixed critical infrastructure and key assets.

Objective 3.2: Transportation Modes

Achieves outcome of: Ensuring the protection of all transportation modes.

Goal 4. Build a Nimble, Effective Emergency Response System and a Culture of Preparedness

Objective 4.1: Response and Recovery

Achieves outcome of: Ensuring Americans and their governments at all levels can respond to and recover from catastrophic incidents.

Objective 4.2: Preparedness

Achieves outcome of: Ensuring Americans are prepared, capable, and ready to respond to adverse incidents.

Goal 5. Strengthen and Unify DHS Operations and Management

Objective 5.1: Strengthen and Unify DHS Operations and Management

Achieves outcome of: Ensuring that DHS management, intelligence, and other mission enabling activities support and improve integrated and informed DHS operations.

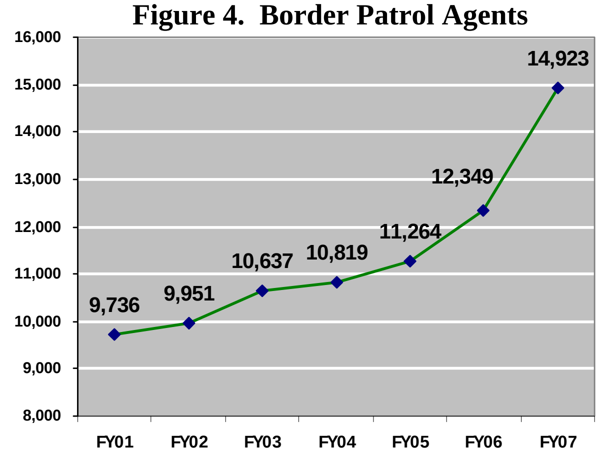
Performance Achievements and Key Performance Measures

This section presents performance achievements and selected key performance measures by Goal.

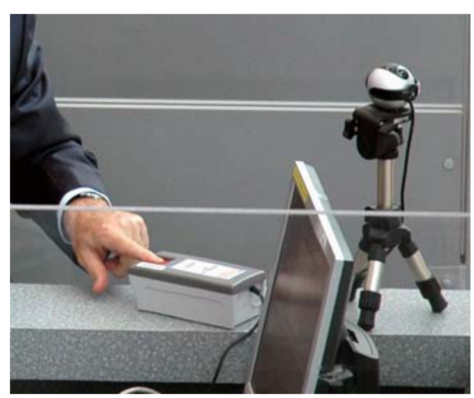
Goal 1. Protect our Nation from Dangerous People

DHS has made progress in achieving effective control of the border and improving the enforcement of our immigration laws in the interior. The Department's main priority is to prevent additional terrorist attacks against the Nation. By managing who enters the United States, DHS has worked to prevent the entry of terrorists while facilitating the legitimate flow of people, goods, and services. Below are a few FY 2007 achievements.

Figure 4. Border Patrol Agents



- **Effectively controlled 599 miles of border**, an annual increase of 150 miles, through personnel, fencing, additional infrastructure, and technology integration.
- **Added 2,574 Border Patrol agents**, totaling 14,923 agents as of September 30.
- **Arrested 18,327 fugitive aliens (2,681 criminals and 15,646 non-criminals).** Since 2005 ICE has increased the number of Fugitive Operations Teams from 18 to 75.
- **Removed 226,677 illegal aliens** from the United States after a final order for removal was issued.
- **Interdicted or deterred 93.7 percent of migrants** attempting to enter the United States via maritime routes.
- **Expanded the E-Verify Program**, a real-time Internet-based system with a new photo screening tool that enables employers to check the employment eligibility of new employees, and detect forged or fake immigration documents (in partnership with the Social Security Administration).
- **Processed more than 6 million immigration applications** and over 500,000 new citizens were naturalized.
- **Operated 4,000 metal detectors and 440 x-ray machines** at airport passenger check points across the country.
- **Trained 50,000 Transportation Security Officers** in advanced explosive detection.
- **Processed more than 120,000 transactions per day through the Automated Biometric Identification System** to support entry/exit screening, enforcement actions, benefit applications, and border crossing card and visa applications.
- **Tested and deployed e-Passport reader technology** in 33 U.S. airports for faster processing and improved security.



Biometric Fingerprint Scanner and Digital Camera

Program:	Border Security and Control between Ports of Entry
Program Performance Goal:	Gain effective control of the U.S. border in areas deemed as high priority for terrorist threat potential or other national security objectives.
Performance Measure:	Border miles under effective control.

Table 2. Border Miles under Effective Control Results

FY 2005	FY 2006	FY 2007		
Result	Result	Target	Result	Met
288	449	524	599	Y

Secretary Chertoff receives a briefing on Border Fence progress from CBP Patrol Agents

Explanation of Results:

Border Patrol exceeded its 524 mile target in FY 2007 through the continued application of the Border Patrol's multi-year strategy to deploy the right mix of personnel, tactical infrastructure, and technology to secure our borders. Most of the gains were attributable to the 2,574 new Border Patrol agents hired during the year. The Border Patrol also received augmentation by National Guard troops participating in Operation Jump Start (OJS). OJS National Guard troops manned Entry Identification Teams which brought additional miles of the border under surveillance. The Border Patrol completed construction of about 67 miles of new fence and 59 miles of new vehicle barriers along the southwest border. Finally, the Border Patrol added four ground surveillance radar systems that greatly enhanced its ability to detect illegal entries in some of the vast, remote areas on the southwest border.

Program:	Migrant Interdiction
Program Performance Goal:	Eliminate the flow of undocumented migrants via maritime routes to the United States.
Performance Measure:	Percent of undocumented migrants who attempt to enter the United States via maritime routes that are interdicted or deterred.

Table 3. Migrant Interdiction Results

FY 2004	FY 2005	FY 2006	FY 2007		
Result	Result	Result	Target	Result	Met
87.1%	85.5%	89.1%	91%	93.7%	Y

Migrant Interdiction Event at Great Bahamas Bank near Cape Lobos Light

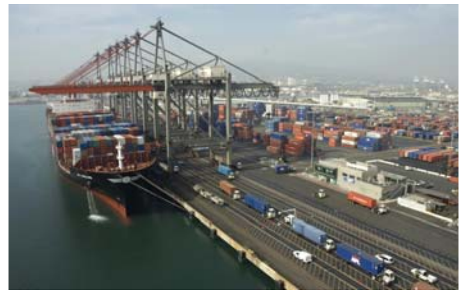
Explanation of Results:

The U.S. Coast Guard interdicted 6,336 total undocumented migrants, including 6,020 undocumented migrants from Cuba, Haiti, the Dominican Republic, and China in FY2007. Despite substantial growth in the threat estimate provided for these countries, successful illegal migrations have not increased significantly, and thus this metric continues to indicate success in interdicting or deterring undocumented migrants attempting to enter the United States via maritime routes. We witnessed a 53 percent drop in the flow of migrants from the Dominican Republic this year, likely due to improvements in political and economic conditions within that country. The U.S. Coast Guard also deployed a prototype mobile biometric identification system in the Mona Pass which identified 257 persons with database matches, 72 of which were brought ashore for prosecution.

Goal 2. Protect our Nation from Dangerous Goods

DHS is expanding its program to identify, track, and intercept nuclear and radiological components and systems at ports of entry and, where practicable, in transportation systems within U.S. borders. DHS is also intensifying its efforts to bolster capabilities to reduce the risk of a biological attack in the United States. Below are a few FY 2007 achievements.

- **Screened 95 percent of all cargo entering the United States** through radiation portal devices.
- **Deployed 157 radiation portal monitors,** which now total 1,012, to U.S. ports of entry, expanding our ability to screen cargo for radiological materials.
- **Screened all U.S. bound shipping containers for nuclear material at three foreign ports** as part of a Secure Freight Initiative operational test, to begin the screening process further from our shores.
- **Provided nuclear and radiological detection training to 2,041 law enforcement officers,** emergency response personnel, and public officials.



Cargo is removed from ship at the Port of Los Angeles/Long Beach. This is the largest and busiest port in the United States, handling about 45 percent of all incoming containers to the United States.

- **Deployed radiation detection network connections to 39 ports** to transmit data for analysis, targeting, and response; established around the clock tactical targeting and analytical research support for cargo related anti-terrorism targeting and screening.
- **Screened 86 percent of shipping containers at foreign ports** before they were shipped to the United States through the Container Security Initiative (CSI), up from 48 percent in FY 2004. CSI is now deployed at 58 foreign ports.
- **Embedded security features in a lightweight shipping container** to detect unauthorized intrusions. This was developed as part of a research project for potential use in securing cargo shipments.

Container Security Initiative Ports

- **Successfully tested the Rapidly Deployable Chemical Detection System** for use at National Special Security Events and other high priority special events.
- **Employed a total of 527 biological monitors in U.S. cities** determined to be at the highest risk for a biological incident.
- **Established agreements with seven interagency partners and the national biosurveillance integration center** continuing to build a comprehensive biosurveillance operating picture.
- **Completed Project BioShield material threat determinations** for all traditional biothreat agents of significant public health concern. The determinations are required to support buying stockpiles of new medical countermeasures.

Program: Domestic Nuclear Detection

Program Performance Goal: Improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport radiological or nuclear material for use against the Nation.

Performance Measure: Percent of cargo, by volume, that passes through radiation portal monitors upon entering the Nation.

Table 4. Radiation Portal Monitor Results

FY 2006	FY 2007		
Result	Target	Result	Met
85%	90%	95%	Y

Radiation Portal Monitors at Ports of Entry

Explanation of Results:

The Domestic Nuclear Detection Office worked with U.S. Customs and Border Protection to continue to deploy an additional 157 radiation portal monitors for screening cargo, with the majority of new systems deployed to the Nation's largest seaports. With the increased number of deployed radiation portal monitors, over 95 percent of incoming cargo containers were screened for dangerous radioactive materials, exceeding the target of 90 percent. A number of systems were also deployed to southern border crossings, where almost all cargo containers are now inspected as they enter the United States.

Program: Medical and Biodefense

Program Performance Goal: Bolster the Nation's biodefense readiness to rapidly detect, characterize, and respond effectively to a large-scale biological event.

Performance Measure: Number of bioaerosol collectors employed in the top threat cities.

Table 5. Bioaerosol Collector Results

FY 2004	FY 2005	FY 2006	FY 2007		
Result	Result	Result	Target	Result	Met
320	350	493	660	527	N

Biodefense Response Unit

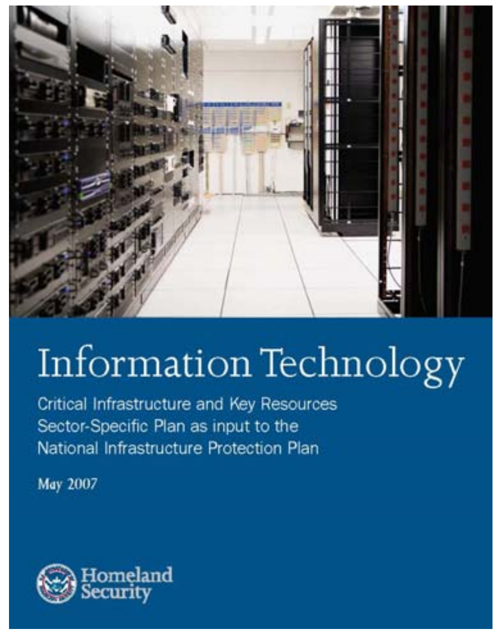
Explanation of Results:

The shortfall in the number of collectors employed is due to some jurisdictions' reluctance to employ bioaerosol collectors in indoor venues until the Biowatch Program issues public health response guidance providing response planning considerations for the indoor detection of biological agents. Effective response plans are necessary to prevent unintentional negative impacts resulting from a positive detection. Additionally, some jurisdictions have not employed indoor bioaerosol collectors as they are waiting for Generation 3 autonomous technology to become available, which will shorten the time it takes to identify and verify a positive hazard occurrence. Populations residing within those jurisdictional networks without fully operational collectors in indoor venues will remain partially at risk until an enhanced network to detect and respond to a covert biological agent attack is completed.

Goal 3. Protect Critical Infrastructure

The Department aims to protect critical infrastructure and key resources (CI-KR), essential government operations, public health and welfare, and the Nation's economic and national security interests that are dependent on that CI-KR. The Department also provides grants at the State and local levels to support planning, organization, equipment, training, and exercises. Below are a few FY 2007 achievements.

- **Arrested/cited 2,879 people, confiscated 764,018 prohibited items, and prevented 337 illegal weapons** from entering Federal buildings due to Federal Protective Service officer and agent intervention.
- **Responded to 37,213 cyber security incidents**, a more than 50 percent increase over the previous year. The increase is due not only to more attacks on public and private networks, but also to increased situational awareness levels and reporting rates.
- **Deployed the Einstein Program at a total of 12 Federal agency sites.** Einstein is a collection of hardware and software that supports an automated process to collect, correlate, analyze, and share cyber security information in defense of Federal Government networks.
- **Released 17 Sector-Specific Infrastructure Protection Plans** creating a comprehensive risk management framework to establish national priorities, goals, and requirements to protect CI-KR.
- **Established a coordinating council for State, local, tribal, and territorial governments** and formed 17 critical infrastructure government and sector coordinating councils to increase collaboration and coordination among stakeholders.



Information Technology Sector-Specific Plan

- **Established national standards for chemical facility security**, a comprehensive set of regulations to improve security at high-risk chemical facilities nationwide.
- **Achieved 100 percent safe arrival and departure for Secret Service protectees** at more than 6,100 travel stops. The Secret Service Domestic Protectees program operates 24 hours a day, 365 days a year to protect the President, Vice President and their families, former Presidents and their spouses, Presidential Candidates, and other individuals designated by statute or Presidential directive.
- **Evaluated security of 64 percent of passenger and mass transit rail systems** through Compliance Security Directive Reviews.

Secret Service Protection of the President

Program: Surface Transportation Security

Program Performance Goal: To protect the surface transportation system while ensuring the freedom of movement for people and commerce.

Performance Measure: Percent of nationally critical surface transportation assets or systems that have been assessed and have mitigation strategies developed based on those assessments.

Table 6. Surface Transportation Security Results

FY 2006	FY 2007		
Result	Target	Result	Met
31%	35%	37%	Y

Oil Pipeline

Explanation of Results:

This measure demonstrates progress in achieving a more secure surface transportation system. Surface Transportation Security operates in non-aviation modes including pipelines, maritime, mass transit, rail, highway and motor carrier and postal and shipping sectors. TSA partners with Federal, State, and local governments, and private industry to conduct assessments. This process enhances the owner/operators' ability to identify risk and develop mitigation strategies, thus improving surface transportation security. Strong partnerships have allowed TSA to surpass their 2007 target.

Program: Infrastructure Protection

Program Performance Goal: Protect the Nation's high-risk and most valued CI-KR by characterizing and prioritizing assets, modeling and planning protective actions, building partnerships, and issuing targeted infrastructure protection grants.

Performance Measure: Percent of high-priority critical infrastructure for which a Buffer Zone Protection Plan (BZPP) has been implemented.

Table 7. Buffer Zone Protection Results

FY 2005	FY 2006	FY 2007		
Result	Result	Target	Result	Met
18%	58%	65%	90%	Y

Nuclear Power Plant Cooling Towers

Explanation of Results:

BZPP is a DHS-administered grant program designed to provide resources to State, local, and tribal law enforcement and other security professionals to enhance security of priority CI-KR facilities. These plans involve a collaborative effort among facility operators and community first responders to identify site vulnerabilities and use this information to select and prioritize a set of protective actions to secure the area surrounding the CI-KR facility, including identifying personnel, equipment and training needs. As the program conducts a growing number of assessments, it has streamlined its processes, implemented best practices, and reduced redundancies leading to significant gains in efficiency.

Goal 4. Build a Nimble, Effective Emergency Response System and Culture of Preparedness

Improving the Nation's ability to respond to disasters, man-made or natural, is a top priority for the Department. Incorporating lessons learned from Hurricane Katrina, other disasters, and the 9-11 Commission Recommendations, the Department is improving its capabilities and preparing those who respond to acts of terror and other emergencies. Below are a few FY 2007 achievements.

- **Confirmed that two-thirds of emergency response agencies use interoperable communications** through the National Interoperability Baseline Survey – a nationwide survey of first responders and law enforcement that assessed progress in achieving interoperable communications. The national interoperability baseline survey was issued to 22,400 randomly selected law enforcement, fire response, and emergency medical services agencies.
- **Provided $968 million for communication interoperability initiatives,** totaling $3 billion since FY 2003, for States and territories through the Public Safety Interoperable Communications grant program (co-administered by the Department of Commerce).
- **Designed and deployed an interoperable Land Mobile Radio System** to allow the Urban Search and Rescue teams and Mobile Emergency Response Support units the ability to securely communicate amongst themselves and all other Components within DHS.

Greensburg, KS May 19, 2007 - Emergency Operations Center during the recovery effort from tornado.

- **Achieved capacity to register 200,000 disaster victims and inspect 20,000 homes per day** with FEMA mobile registration units.
- **Upgraded the strategic stockpiles of emergency food and equipment.**
- **Improved logistics management** by achieving near real-time tracking of trucks and equipment through improved planning and upgraded supply line management systems.
- **Created a preparedness coalition of 625 organizations** across national, regional, State, and local communities. Through successful sponsorship of the 4th Annual National Preparedness Month of September, more than 1,800 coalition members coordinated at least 1,000 events and activities across America in support of the *Ready Campaign*, reaching individuals, families, and diverse communities with the message of emergency preparedness.
- **Trained over 60,000 individuals by the Federal Law Enforcement Training Center**, providing them skills needed to perform law enforcement duties to help secure our Nation.

Program: Disaster Operations

Program Performance Goal: Ensure the core, coordinated Federal operational capability is in place to save lives, minimize suffering, and protect property in a timely and effective manner in communities overwhelmed by acts of terrorism, natural disaster, or other emergencies.

Performance Measure: Percent of response teams reported at operational status.

Table 8. Disaster Operations Team Results

FY 2005	FY 2006	FY 2007		
Result	Result	Target	Result	Met
50%	85%	88%	88%	Y

Response Team in Action

Explanation of Results:

Meeting the target of 88 percent of all teams reporting at operational status ensures that Federal emergency response systems and capabilities are properly poised to support States and communities overwhelmed by disasters and emergencies. The measure tracks the operational status of three types of teams: the 28 task forces of Urban Search and Rescue (US&R); the five Mobile Emergency Response Support (MERS) detachments; and the two Federal Incident Response Support Teams (FIRSTs). Operational status is defined as teams having the necessary staffing, equipment and training required for response to a disaster or incident.

Program: Disaster Assistance

Program Performance Goal: Help individuals and communities affected by federally declared disasters return to normal function quickly and efficiently, while planning for catastrophic disaster recovery operations.

Performance Measure: Percent of customers satisfied with individual recovery assistance.

Table 9.

FY 2004	FY 2005	FY 2006	FY 2007		
Result	Result	Result	Target	Result	Met
90.4%	93%	91%	91%	92.2%	Y

FEMA Community Relations Lead visiting a flood victim in his new housing with some ice after assisting in his relocation.

Explanation of Results:

This measure indicates the percent of respondents who said they were satisfied with the recovery assistance provided by this program. Results exceeded the established target by creating "engaging partnerships" with State and local governments, and enhancing disaster assistance capabilities through the operation of four National Processing Service Centers ensuring the timeliness of registrations. This well-established customer survey meets all industry standards, including neutrality and random selection. Responses gathered throughout the year are representative of the multitude of disaster assistance customers who received monetary housing and/or other needs assistance through Individual Assistance Programs.

Goal 5. Strengthen and Unify DHS Operations and Management

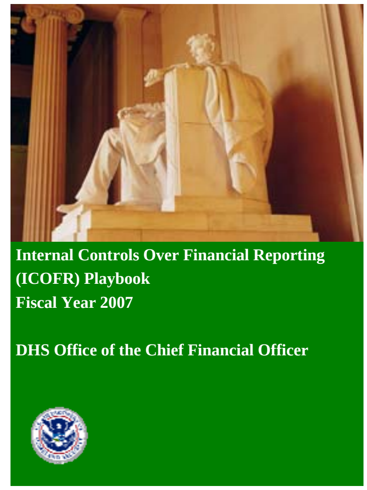
An agile and effective Department is essential to the rapid implementation of homeland security priorities, policies, and objectives. As such, DHS has aligned its programs and activities to its goals and objectives and is continuously measuring its achievement in meeting its targets. We continue to improve systems for intelligence and information sharing. Ensuring that DHS is managed and operated in an efficient and unified manner is a key to our success. Below are a few FY 2007 achievements.

- **Designed a consolidated DHS Headquarters facility** that will co-locate disparate national capital regional offices. The design completed phase one of the consolidation plan.
- **Increased leadership capacity** by adding 73 additional senior executive service positions – a 17 percent increase in the Senior Executive Service (SES) positions from FY 2006. Also reduced unfilled executive positions to 10 percent while improving executive hiring timeline.
- **Improved the hiring and retention of talent** needed to achieve DHS's mission by focusing on five key priorities in the FY 2007-2008 Human Capital Operational Plan and accomplishing all 47 goals identified for FY 2007.
- **Streamlined training delivery and opportunities for employees** through a new, comprehensive DHS University System and integrated Learning Management System.
- **Increased procurement operational and strategic sourcing effectiveness** by implementing a central DHS-wide Program Management Support Office.
- **Established a process for the DHS Chief Information Officer (CIO) to approve procurements that contain Information Technology (IT) elements of $2.5 million** and above to ensure that all contracts fully comply with the Federal Information Security Management Act (FISMA). Partnered with the Office of Procurement Operations (OPO) and Chief of Administrative Services (CAO) to share data to provide offices with advanced notice of procurements and purchases of property.
- **Implemented a strategy to enhance information sharing** by improving workflow, document management, and business processes to increase user satisfaction by 40 percent, decrease cost by 15 percent, and reduce production time by 25 percent.
- **Dramatically improved internal controls over financial reporting** and reduced the number of financial material weakness conditions, improving the Department's ability to report accurate and timely financial information.

National Operations Center (NOC)

- **Implemented Satellite Communications Network** to support disaster response and recovery efforts.
- **Integrated the Infrastructure Critical Asset Viewer** capability with the National Operations Center Common Operating Picture.
- **Activated an iDirect teleport** to support deployed field teams with Internet, Voice over Internet Protocol, Video Teleconference, and streaming video capability.

Program:	Departmental Management Operations
Program Performance Goal:	Provide comprehensive leadership, management, oversight, and support, while improving the effective and efficient delivery of business and management services throughout the Department.
Performance Measure:	Total instances of material weakness conditions reported by the independent auditor on the DHS financial statements.



FY 2007 Internal Controls over Financial Reporting (ICOFR)

Table 10. DHS Material Weakness Results

FY 2004	FY 2005	FY 2006	FY 2007		
Result	Result	Result	Target	Result	Met
26	28	25	≤ 25*	16	Y

Explanation of Results:

DHS has made significant progress towards getting a clean audit opinion by systematically working to eliminate our financial weaknesses. Annually, an independent auditor reviews DHS financial statements and reports to the public on areas that must be improved to ensure taxpayer dollars are accurately accounted for. On March 1, 2007 the Department issued the inaugural version of the Internal Controls Over Financial Reporting Playbook, outlining the Department's plan to correct material weakness conditions and build management assertions. By implementing and tracking progress against this plan, the Department was able to eliminate pervasive material weakness conditions.

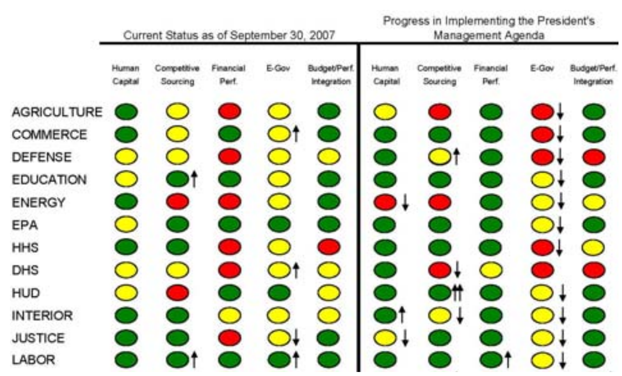
*The FY 2007 target and prior year results were restated in accordance with the revised methodology used by the Department's external auditors as required by OMB.

Program:	Departmental Management Operations
Program Performance Goal:	Provide comprehensive leadership, management, oversight, and support, while improving the effective and efficient delivery of business and management services throughout the Department.
Performance Measure:	Number of President's Management Agenda (PMA) initiative scores that improved over the prior year or were rated green in either status or progress.

Table 11. PMA Initiative Results

FY 2004	FY 2005	FY 2006	FY 2007		
Result	Result	Result	Target	Result	Met
6	6	6	7	5	N

Table 12. Executive Branch PMA Scorecard



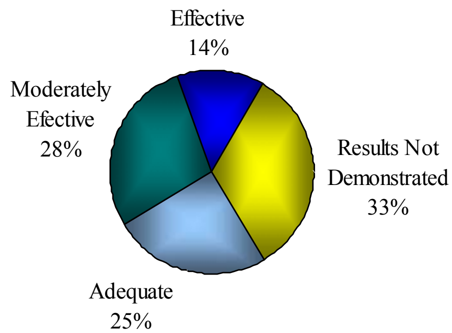
Explanation of Results:

In FY 2007, the Department continued work to improve in the President's Management Agenda (PMA) initiatives. DHS consistently performed in the areas of Real Property and Human Capital over the course of the year and was rated green in progress for both initiatives. The Department also earned a green rating in progress for Eliminating Improper Payments. Though there has been significant progress in all PMA initiatives, the Department missed the performance target in part because it did not meet all OMB expectations and milestones in Budget and Performance and E-government. Senior leadership within the Department closely monitors PMA performance, however, and has plans to address shortfalls in FY 2008 to ensure continued improvement.

PART Ratings Overview

Integral to DHS performance management are the program evaluations that occur in collaboration with the Office of Management and Budget (OMB) using the Program Assessment Rating Tool (PART). The PART process evaluates programs across a set of performance-related criteria, including program design, strategic planning, program management, and delivery of results. For more detailed information on PART, please visit www.expectmore.gov.

Figure 5. FY 2007 PART Ratings



Scorecard on the President's Management Agenda

DHS is also striving to improve critical management functions in the Department. Criteria for success and milestones to achieve progress are established in conjunction with OMB as part of the President's Management Agenda (PMA). The PMA was launched in August 2001 as a strategy for improving the management and performance of the Federal Government. For more information on the PMA, please visit www.results.gov. In addition, the Management Challenges section of the report discusses efforts under-way to improve the overall management of DHS.

Table 13. DHS PMA Scorecard as of the End of FY 2007

	Status				Progress
	FY '04	FY '05	FY '06	FY '07	FY '07
Human Capital	Red	Yellow	Yellow	Yellow	Green
Competitive Sourcing	Yellow	Yellow	Yellow	Yellow	Red
Financial Performance	Red	Red	Red	Red	Yellow
E-Government	Red	Red	Red	Yellow	Red
Budget & Performance	Yellow	Yellow	Yellow	Yellow	Red
Eliminating Improper Payments	Red	Red	Yellow	Red	Green
Real Property	Red	Red	Yellow	Yellow	Green

DHS integrates performance measurement results and PART evaluations into the development of a performance budget, using the Planning, Programming, Budgeting, and Execution (PPBE) process. As an element of the programming phase of the PPBE cycle, performance measurement information and program evaluations are considered in the resource allocation plans and decisions for each Component. The process culminates in the annual development of the Department's Future Years Homeland Security Program (FYHSP). The FYHSP expresses the Secretary's five-year strategic resource allocation intentions, and connects the multi-year spending priorities of each program in the Department with the achievement of the goals and objectives of the DHS Strategic Plan.

Completeness and Reliability of Performance Measures

The Department recognizes the importance of collecting complete, accurate, and reliable performance data, as this helps determine progress toward achieving our goals and objectives. As part of the annual planning and resource allocation process, the verification and validation information for performance measures is evaluated by both program and DHS Headquarters staff. This evaluation confirms that the scope of the data, the source of the data, the collection methodology, and methods to verify or double-check the accuracy of the data are in place. Program Managers are responsible to ensure the data collection and reporting follows the verification and validation procedures described for their performance measures.

Looking Forward

While the previous performance overview section presents achievements for the current fiscal year, below are a few of our focus areas in the coming year:

- We intend to continue our secure documentation requirements by moving forward on our Western Hemisphere Travel Initiative (WHTI). As early as the summer of 2008, we will start to require WHTI-compliant credentials - a passport, a People Access Security Service card, or other acceptable documents as defined in the final rule.
- With increased presence of personnel and technological advances, we will continue to improve the control of our Nation's borders. We will expand the number of Border Patrol agents and extend our fencing and vehicle barriers along our southern border. We intend to increase the use of manned and unmanned aerial surveillance and increase the number of camera and radar towers.
- To continue our efforts to protect our infrastructure from dangerous people and goods, we will be expanding our focus to include passenger screening requirements for private aircraft entering or departing from the United States to be in-line with requirements that currently apply to commercial air carriers. We will also be expanding our focus to include the 17 million "small boats" on our waterways to guard against the smuggling of weapons of mass destruction, water-borne improvised explosive devices, smuggling of dangerous people, and the potential use of these vessels to launch an attack on the maritime industry or other critical infrastructure.
- If we are going to progress in our efforts to protect people and critical infrastructure across our Nation, we need to concentrate more on how we share accurate, timely, and actionable intelligence, particularly with State and local governments. To that end, we are increasing our participation in State and local fusion centers. Our goal is to help build a national fusion center network.
- To meet our Department-wide goals in the coming years, it is essential that we continue our efforts to build a unified, integrated Department of Homeland Security. For example, OneNet will give us a secure, standard platform to facilitate information flow and streamline our IT infrastructure by consolidating seven locations into one.

Financial Overview

Overview and Analysis of DHS Financial Statements

DHS primarily uses the cash basis of accounting for its budget, which was approximately $57 billion for FY 2007. The budget represents our plan for 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 budgets using budgetary controls. DHS prepares its annual financial statements on an accrual basis, in accordance with generally accepted accounting principles, meaning that economic events are recorded as they occur, regardless of when cash is received or disbursed. These financial statements provide the results of our operations and financial position, including long-term commitments and obligations. The independent accounting firm, KPMG LLP, was engaged to audit the DHS statements.

DHS's FY 2007 budget increased by $2.7 billion from FY 2006, excluding borrowing authority, reflecting additional funding for Border Security, the Coast Guard, and the Domestic Nuclear Detection Office. During FY 2007, DHS underwent a substantial reorganization implementing lessons learned from the 2005 hurricane season and the effect those events had on the Departmental operations. The effects of the reorganization are discussed in Footnote 1. In addition, DHS restated FY 2006 balances primarily as a result of actions completed to correct financial management weaknesses reported in prior financial statement audit reports.

Balance Sheet

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

Table 14. Condensed Consolidated Balance Sheet
As of September 30, 2007 and 2006
(In Millions)

	FY 2007	FY 2006 (Restated)	Change
ASSETS			
Fund Balance with Treasury	$56,185	$59,569	($3,384)
General Property, Plant and Equipment, Net	12,275	11,151	1,124
Other	10,336	8,629	1,707
Total Assets	**$78,796**	**$79,349**	**($553)**
LIABILITIES			
Federal Employee and Veterans Benefits	$34,910	$32,278	$2,632
Debt	18,153	17,446	707
Employee related and other	10,801	16,529	(5,728)

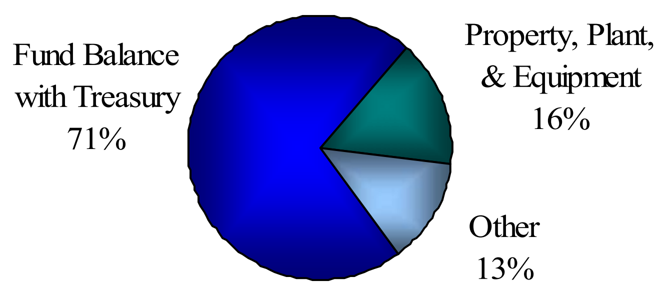
Accounts Payable	5,069	4,536	533
Total Liabilities (Note 17)	**$68,933**	**$70,789**	**($1,856)**
Net Position			
Unexpended Appropriations	$49,003	$48,816	$187
Cumulative Results of Operations	(39,140)	(40,256)	1,116
Total Net Position	**9,863**	**8,560**	**1,303**
Total Liabilities and Net Position	**$78,796**	**$79,349**	**($553)**

Composition of Assets

Assets represent amounts owned by DHS that can be used to accomplish its mission. At September 30, 2007, DHS had $78.8 billion in assets, representing a $553 million decrease from FY 2006 restated assets of $79.3 billion. The decrease is attributable to a reduction in the amount of cash DHS advanced to other federal agencies from FEMA's Disaster Relief Fund (described further in Footnote 13), decreases in receivables due from the public for reimbursable services and user fees, and slight decreases in inventory and related property, and other assets.

Fund Balance with Treasury (FBwT), which is the Department's largest asset, comprises 71 percent ($56.2 billion) of the total assets. Included in FBwT is the remaining balance of DHS unspent prior year budgets plus miscellaneous receipts. FBwT decreased approximately $3.4 billion from FY 2006 in part due to a reduction in refunds due to CBP for Canadian Softwood lumber duties, an increase in rescissions DHS-wide and a reduction in the amount of appropriations received by S&T.

Figure 6. DHS Assets as of September 30, 2007



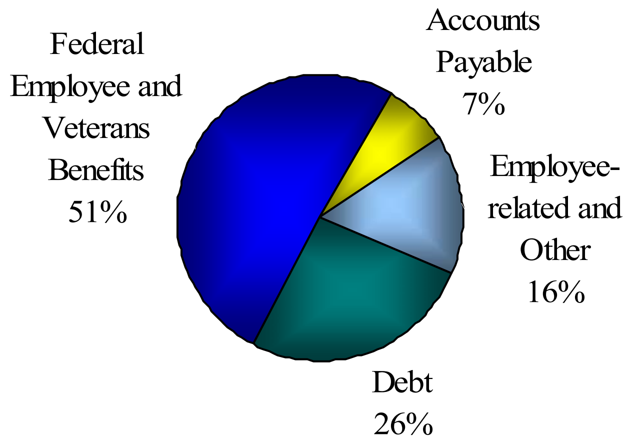
Property, Plant, and Equipment (PP&E) is the second largest asset, comprising 16 percent of total assets. The major items in this category include construction in progress, buildings and facilities, vessels, aircraft, and other equipment. In acquiring these assets, DHS either spent cash or incurred a liability to make payment at a future date; however, because we expect these assets to provide future benefits to DHS to help us accomplish our mission, we report 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 2007, PP&E increased by $1.1 billion. Contributing to this increase was CBP's initiative to protect America's borders by constructing fencing and implementing the Secure Border Initiative (SBI), a series of mobile sensor towers, as well as an increase to construction in progress for Coast Guard's Deepwater Program.

Composition of Liabilities

At September 30, 2007, DHS reported approximately $68.9 billion in total liabilities. Liabilities represent 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. Eight-one percent of these liabilities are unfunded, meaning they will need to be paid from funds received in future appropriations. DHS's largest unfunded liability is for Federal Employee and Veterans Benefits, arising primarily from U.S. Coast Guard personnel benefits. The National Flood Insurance Program (NFIP) administered by FEMA is the second largest unfunded liability. Both are discussed in more detail below.

Liabilities decreased of approximately $1.8 billion from FY 2006 restated liabilities totaling $70.8 billion. The decrease results from lower insurance liabilities existing at September 30, 2007 due to flood insurance claim payments related to hurricanes Katrina and Rita being made in 2006 (described further in Footnote 20) and a decrease in the amount of refunds and drawbacks due from CBP to importers and exporters at year-end.

Figure 7. DHS Liabilities as of September 30, 2007



DHS's largest liability is for Federal Employee and Veterans Benefits, representing 51 percent of total liabilities. This liability increased more than 8 percent from FY 2006 due to an increase in actuarial amounts for TSA and CG employees and an increase in personnel at CBP. 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 worker's compensation costs. Ninety-five percent of this liability is not covered by current budgetary resources, and DHS will need to seek future appropriations to cover these liabilities.

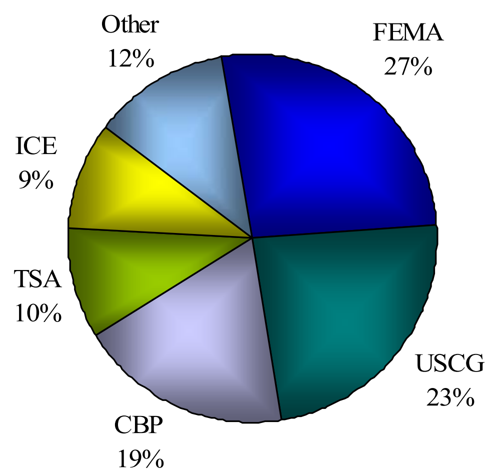
Debt is the next largest liability, representing 26 percent of total liabilities. This debt results from Treasury loans and related interest payable to fund the NFIP and Disaster Assistance Direct Loan Program operations of FEMA. Debt increased by 4 percent from FY 2006 as a result of the NFIP debt. Most of this debt is not covered by current budgetary resources. The premiums collected by FEMA for disaster assistance do not cover the cash outlays. Congress will need to enact legislation to provide funding to repay the Treasury Department, or to forgive the debt. This is discussed further in the Footnote 15.

Employee-related and other liabilities comprise 16 percent of the Department's liabilities, a decrease of almost 35 percent from FY 2006, due to the reduction of insurance liabilities and refunds and drawbacks, as discussed above. Also included in these liabilities are unpaid wages and benefits for current DHS employees. Seven 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

The Statement of Net Cost presents the annual net cost DHS expends to fulfill its mission. The statement shows all costs less certain revenue, such as fees collected at USCIS that offset our costs. For FY 2007, DHS used the Secretary's goals as a basis to integrate its net costs.

Figure 8. Composition of Net Costs at September 30, 2007



FEMA represents 27 percent of the Department's net costs, a 57 percent reduction from FY 2006 when FEMA funded much of the recovery costs associated with Hurricanes Katrina and Rita. USCG incurred 23 percent of total net costs in ensuring maritime safety, security, and stewardship and represents a slight increase from FY 2006. CBP's net costs increased by 15 percent from 2006, reflecting the increase in number of border patrol agents and costs associated with employing new technologies to protect the border. Net costs for TSA and ICE, representing 10 percent and 9 percent of total net costs, respectively, increased from FY 2006. TSA's net costs increased 17 percent as a result of an overall increase in program costs and increased costs for depreciation and benefits expenses. Net costs for ICE, which includes the Federal Protective Service, increased 9 percent.

During FY 2007, the Department earned approximately $8.4 billion in revenues; this is an increase of about $259 million from the restated amount of $8.2 billion on September 30, 2006. 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. Examples of non-exchange revenues are 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. Donations to the Department are also reported as non-exchange revenues. Non-exchange revenues are either retained by the Department to further its mission or returned to the General Fund of the Treasury.

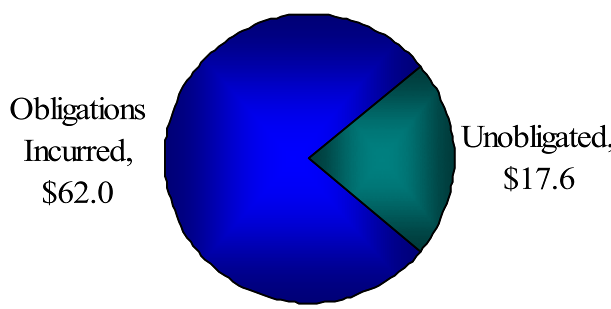
Statement of Changes in Net Position

The Statement of Changes in Net Position shows the "accrual-based" results of DHS's operations and its affect on our overall net financial 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 2007, FEMA had fewer disaster-related costs, thus contributing to the change in DHS's overall net position.

Statement of Budgetary Resources

This statement provides information on the status of the approximately $79.6 billion of budgetary resources available to DHS during FY 2007. This authority was derived from appropriations of $46.5 billion, $17.3 billion in authority carried forward from FY 2006, $9.9 billion in collections, and $5.9 billion of miscellaneous authority. The total amount of resources available decreased by approximately $29 billion, primarily as a result of a decrease of $17.5 billion in borrowing authority and increased obligations incurred during FY 2006 that reduced the FY 2007 unobligated carryover balance.

Figure 9. Status of Budgetary Resources at September 30, 2007 (in billions)



Of the total budget authority available, DHS incurred a total of $62 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 September 30, 2007, $17.6 billion of the $79.6 billion was not obligated.

Statement of Custodial Activities

This statement presents the disposition of revenues collected and disbursed by DHS on behalf of other recipient entities. CBP and USCIS collect revenue from a variety of duties, excise taxes and various other fees that are subsequently remitted to the Treasury's General Fund or to other entities. Footnote 32 provides additional information on these activities. Total cash collections increased by more than $2 billion in FY 2007. The increase is primarily attributable to an increase in duties, but also to an increase in user fees and excise taxes.

Stewardship Assets and Investments

DHS's Stewardship PP&E primarily consists of USCG Heritage Assets, which include sunken craft, ship's equipment, historical buildings, artifacts 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 agency. Of the USCG buildings and structures designated as Heritage Assets, including memorials, recreational areas and other historical areas, over two-thirds are multi-use Heritage assets. The remainder is comprised of historical lighthouses, which are no longer in use and awaiting transfer or disposal. CBP also 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.

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. These include investments in Human Capital and Research and Development.

Other Key Regulatory Requirements

See 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.C. 3512 Sections 2 and 4, and the Federal Financial Management Improvement Act, P.L. 104-208, are met. To identify material weaknesses and non-conformance 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 Non Compliance with Laws and Regulation; and
- Financial management systems conformance to government-wide systems requirements.

In addition, the Department of Homeland Security Financial Accountability Act, P.L. 108-330, requires a separate assertion of internal control over financial reporting 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 Office of Inspector General and the Government Accountability Office conduct reviews, audits, inspections, and investigations.

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

Homeland Security

November 15, 2007

Secretary's Assurance Statements

The Department of Homeland Security is dedicated to ensuring that internal control systems are comprehensively designed to achieve the mission and execute the strategy of the Department. The Department's management is responsible for establishing and maintaining effective internal control over the three internal control objectives of effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. In addition, the safeguarding of assets is a subset of these objectives. 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 controls at the Department of Homeland Security in effect during the fiscal year ended September 30, 2007. This evaluation was conducted in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*, revised December 21, 2004. Based on the results of this evaluation, the Department provides the following assurance statements.

Effectiveness of Internal Control over Financial Reporting (FMFIA § 2 and DHS FAA)

In accordance with the Department's OMB approved plan for Appendix A of OMB Circular A-123, our efforts focused on designing and implementing Department-wide internal controls. Based on information provided, for the processes assessed within Exhibit I, the Department provides reasonable assurance that internal control over financial reporting is designed effectively, with the exception of the following known material weaknesses:

- Entity Level Internal Controls at U.S. Coast Guard (USCG) and Federal Emergency Management Agency (FEMA);
- General Ledger Management including:
  - Financial Reporting at USCG, FEMA, DHS Headquarters (DHS HQ) Operational Offices; and
  - Intragovernmental Account Reconciliations;
- Fund Balances with Treasury Management at USCG;
- Financial System Security;
- Budget Resource Management at USCG, FEMA, and Transportation Security Administration (TSA);
- Property Management at USCG and FEMA;
- Grants Management at FEMA;
- Insurance Management at FEMA; and
- Human Resource and Payroll Management at USCG.

Although the Department has begun tests of operating effectiveness, we have not yet completed enough testing to provide reasonable assurance that internal control over financial reporting was operating effectively.

Effectiveness of Internal Control over Operations (FMFIA § 2)

Based on information provided, the Department provides reasonable assurance as to the effectiveness of internal control over operations, with the exception of the following known material weaknesses:

- Entity Level Internal Controls at FEMA and National Preparedness and Protection Directorate (NPPD);
- Improper Payments Information Act Noncompliance at FEMA;
- Anti-Deficiency Act Controls at TSA;
- Security Controls over Collection and Depositing of Fees at U.S. Citizenship and Immigration Services (USCIS);
- Federal Protective Service Transformation at U.S. Immigration and Customs Enforcement (ICE);
- DHS Headquarters Consolidation;
- Acquisition Management, including:
    - Deepwater Acquisition at USCG; and
    - Secure Border Initiative Acquisition at U.S. Customs and Border Protection (CBP);
- Human Capital Management;
- Information Technology Management, including:
    - Laptop Security at CBP;
    - Office of Chief Information Officer Management at USCIS; and
    - Personnel Data Security; and
- Long Term Strategic Planning and Outcome Based Management.

Conformance with Financial Management System Requirements (FMFIA § 4)

The Department's financial management systems do not substantially conform to government-wide requirements mandated by the Federal Financial Management Improvement Act. The following are known non-conformances:

- Federal Financial Management Systems Requirements, including:
    - Financial Systems Security;
    - Integrated Financial Management Systems, including:
        - Integration of CBP Revenue System with CBP Core Financial System;
        - Integration of ICE Financial, Acquisition, and Asset Management Systems;
        - Integration of USCG Financial and Mixed Systems;
- Noncompliance with U.S. Standard General Ledger at USCG; and
- Federal Accounting Standards at USCG.

Michael Chertoff

Summary of Internal Control Accomplishments

Since the passage of the *Department of Homeland Security Financial Accountability Act*, DHS has worked collaboratively with the Congress, the Government Accountability Office, OMB, DHS Inspector General, and our Independent Public Accountant to ensure we achieve the law's intended outcome of the design and implementation of Department-wide internal controls to support the DHS mission. On March 1, 2007, the Secretary issued the inaugural version of the Internal Controls Over Financial Reporting (ICOFR) Playbook. The ICOFR Playbook outlines the Department's strategy and process to design and implement internal controls through corrective actions and build management assertions for the operating effectiveness of internal controls. The results of the FY 2007 ICOFR Playbook are displayed below.

Table 15. Internal Controls over Financial Reporting Assessment Results FY 2007

Exhibit 1: Internal Controls over Financial Reporting Assessment Results FY 2007

Internal Control Component	DHS Headquarters	U.S. Customs & Border Protection	U.S. Coast Guard	U.S. Immigration & Customs Enforcement	Federal Emergency Management Agency	Transportation Security Administration	U.S. Citizenship & Immigration Services	Federal Law Enforcement Training Center	U.S. Secret Service	Science & Technology	Inspector General
Entity Level Controls											
General Ledger Management											
Fund Balance with Treasury Management											
Financial System Security											
Budgetary Resources Management											
Property Management		FY08		FY08				FY08			
Grants Management						FY08					
Payment Management	FY08										
Insurance Management											
Revenue Management		FY08	FY08	FY08	FY08	FY08					
Contingent Liabilities		FY08	FY08	FY08	FY08	FY08				FY08	
Receivable Management	FY08	FY08	FY08	FY08	FY08	FY08				FY08	
Human Resources and Payroll Management		FY08		FY08	FY08	FY08	FY08		FY08		

Legend

	Tests of Design (TOD) and Tests of Operating Effectiveness (TOE) Completed. No Material Weakness Conditions Identified.
	TOD Completed and Corrective Actions Implemented to Design Controls; however, TOE Not Yet Complete. No Material Weakness Condition Identified.
	Material Weakness Identified, Corrective Actions Needed.
FY 08	Process Scheduled for TOD in FY08.
	Process Deemed Immaterial to DHS Consolidated.

Office of Inspector General

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

Homeland Security

NOV 15 2007

MEMORANDUM FOR: The Honorable David Norquist
Chief Financial Officer

FROM: Richard L. Skinner
Inspector General

SUBJECT: Independent Auditors' Report on DHS' FY 2007 Internal Controls over Financial Reporting

The attached report presents our independent auditors' opinion on the Department of Homeland Security's (DHS) internal controls over financial reporting as of September 30, 2007. The Department of Homeland Security Financial Accountability Act (The Act) (P.L. 108-330) Section 4, requires that the Secretary of Homeland Security include an audit opinion of DHS' internal controls over its financial reporting in each performance and accountability report beginning after fiscal year 2005. DHS management is responsible for establishing and maintaining effective internal control over financial reporting in accordance with criteria established under the Federal Managers' Financial Integrity Act (FMFIA). Our responsibility is to express an opinion on the effectiveness of DHS' internal control based on our examination.

In our report on internal control as of September 30, 2006, we reported that DHS' internal controls over financial reporting were ineffective because of material weaknesses reported in the Secretary's Assurance Statement and the Independent Auditor's Report. Although deficiencies were identified in the same areas in fiscal year 2007, we recognize DHS efforts towards meeting its goals for the correction of material weaknesses and compliance with FMFIA.

We appreciate the cooperation extended to the auditors by DHS' 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

Office of Inspector General

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

Homeland Security

NOV 1 5 2007

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.

This report addresses the effectiveness of DHS' internal control over financial reporting. It is based on a review of applicable documents. We performed our review during the course of DHS' FY 2007 financial statement audit in conjunction with the independent public accountant, KPMG LLP. KPMG was engaged to audit the Department's balance sheet as of September 30, 2007 and 2006, and the related statement of custodial activity for the year ended September 30, 2007 (referred to herein as "financial statements"). KPMG was unable to provide an opinion on DHS' financial statements as of September 30, 2007 and 2006.

It is our hope that 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

Richard L. Skinner

Richard L. Skinner
Inspector General

Office of Inspector General

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

Homeland Security

NOV 1 5 2007

We have examined the effectiveness of DHS' internal control over financial reporting as of September 30, 2007 based on the criteria established under the Federal Managers' Financial Integrity Act (FMFIA). DHS management is responsible for establishing and maintaining effective internal control over financial reporting. Our responsibility is to express an opinion on the effectiveness of DHS' internal control based on our examination.

Our examination was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States and attestation standards, established by the American Institute of Certified Public Accountants. It included obtaining an understanding of the internal control over financial reporting and performing such other procedures as we considered necessary in the circumstances. We believe that our examination and the report of the independent auditor provide a reasonable basis for our opinion.

Because of inherent limitations in any internal control, misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A material weakness is a significant deficiency or combination of significant deficiencies that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

During fiscal year 2007, the following material weaknesses were identified by an independent auditor. Due to the issues noted below, additional material weaknesses may exist that have not been reported.

- Financial Management and Entity-Level Controls;
- Financial Reporting;
- Financial Systems Security;
- Fund Balance with Treasury;
- Capital Assets and Supplies;

- Actuarial and Other Liabilities;
- Budgetary Accounting.

Because of the effects of the material weaknesses mentioned above, in our opinion, DHS did not maintain effective internal control as of September 30, 2007, to meet the following objectives: (1) transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements and stewardship information in conformity with GAAP, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; and (2) transactions are executed in accordance with laws governing the use of budget authority and with other significant laws and regulations that could have a direct and material effect on the financial statements and stewardship information. Consequently, DHS' internal control did not provide reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

Richard L. Skinner
Richard L. Skinner
Inspector General

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

Homeland Security

November 15, 2007

MEMORANDUM FOR: Richard L. Skinner, Inspector General

FROM: David L. Norquist, Chief Financial Officer

SUBJECT: Audit Opinion of the Department's Internal Controls over Financial Reporting

Thank you for the opportunity to review your draft audit opinion of the Department's internal controls over financial reporting. I agree with your conclusions. I am pleased with how we have worked together to implement the *Department of Homeland Security Financial Accountability Act*. As we conclude the third year of implementing the Act, the progress the Department has made is remarkable. That success began with the strong working relationship between our offices, and in particular, Management's *Internal Control Over Financial Reporting Playbook* and your independent performance audits that together identified the root causes and the necessary corrective actions. While challenges remain, the Department has shown its ability to implement corrective actions, as evidenced by the following FY 2007 achievements:

- Strengthened the control environment and bolstered oversight functions with the strong support of the Department's Secretary and Under Secretary for Management;
- Executed year two of the Department's multi-year plan for OMB Circular No. A-123, resulting in the Secretary's first ever assurance statement on the design effectiveness of internal controls over financial reporting;
- Partnered with the Under Secretary for Management, Chief Information Officer, and Chief Information Security Officer, to achieve compliance with the *Federal Information Security Management Act*;
- Corrected material weakness conditions for Legal Liabilities and reduced the severity of Capitalization of Internal Use Software to a significant deficiency condition;
- Corrected TSA's Financial Reporting material weakness condition and reduced the severity of TSA's Capital Assets and Other Liabilities conditions to significant deficiencies;
- Sustained FY 2006 progress at ICE and eliminated all remaining ICE material weakness conditions;
- Designed Department-wide financial reporting process improvements; and
- Developed Department-wide financial management policies and procedures.

Thank you for your office's support throughout this audit. I look forward to continued cooperation and progress in the future.

SUCCESS STORIES

DHS's Critical Role to Take Down JFK Terror Plot

Situation

- January 2006: Four men led by a former airport cargo worker plot to ignite JFK airport jet fuel lines.
- The plot is revealed when the terrorists try to recruit a person who is a law enforcement informant.
- The Federal Bureau of Investigation (FBI) infiltrate terrorist cell; the FBI, Department of Justice, National Security Agency, Central Intelligence Agency, DHS (CBP, TSA), and international partners follow and monitor the cell for 18 months in U.S. and abroad.

Action

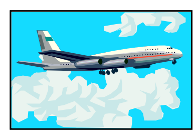
- DHS reaches out to leaders of the oil & gas sector and the transportation sector who run JFK airport.
- Sharing information helps private sector gain DHS assessments of the targets and analyze outcomes.
- As the FBI infiltrates the cell, DHS regularly briefs the sectors from onset to address concerns and fears.
- Jun 2, 2007: 3 men arrested; Jun 5: 4th is caught.

Result

- The plot is disrupted before it can take place.
- The private sector does not leak any information over 18 month period to jeopardize the operation.
- Industry sector representatives are impressed by access to information and regular briefings by DHS.
- The ability of DHS to share information with the private sector, as well as law enforcement, is critical to protecting the nation's critical infrastructure.

JFK International Airport Handles…

More than 1,000 flights daily, about half of which are international flights…



About 45 million passengers annually…

More than 1.5 million tons of cargo with an estimated value of $120 billion…

SUCCESS STORIES

USCG Has Conducted 1 Million Rescues Since Founding

Situation

- The USCG was founded in 1790 during George Washington's presidency with a fleet of just ten wooden vessels.
- Each year, thousands of boaters and marine enthusiasts find themselves in need of assistance on the open water.
- As the USCG has grown, so has its rescue mandate; in 2003 it joined the ranks of DHS.

Action

- The USCG deploys personnel and assets for a wide range of rescue operations.
- Rescues and other operations are often performed in dangerous conditions, forcing personnel to risk their own lives to save the lives of others.
- In 2007, the USCG received well over 27,000 calls for service.
- The USCG saved 4,536 lives in 2007 alone.

Result

- Since its inception, the USCG has saved the lives of at least 1,109,310 individuals.
- Included are migrant interdictions: Cubans/Haitians.
- In 2005, more than 33,000 people were rescued during Hurricane Katrina; 1937 saw the largest rescue of approximately 44,000 people.
- The USCG provides the world's fastest and most effective response to maritime distress calls for those in U.S. waters and elsewhere.

"[The U.S. Coast Guard has] …the same commitment to saving lives that it did more than 200 years ago." – Commandant Adm. Thad Allen

Financial Information

The ***Financial Information*** demonstrates our commitment to effective stewardship over the funds DHS receives to carry out the mission of the Department, including compliance with relevant financial management legislation. It includes the ***Independent Auditor's Report***, an independent opinion on the Balance Sheet and Statement of Custodial Activities provided by the Department's Office of Inspector General (OIG), and provides the Department's ***Annual Financial Statements*** and accompanying ***Notes to the Financial Statements***.

Introduction

The principal financial statements included in this report are prepared pursuant to the requirements of the *Chief Financial Officers Act of 1990 (P.L. 101-576)*, as amended by the *Government Management Reform Act of 1994 (P.L. 103-356)*. Other requirements include the Office of Management and Budget (OMB) Circular Number A-136, *Financial Reporting Requirements*. The responsibility for the integrity of the financial information included in these statements rests with the management of DHS. An independent certified public accounting firm, selected by the Department's Inspector General, was engaged to audit the Balance Sheet and the Statement of Custodial Activity. The independent auditors' report accompanies the principal financial statements. These financial statements include the following:

- The **Balance Sheets** present as of September 30, 2007 and 2006, those resources owned or managed by DHS which 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, 2007 and 2006. 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, 2007 and 2006.

- The **Statements of Budgetary Resources** present how and in what amounts budgetary resources were made available to DHS during FY 2007 and FY 2006, the status of these resources at September 30, 2007 and 2006, the changes in the obligated balance, and outlays of budgetary resources for the fiscal years ended September 30, 2007 and 2006.

- 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, 2007 and 2006.

- 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, 2007 and 2006.

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 agency in accordance with U.S. 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.

Independent Auditors' Report

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Independent Auditors' Report on DHS' FY 2007 Financial Statements

OIG-08-12 November 2007

Office of Inspector General

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

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 financial information excerpted from DHS' *Annual Financial Report* (AFR) and the results of the DHS financial statement audits for fiscal year (FY) 2007 and FY 2006. 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 was unable to provide an opinion on DHS' balance sheet as of September 30, 2007 and 2006. The FY 2007 auditor's report discusses eight significant deficiencies, seven of which are considered material weaknesses in internal control, and eight instances of noncompliance with laws and regulations. KPMG is responsible for the attached auditor's report dated November 15, 2007, and the conclusions expressed in the report. We do not express opinions on DHS' financial statements or internal control or conclusions on compliance with laws and regulations.

The recommendations herein have been discussed in draft with those responsible for implementation. It is our hope that 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Independent Auditor's Report on DHS' FY 2007 Financial Statements

Table of Contents

Office of Inspector General

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

Homeland Security

NOV 15 2007

MEMORANDUM FOR: The Honorable Michael Chertoff
Secretary

FROM: Richard L. Skinner
Inspector General

SUBJECT: *Independent Auditors' Report on DHS' FY 2007 Balance Sheet and Statement of Custodial Activity*

The attached report presents the results of the Department of Homeland Security's (DHS or Department) financial statement audits for fiscal year (FY) 2007 and FY 2006. These audits were required by the *Chief Financial Officers Act of 1990*. This report is incorporated into the *Department's FY 2007 Annual Financial Report*. We contracted with the independent public accounting firm KPMG LLP (KPMG) to perform the audits.

Generally the corrective action plans for DHS's non-military components, except for FEMA, have started to show results of improving financial reporting during FY 2007, although overall the department still has much work remaining. For the fourth year, KPMG was unable to provide an opinion on the department's balance sheet; although elements and conditions of prior year weaknesses have been corrected, material weaknesses exist in the same processes as in prior years.

Summary

KPMG was unable to express an opinion on the Department's balance sheets as of September 30, 2007 and 2006 and on the related statements of custodial activity for the years then ended, because DHS was unable to represent that certain financial statement balances were correct, and unable to provide sufficient evidence to support its financial statements. In connection with the audits, DHS' internal controls over financial reporting and compliance with certain provisions of laws and regulations were considered. As a result, the FY 2007 Independent Auditors' Report discusses seven material weaknesses, one other significant deficiency in internal control, and eight instances of non-compliance with laws and regulations, as follows:

Significant Deficiencies That Are Considered To Be Material Weaknesses

A. Financial Management and Entity-level Controls
B. Financial Reporting
C. Financial Systems Security
D. Fund Balance with Treasury

E. Capital Assets and Supplies
F. Actuarial and Other Liabilities
G. Budgetary Accounting

Other Significant Deficiency

H. Custodial Revenue and Drawback

Non-compliance with Laws and Regulations

I. Federal Managers' Financial Integrity Act of 1982 (FMFIA)
J. Federal Financial Management Improvement Act of 1996 (FFMIA)
K. Single Audit Act Amendments of 1996, and laws and regulations supporting OMB Circular No. A-50, Audit Follow-up, as revised
L. Improper Payments Information Act of 2002 (IPIA)
M. Chief Financial Officers Act of 1990
N. Government Performance and Results Act of 1993 (GPRA)
O. Debt Collection Improvement Act of 1996 (DCIA)
P. Anti-deficiency Act

Moving DHS' Financial Management Forward

While the auditors' noted improvement toward correction of internal control weaknesses, the Department was unable to represent that its financial statements as of, and for the year ended, September 30, 2007, were presented in conformity with U.S. generally accepted accounting principles. The U.S. Coast Guard, (USCG), DHS-HQ / Office of Financial Management (OFM), and Federal Emergency Management Agency (FEMA), were unable to provide sufficient evidence to support account balances presented in the financial statements and collectively contributed to the auditors' inability to render an opinion.

However, OFM has fully corrected its material weakness in *Financial Management and Entity Level Controls* reported in FY 2006. Additionally, in FY 2007 OFM, Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), US-Visit and the Federal Law Enforcement Training Center (FLETC) mitigated the severity of their financial systems security material weaknesses through corrective actions implemented during 2006 and 2007, but have not completely resolved their financial systems security control weaknesses as of September 30, 2007.

The Coast Guard began FY 2007 with a focus on financial management oversight, financial reporting, and fund balance with Treasury. However, the Coast Guard was not able to fully remediate prior year control weaknesses, and the auditors again reported that the Coast Guard contributed to all seven material weaknesses, and did not have an organizational structure that fully supported the development and implementation of effective policies, procedures, and internal controls. Management officials within the Coast Guard acknowledged to the auditors that longstanding procedural, control, personnel, and cultural issues existed and had impeded their progress in installing an effective financial management structure. The auditors' reported that the Coast Guard's personnel rotation policy, among other issues, made it difficult for the Coast Guard's Chief Financial Officer to institutionalize internal controls related to financial management and reporting.

Conditions at FEMA deteriorated in FY 2007 with FEMA now contributing to six material weaknesses instead of two material weaknesses in FY 2006. The auditors identified that FEMA has not established a financial management organizational structure, with clear oversight and supervisory review functions that support the development and implementation of effective policies, procedures, and internal controls over financial reporting, to ensure that accounting principles are correctly applied, and accurate financial data is submitted to OFM for consolidation in a timely manner. The auditors also noted that the FEMA Chief Financial Officer does not have clearly defined and complete authority and responsibility for all financial accounting policy, processes and control functions throughout the agency.

Many of the DHS' difficulties in financial management and reporting can be attributed to the original stand-up of a large, new, and complex executive branch agency without adequate organizational expertise in financial management and accounting. Although the Department made strides in remediating weaknesses during FY 2007, it has committed to focusing on remediation efforts at USCG and FEMA, while sustaining progress made throughout FY 2007. Additionally, the department remains committed to obtaining additional human resources and other critical infrastructure necessary to develop reliable financial processes, policies, procedures, and internal controls that will enable management to represent that financial statements are complete and accurate. These resources and infrastructure are critical to the implementation of effective corrective actions and to establishing an effective financial management oversight function. During the past year, the Department and its components continued the extensive effort to develop meaningful corrective action plans to address specific material internal control weaknesses. We are evaluating the effectiveness of those corrective action plans in a separate series of audits.

*****

KPMG is responsible for the attached independent auditor's report dated November 15, 2007, 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 each of the Department's chief financial officers provide us with a corrective action plan that demonstrates their progress in addressing the report's recommendations.

- 3 -

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 Richards, Assistant Inspector General for Audits, at 202-254-4100.

Attachment

- 4 -

KPMG LLP
2001 M Street, NW
Washington, DC 20036

INDEPENDENT AUDITORS' REPORT

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

We were engaged to audit the accompanying balance sheets of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2007 and 2006, and the related statements of custodial activity for the years then ended (referred to herein as "financial statements"). In connection with our fiscal year 2007 audit, we also considered DHS' internal controls over financial reporting, and DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on these 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, 2007 and 2006 (referred to herein as "other fiscal year 2007 and 2006 financial statements").

Summary

As discussed in our report on the financial statements, the scope of our work was not sufficient to express an opinion on the DHS balance sheets as of September 30, 2007 and 2006, or the related statements of custodial activity for the years then ended.

In fiscal year 2007, DHS changed its method of reporting the reconciliation of budgetary resources obligated to the net cost of operations, and changed its method of reporting certain mixed funding budgetary authority.

Our consideration of internal control over financial reporting resulted in the following conditions being identified as significant deficiencies:

A. Financial Management and Entity Level Controls
B. Financial Reporting
C. Financial Systems Security
D. Fund Balance with Treasury
E. Capital Assets and Supplies
F. Actuarial and Other Liabilities
G. Budgetary Accounting
H. Custodial Revenue and Drawback

We consider significant deficiencies A through G, above, to be material weaknesses.

We noted that DHS did not present five years of Required Supplemental Stewardship Information (RSSI) information, as required by U.S. generally accepted accounting principles.

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*:

I. *Federal Managers' Financial Integrity Act of 1982* (FMFIA)
J. *Federal Financial Management Improvement Act of 1996* (FFMIA)

K. *Single Audit Act Amendments of 1996*, and Laws and Regulations Supporting OMB Circular No. A-50, *Audit Follow-up,* as revised
L. *Improper Payments Information Act of 2002*
M. *Chief Financial Officers Act of 1990*
N. *Government Performance and Results Act of 1993*
O. *Debt Collection Improvement Act of 1996*
P. *Anti-deficiency Act*

We also reported other matters related to compliance with the *Anti-deficiency Act* at the National Protection and Programs Directorate (NPPD) and at the Federal Law Enforcement Training Center (FLETC).

Other internal control matters and other instances of non-compliance may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheets as of September 30, 2007 and 2006, and the related statements of custodial activity for the years then ended, and had we been engaged to audit the other fiscal year 2007 and 2006 financial statements.

The following sections discuss the reasons why we are unable to express an opinion on the accompanying DHS balance sheets as of September 30, 2007 and 2006, and on the statements of custodial activity for the years then ended; our consideration of DHS' internal control over financial reporting; 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 were engaged to audit the accompanying balance sheets of the U.S. Department of Homeland Security as of September 30, 2007 and 2006, and the related statements of custodial activity for the years then ended. 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, 2007 and 2006.

The United States Coast Guard (Coast Guard) was unable to provide sufficient evidential matter or make knowledgeable representations of facts and circumstances, that support transactions and account balances of the Coast Guard, as presented in the DHS balance sheets at September 30, 2007 and 2006; particularly with respect to fund balance with Treasury, accounts receivable, inventory and related property, certain categories of property, plant and equipment, actuarially-derived liabilities, environmental and other liabilities, undelivered orders and changes in net position, and adjustments, both manual and automated, made as part of Coast Guard's financial reporting process. The Coast Guard was unable to complete corrective actions, and make adjustments, as necessary, to these and other balance sheet amounts, prior to the completion of the DHS 2007 *Annual Financial Report* (AFR). Because of the significance of these account balances and/or transactions and conditions noted above, Coast Guard management was unable to represent that the Coast Guard's balance sheets as of September 30, 2007 and 2006, were fairly stated in conformity with U.S. generally accepted accounting principles. The total assets of Coast Guard, as reported in the accompanying DHS balance sheet, were \$15.9 billion and \$12.5 billion, or 20 percent and 16 percent of total DHS consolidated assets as of September 30, 2007 and 2006, respectively.

DHS Office of Financial Management (OFM) and certain DHS components were unable to reconcile intragovernmental transactions and balances with other Federal trading partners totaling approximately \$1.5 billion as of September 30, 2007, prior to the completion of the DHS 2007 AFR. In addition, DHS was unable to provide sufficient evidential matter to support its recording of \$1.5 billion in both fund balance with Treasury and undelivered orders at September 30, 2007, resulting from a budgetary allocation transfer made by the Office of Health Affairs (OHA), a DHS component, to another Federal agency, in fiscal year 2007. Because of the significance of this allocation transfer, DHS management was unable to represent that the balance sheet of OHA is fairly stated in conformity with U.S. generally

2

accepted accounting principles at September 30, 2007. The total assets of OHA, as reported in the accompanying DHS balance sheet as of September 30, 2007, were $3.3 billion or 4 percent of total DHS consolidated assets. In fiscal year 2006, OFM and certain DHS components were unable to provide sufficient evidential matter supporting the completeness and accuracy of the Department's accrued legal liability totaling $71 million as of September 30, 2006, and related contingent legal liabilities as disclosed in Note 21 to the financial statements; reconcile intragovernmental transactions and balances with other Federal trading partners totaling $3.5 billion, as of September 30, 2006; or provide sufficient evidential matter or make knowledgeable representations of the facts and circumstances that support its implementation of Statement of Federal Financial Accounting Standard (SFFAS) No. 27, *Identifying and Reporting Earmarked Funds*, prior to the completion of DHS' 2006 *Performance and Accountability Report* (PAR).

Federal Emergency Management Agency (FEMA) was unable to fully support the accuracy and completeness of certain stockpiled supplies, unpaid obligations related to mission assignments, and certain grants payable/advances, and the related effects on net position, if any, prior to the completion of the DHS 2007 AFR. The stockpiled supplies, as reported in the accompanying DHS balance sheet as of September 30, 2007 were $243 million or 38 percent of DHS' consolidated inventory and related property. FEMA's unpaid obligations related to mission assignments, as reported in the accompanying DHS balance sheet as of September 30, 2007, were $2.6 billion or 5 percent of DHS' consolidated unexpended appropriations. FEMA's net grants payable/advances, as reported in the DHS balance sheet as of September 30, 2007, were $149 million or 3 percent of DHS' consolidated accounts payable. The total net position of FEMA as reported in the accompanying DHS balance sheet as of September 30, 2007, was $10.1 billion or 12.8 percent of DHS' consolidated liabilities and net position. In fiscal year 2006, FEMA was unable to fully support the accuracy and completeness of certain unpaid obligations and accounts payable, and the related effect on net position, if any, prior to the completion of DHS' 2006 PAR. FEMA's unpaid obligations, as reported in the accompanying DHS balance sheet as of September 30, 2006, were $22.3 billion or 46 percent of DHS' consolidated unexpended appropriations. FEMA's accounts payable, as reported in the DHS balance sheet as of September 30, 2006, were $1.5 billion or 33 percent of DHS' consolidated accounts payable. The total net position of FEMA as reported in the accompanying DHS balance sheet as of September 30, 2006, was $11.2 billion or 14 percent of DHS' consolidated liabilities and net position.

In fiscal year 2006, Transportation Security Administration (TSA) was unable to provide sufficient evidential matter or make knowledgeable representations of facts and circumstances that support certain transactions and account balances of TSA, as presented in the DHS balance sheet at September 30, 2006, particularly with respect to property and equipment, accounts payable, accrued unfunded employee leave, and the components of net position. Because of the significance of these account balances and/or transactions and conditions noted above, TSA management was unable to represent that TSA's balance sheet as of September 30, 2006, was fairly stated in conformity with U.S. generally accepted accounting principles. The total assets of TSA as reported in the accompanying DHS balance sheet as of September 30, 2006, were $4.1 billion or 5 percent of DHS consolidated assets.

In fiscal year 2006, Immigration and Customs Enforcement (ICE), was unable to fully support the accuracy and completeness of certain accounts payable and undelivered orders, and the related effect on net position, if any, prior to the completion of the DHS 2006 PAR. ICE's accounts payable and undelivered orders, as reported in the accompanying DHS balance sheet as of September 30, 2006, were $319 million or 7 percent of DHS' consolidated total accounts payable, and $1.2 billion or 2.5 percent of DHS' consolidated unexpended appropriations, respectively.

In fiscal year 2006, the Management Directorate was unable to fully support the accuracy and completeness of certain accounts payable and undelivered orders, and the related effect on net position, if any, prior to the completion of the DHS 2006 PAR. The Management Directorate's accounts payable and undelivered orders, as reported in the accompanying DHS balance sheet as of September 30, 2006, KPMG

were $60 million or 1.3 percent of consolidated total accounts payable, and $527 million or 1.1 percent of DHS consolidated unexpended appropriations, respectively.

In addition, we were unable to obtain appropriate representations from DHS management, regarding the matters described above, including certain representations as to compliance with U.S. generally accepted accounting principles, with respect to the accompanying DHS balance sheets and related statements of custodial activity as of and for the years ended September 30, 2007 and 2006, and were unable to determine the effect of the lack of such representations on the 2007 and 2006 DHS' financial statements.

It was impractical to extend our procedures sufficiently to determine the extent, if any, to which the DHS balance sheets as of September 30, 2007 and 2006, and the related statements of custodial activity for the years then ended, may have been affected by the matters discussed in the seven preceding paragraphs. Accordingly, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on these 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, 2007 and 2006, and accordingly, we do not express an opinion on these financial statements.

As discussed in Note 34, DHS restated its fiscal year 2006 financial statements to correct multiple errors identified by TSA, ICE, NPPD, United States Citizenship and Immigration Services, Science and Technology Directorate, FLETC, and Management Directorate that required adjustment of balances previously reported in DHS' fiscal year 2006 financial statements. Because of the matters discussed above regarding our fiscal year 2006 audit, and the control deficiencies described in our report on internal control over financial reporting, we were unable to audit the restatements discussed in Note 34, and accordingly, we have not concluded on the appropriateness of this accounting treatment or the restatement of the DHS balance sheet as of September 30, 2006.

As discussed in Notes 35 and 36 to the financial statements, in fiscal year 2007, DHS changed its method of reporting the reconciliation of budgetary resources obligated to the net cost of operations and changed its method of reporting certain mixed funding budgetary authority.

The information in the Management's Discussion and Analysis (MD&A), RSSI, and Required Supplementary Information (RSI) sections of the DHS AFR is not a required part of the financial statements, but is supplementary information required by U.S. generally accepted accounting principles and OMB Circular A-136. 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 previous paragraphs of this section of our report. Certain information presented in the MD&A, RSSI, and RSI is based on fiscal year 2007 and 2006 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, in fiscal year 2007, we noted that DHS did not present five years of RSSI information that U.S. generally accepted accounting principles has determined is necessary to supplement, although not required to be part of, the financial statements.

The information in pages 12 through 23, Section II – Performance Achievements and Key Performance Measures, Section IV – Other Accompanying Information, and Section V – Appendices, of DHS' 2007 AFR are presented for purposes of additional analysis, and are 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.

Internal Control over Financial Reporting

Our consideration of the internal control over financial reporting was for the limited purpose described in the Responsibilities section of this report and would not necessarily identify all deficiencies in the internal control over financial reporting that might be significant deficiencies or material weaknesses.

KPMG

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects DHS' ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of DHS' financial statements that is more than inconsequential will not be prevented or detected by DHS' internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by DHS' internal control.

Significant deficiencies in internal control over financial reporting and its operation are described in Exhibits I, II, and III. Deficiencies that are considered to be material weaknesses at the Coast Guard, when aggregated at the consolidated level, are presented in Exhibit I. Deficiencies that are considered to be material weaknesses at DHS-Headquarters (HQ), OFM, and all other DHS components, when aggregated at the consolidated level, are presented in Exhibit II. Exhibit III presents other significant deficiencies that are not considered to be material weaknesses. As discussed in the Report on the Financial Statements section, the scope of our work was not sufficient to express an opinion on the balance sheets as of September 30, 2007 and 2006, and the related statements of custodial activity for the years then ended, and accordingly, other internal control matters may have been identified and reported had we been able to perform all procedures necessary to express an opinion on those financial statements, and had we been engaged to audit the other fiscal year 2007 and 2006 financial statements. A summary of the status of fiscal year 2006 reportable conditions is included as Exhibit V.

We also noted certain additional matters involving internal control over financial reporting and its operation that we will report to the management of DHS in a separate letter.

Compliance and Other Matters

Our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements, as described in the Responsibilities section of this report, exclusive of those referred to in the FFMIA, disclosed eight instances of noncompliance that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 07-04, and are described in Exhibit IV.

The results of our tests of compliance exclusive of those referred to in FFMIA, disclosed no other 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 Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level.

As discussed in our report on the financial statements, the scope of our work was not sufficient to express an opinion on the balance sheets as of September 30, 2007 and 2006, and the related statements of custodial activity for the years then ended, and accordingly, other instances of non-compliance with laws, regulations, contracts, and grant agreements may have been identified and reported, had we been able to perform all procedures necessary to express an opinion on those financial statements, and had we been engaged to audit the other fiscal year 2007 and 2006 financial statements.

Other Matters. NPPD management has initiated a review of the classification and use of certain funds that may identify a violation of the *Anti-deficiency Act*, or other violations of appropriation law in fiscal year 2007 or in previous years. In addition, FLETC management has initiated a review of the classification of certain liabilities, recorded in their accounting records that may identify a violation of

5

the *Anti-deficiency Act,* or other violations of appropriation law that may have occurred during fiscal year 2007 or during previous years.

Management's Response to Internal Control and Compliance Findings

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's response and, accordingly, we express no opinion on it.

Responsibilities

Management's Responsibilities. The United States Code, Title 31, Sections 3515 and 9106 require agencies to report annually to Congress on their financial status and any other information needed to fairly present their financial position and results of operations. To meet these reporting requirements, DHS prepares and submits financial statements in accordance with OMB Circular No. A-136.

Management is responsible for the financial statements, including:

- Preparing the financial statements in conformity with U.S. generally accepted accounting principles;
- Preparing the MD&A (including the performance measures), RSI, and RSSI;
- Establishing and maintaining effective internal control; and
- Complying with laws, regulations, contracts, and grant agreements applicable to DHS, including FFMIA.

In fulfilling this responsibility, management is required to make estimates and judgments to assess the expected benefits and related costs of internal control policies.

Auditors' Responsibilities. As discussed in the report on the financial statements section, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on the DHS balance sheets as of September 30, 2007 and 2006, or on the related statements of custodial activity for the years then ended; and 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, 2007 and 2006.

In connection with our fiscal year 2007 engagement, we considered DHS' internal control over financial reporting by obtaining an understanding of DHS' internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and OMB Bulletin No. 07-04. We did not test all internal controls relevant to operating objectives as broadly defined by the FMFIA. The objective of our engagement was not to provide an opinion on the effectiveness of DHS' internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of DHS' internal control over financial reporting. Further, other matters involving internal control over financial reporting may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheet as of September 30, 2007, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other fiscal year 2007 financial statements.

In connection with our fiscal year 2007 engagement, 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, 2007, 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 certain provisions referred to in 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 the DHS. However, providing an opinion on compliance with laws, regulations, contracts, and grant agreements was not an objective of our engagement and, accordingly, we do not express such an opinion. In addition, other matters involving compliance with laws, regulations, contracts, and grant agreements may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheet as of September 30, 2007, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other fiscal year 2007 financial statements.

Under OMB Bulletin No. 07-04 and FFMIA, we are required to report whether DHS' financial management systems 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. To meet this requirement, we performed tests of compliance with FFMIA Section 803(a) requirements. However, as discussed in our report on the financial statements, the scope of our work was not sufficient to express an opinion on the balance sheet as of September 30, 2007, and the related statement of custodial activity for the year then ended, and accordingly, other instances of non-compliance may have been identified and reported, had we been able to perform all procedures necessary to express an opinion on the those financial statements, and had we been engaged to audit the other fiscal year 2007 financial statements.

Restricted Use

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 15, 2007

7

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, contacts, and grant agreements presented herein were identified during our engagement to audit the Department of Homeland Security (DHS or Department) balance sheet and related statement of custodial activity as of and for the year ended September 30, 2007. We were not engaged to audit the Department's fiscal year 2007 statements of net cost, changes in net position, and budgetary resources (referred to as other fiscal year 2007 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 Coast Guard. All of the significant deficiencies reported in Exhibit I are considered material weaknesses that individually, or when combined with other significant deficiencies reported in Exhibit II, are considered material weaknesses at the DHS consolidated financial statement level.

Exhibit II Significant deficiencies in internal control identified at other DHS components and the Office of the Chief Financial Officer (collectively referred to as DHS Civilian Components). All of the significant deficiencies reported in Exhibit II are considered material weaknesses that individually, or when combined with other significant deficiencies reported in Exhibit I, are considered material weaknesses at the DHS consolidated financial statement level.

Exhibit III A significant deficiency that is 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*.

Exhibit V The status of our findings reported in fiscal year 2006.

As stated in our Independent Auditors' Report, our consideration of internal control over financial reporting would not necessarily disclose all matters that might be significant deficiencies or instances of noncompliance. We were not engaged to audit the other 2007 financial statements. In addition, the scope of our work was not sufficient to express an opinion on the financial statements that we were engaged to audit; consequently, other internal control matters and instances of noncompliance may have been identified and reported had we been engaged to audit all of the FY 2007 financial statements, and had we been able to perform all procedures necessary to express an opinion on those financial statements.

The determination of which findings rise to the level of a material weakness is based on an evaluation of how all component conditions, considered in aggregate, may affect the DHS balance sheet as of September 30, 2007 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. All of the material weaknesses identified and reported in Exhibit I for the Coast Guard are repeated from our FY 2005 and FY 2006 report, and include updates for new findings resulting from our 2007 audit procedures. To provide trend information for the DHS Civilian Components, Exhibit II contains a Trend Table next to the heading of each finding, except Exhibit II-C, *Financial Systems Security*. The Trend Table depicts the level and current status of findings, by component, that have contributed to that finding from 2005 through

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

2007. Significant deficiencies and material weaknesses, by component, included in the Exhibit II trend tables, are presented below.

The table below presents a summary of our internal control findings, by component, for fiscal year 2007. We have reported seven material weaknesses at the Department level in 2007, which is reduced from ten reported in 2006. While the DHS Civilian Components have made substantial progress in correcting control deficiencies, as shown in the Trend Tables in Exhibit II, the reduction in material weaknesses at the Department level in 2007 is due to a consolidation of findings into fewer, but broader categories for reporting purposes.

SUMMARIZED DHS FY 2007 INTERNAL CONTROL FINDINGS

		Coast Guard	DHS HQ	CBP	FEMA	ICE	US - Visit	TSA	FLETC
Material Weaknesses		Exhibit I	Exhibit II						
A	Financial Management & ELC	MW			MW				
B	Financial Reporting	MW	MW		MW			SD	
C	Financial Systems Security	MW	SD	SD	MW	SD		MW	SD
D	Fund Balance With Treasury	MW							
E	Capital Assets and Supplies	MW			MW		SD	SD	
F	Actuarial and Other Liabilities	MW			MW			SD	
G	Budgetary Accounting	MW			MW			MW	
Significant Deficiencies			Exhibit III						
H	Custodial Revenue and Drawback			SD					

SD Significant Deficiency (SD's in Exhibit II contribute to Department level material weakness)
MW Material Weakness (individually, or when combined with other findings, result in Department level material weakness)

All components of DHS, as defined in Note 1A – *Reporting Entity,* to the financial statements, were included in the scope of our engagement to audit the consolidated balance sheet of DHS as of September 30, 2007 and the related statement of custodial activity for the year then ended. Accordingly, our audit considered significant account balances and transactions 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 reportable control deficiency at the DHS consolidated financial statement level.

i.2

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

I-A Financial Management and Entity-Level Controls

Background: In FY 2006, we reported that significant weaknesses in financial management oversight hindered the United States Coast Guard's (Coast Guard) ability to prepare accurate, complete, and timely financial information. Those conditions have not been corrected and continue to affect Coast Guard's financial management and reporting processes. During FY 2007, the Coast Guard developed a Corrective Action Plan (CAP) called the *Financial Strategy for Transformation and Audit Remediation* (FSTAR) to address the conditions described below, and throughout this Exhibit. However, significant steps to correct the conditions that cause the material weaknesses in internal control are not planned until after 2007.

Conditions: Many of the conditions described below are indicators of a weak control environment or entity-level controls. The control environment begins at the top with the Commandant, and permeates the organization with a mindset of quality, care, and commitment of resources to reasonably ensure the integrity of the Coast Guards' financial processes, controls, and information technology (IT) systems. We noted the following conditions related to the control environment which existed in prior years, and have been updated for this report.

The Coast Guard has not fully implemented a financial management organizational structure where:

- U.S. generally accepted accounting principles (GAAP) are applied and financial statement balances are appropriately supported, resulting in the Coast Guard not being able to assert to the completeness, existence (validity), accuracy, valuation, or presentation of their financial data.
- Appropriate and clear internal reporting relationships have been established resulting in effective financial guidance and oversight over internal and external distribution of financial information, particularly related to the *Federal Managers' Financial Integrity Act of 1982* (FMFIA).
- Clear and complete authority and responsibility for all financial accounting policy, processes, and control functions vests with the Coast Guard Chief Financial Officer (CFO).
- Financial management oversight functions, complete with an organizational chart, job descriptions, roles and responsibilities, and skill sets required, are defined.
- The financial management infrastructure is appropriately staffed with experienced financial managers and staff, to expeditiously identify and address control weaknesses, and develop and implement effective policies, procedures, and internal controls to ensure that data supporting financial statement assertions are complete and accurate.
- The objectives of sound fiscal management, as defined by various government sources, described in the criteria section below, are embraced by all officers and personnel of the Coast Guard.

Cause/Effect: The Coast Guard's management has acknowledged that longstanding procedural, control, personnel, and cultural issues have impeded progress toward installing an effective financial management structure. In addition, the Coast Guard's CFO must coordinate with heads of various divisions who have a role in the accounting and financial reporting processes, but who otherwise have limited exposure to financial statement audits. Further, these division heads change regularly as part of the Coast Guard military assignment and rotation polices, making it

I.1

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

difficult for the CFO to institutionalize internal controls related to financial management and reporting that are outside the CFO's direct organization. The conditions described above continue to prevent the Coast Guard and DHS from timely preparation of accurate financial information and reports and have also contributed to the conditions reported in Exhibit I-B, *Financial Reporting*, as well as other material weaknesses described in this Exhibit.

Criteria: OMB Circular No. A-123, Revised, *Management's Responsibility for Internal Control*, defines internal controls as the organization, policies, and procedures used by agencies to reasonably ensure that (i) programs achieve their intended results; (ii) resources are used consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported, and used for decision making.

FMFIA requires that agencies establish internal controls according to standards prescribed by the Comptroller General and specified in the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government (Standards)*. The GAO defines internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

The GAO *Standards* identify the control environment, as one of the five key elements of control, which emphasizes the importance of control conscientiousness in management's operating philosophy and commitment to internal control. These standards cover controls such as human capital practices, supervisory reviews, and segregation of duties, policies, procedures, and monitoring.

OMB Circular No. A-50, *Audit Follow-up*, as revised, states that corrective action taken by management on audit findings and recommendations is essential to improving the effectiveness and efficiency of Government operations. Each agency shall establish systems to assure the prompt and proper resolution and implementation of audit recommendations. These systems shall provide for a complete record of action taken on both monetary and nonmonetary findings and recommendations.

Recommendations: We recommend that the Coast Guard:

1. Initialize the CAP/FSTAR process with an assessment of the control environment (entity-level controls), develop effective corrective actions, and implement improved financial processes and systems;
2. Delegate responsibility for sound fiscal management centrally with the CFO who has full authority to implement change as needed, including new policies, procedures, controls and IT systems requirements, to have the ability, and appropriate resources for Coast Guard financial management and reporting functions;
3. Engage an expert from outside the organization to evaluate the existing financial management organizational and internal control structure. The organizational specialist should conduct an assessment of the financial management organizational structure to consider the conditions cited above. In addition, the organizational specialist should consider other conditions identified in Exhibit I-B, *Financial Reporting,* below, such as the number and type of personnel and resources needed, along with the requisite skills and abilities necessary, to provide effective guidance and oversight to program offices that are significant to financial management and reporting, and make recommendations to senior management for appropriate changes; and

I.2

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

4. Ensure that its CAP/FSTAR actions as designed and performed are:
   a) Effective in addressing all of the material weakness described in this Exhibit; and
   b) Coordinated and prioritized with the input from Departments CFO to address matters that are preventing the Department from preparing reliable financial statements and executing its fiscal management responsibilities.

I-B Financial Reporting

Background: In FY 2006, we reported that the Coast Guard had numerous internal control weaknesses that led to a material weakness in financial reporting. While the Coast Guard developed FSTAR to address the control weaknesses, they were not able to make substantial progress in execution of their corrective actions, and, consequently, many of the conditions reported in prior years are repeated below.

Conditions: 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 are significantly noncompliant with the requirements of the *Federal Financial Management Improvement Act* (FFMIA). Specifically:
  - The general ledgers are not compliant with the United States Standard General Ledger (USSGL) at the transaction level, include noncompliant chart of account definitions, invalid accounts, improper posting logic codes and inconsistent crosswalks to the Coast Guard *Treasury Information Executive Repository* (TIER) database. The general ledgers also have static balances related to a legacy general ledger conversion and unsubstantiated automated changes to CAS financial data through the use of hundreds of scripts, implemented without effective controls to correct system problems;
  - The Coast Guard's TIER submissions to the Department's Office of Financial Management (OFM) are from a database that does not have detail at the transactional level, and is not reconciled or supported by the transaction level detail in the Coast Guard's three general ledgers; and
  - The financial reporting process is overly complex and labor intensive, and requires a significant number of "on-top" adjustments (adjustments made outside the core accounting system for presentation of financial information given to the Department for consolidation). These topside adjustments are not supported at the transaction level and are not recorded to the respective general ledgers at a detailed transactional level. Thus, period-end and opening balances are only supported by the Coast Guard TIER database, and the three general ledgers do not support the financial statements.
- Has significant deficiencies in its policies, procedures, and controls surrounding its financial reporting process. For example, the Coast Guard does not have
  - Effective procedures to support beginning balance, year-end close out and the cumulative results of operation analysis;
  - A process to record all financial transactions, in detail at the transactional level, to the general ledger systems;

I.3

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

- Effective policies and procedures to identify the cause and resolve abnormal balances and account relationship discrepancies, e.g., budgetary to proprietary reconciliations, and identified potential errors in its financial data;
- Effective procedures and internal controls over the process of preparing and reviewing adjustments to account balances, and financial statement disclosures, and uses high-level analytical comparisons to identify adjusting entries;
- Effective procedures to assess potential financial system problems, such as potential posting logic errors and automated changes to financial data through scripts (system modifications);
- Fully effective and accurate reporting tools for financial data analysis (Facts & Figures Quick Report Tool);
- An effective process to record, review, and monitor accounts receivable activity;
- Effective policies, procedures, and internal controls to compile, support, review, and report financial statement disclosures submitted for incorporation in the DHS financial statements, to include the effective completion the GAO Disclosure Checklist and valid support for the preparation of statement of net cost disclosure; and
- A validated, comprehensive process, to include effective internal controls, to fully track and reconcile intragovernmental transactions with its Federal trading partners, especially those outside DHS, and to determine that Coast Guard intragovernmental balances, as reported in the DHS financial statements, are complete, accurate, appropriately valued, belong to Coast Guard, and presented properly in the financial statements.

Cause/Effect: Many of the issues mentioned above stem from the conditions described in Exhibit I-A *Financial Management and Entity-Level Controls.* At the Coast Guard, the accuracy of financial information is highly dependent on the knowledge and experience of a limited number of key financial personnel rather than on clearly documented procedural manuals and process-flow documentation. In addition, the Coast Guard has serious general ledger structural and IT system functionality deficiencies that make the financial reporting process more complex and difficult. Consequently, the Coast Guard can not be reasonably certain that its financial statements are complete or accurate at any time. In its annual Assurance Statement provided to the DHS Secretary in September 2007, the Coast Guard was unable to provide reasonable assurance that internal controls over financial reporting are operating effectively, and was unable to represent to us that any significant balance sheet line items are fairly stated at September 30, 2007.

Criteria: FFMIA Section 803(a) requires that Federal financial management systems comply with (1) Federal accounting standards, (2) Federal system requirements, and (3) the 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.

FMFIA requires that agencies establish internal controls according to standards prescribed by the Comptroller General and specified in the GAO *Standards*. These standards define internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

I.4

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

The GAO *Standards* require that internal controls be documented in management directives, administrative policies or operating manuals; transactions and other significant events be clearly documented; and information be recorded and communicated timely with those who need it within a timeframe that enables them to carry out their internal control procedures and other responsibilities.

Recommendations: We recommend that the Coast Guard:

1. Conduct an assessment of its current financial reporting process, including a review of its three general ledger systems, with the goal of establishing a general ledger that is FFMIA compliant at the transaction level, e.g., all financial transactions are recorded in the general ledger at the detail USSGL level as they occur, all financial statement line items are fully reconciled and supported by transactional detail contained in the general and subsidiary ledgers, reducing complexity, implementing appropriate internal controls, improving financial systems integration and automating manual processes;
2. 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) On-top adjustments to account balances and abnormal balances and account relationship discrepancies, e.g., budgetary to proprietary reconciliations are identified, reviewed and documented;
   c) Account reconciliations, for each of the three general ledgers and the monthly TIER submission, are performed timely and completely each month, and differences are researched and resolved before the next month's reporting cycle. Reconciliations should include all funds maintained by the Coast Guard, including revolving, special, and trust funds;
   d) The Coast Guard identifies all accounts receivables and then implements comprehensive Coast Guard-wide policies and procedures, including internal controls, at a sufficient level of detail to determine that the accounts receivable process is effective to support management assertions, in compliance with generally accepted accounting principles, for the accounts receivable balance reported on the Coast Guard balance sheet; and
   e) The Coast Guard develops and implements effective policies, procedures and internal controls to compile, support, review, and report financial statement disclosures submitted for incorporation in the DHS financial statements, to include the effective completion the GAO Disclosure Checklist and valid support for the preparation of statement of net cost disclosure;
3. Investigate potential financial system problems such as potential posting logic errors and automated changes to financial data through scripts (system modifications); and
4. Establish a formal documented review and approval process over reconciliation activities performed by Coast Guard to ensure that all intragovernmental activity and balances are identified and differences are being resolved in a timely manner in coordination with the OFM (see Exhibit II-B, *Financial Reporting*). Procedures should also include obtaining positive confirmation of balances with DHS trading partners and make appropriate system

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

changes to include updating and validating the information in the vendor tables for trading partner data, and correct known errors.

I-C Financial Systems Security

Background: The Coast Guard maintains three general ledger systems that support its financial statements and other financial data provided to DHS OFM for consolidation, which are CAS, ALMIS, and NESSS – described in Exhibit I-B, *Financial Reporting*. Our audit included a review of the Coast Guard's IT general control (ITGC), and specifically in six key control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. During FY 2007, the Coast Guard took actions to improve aspects of its ITGC to address our prior year findings; however, the Coast Guard did not make all of the necessary improvements that they had planned to make during the year. The Coast Guard also serves as Transportation Security Administration's (TSA)'s accounting service provider; therefore, some financial accounting system and process weaknesses at the Coast Guard may affect the TSA's accounting records, as well.

Conditions: During our 2007 ITGC testing, we identified 42 findings, of which 36 are repeat findings and 6 are new findings. The ITGC and other financial system control weaknesses were identified at Coast Guard Headquarters and its components. We noted control deficiencies in all six general control areas that when combined, present more than a remote possibility of materially impacting financial data integrity. The significant deficiencies identified included: 1) excessive access to key Coast Guard financial applications, 2) application change control processes that are not adequately designed nor operating effectively, 3) entity-wide security program issues involving personnel background checks, 4) system software weaknesses involving patch management and configuration management, 5) segregation of duties involving lack of policies and procedures and excessive privilege access issues, and 6) service continuity issues involving the lack of testing of disaster recovery testing. Significant deficiency Nos. 1 and 2, above, are considered to be material weaknesses impacting the DHS consolidated financial statements. In addition, the significant deficiencies in application change control processes are among the principle causes of Coast Guard's inability to support their financial statement balances. See Exhibit I-B, *Financial Reporting,* for a discussion of the related conditions causing significant noncompliance with the requirements of FFMIA. Our ITGC findings are described in greater detail in a separate *Limited Official Use* (LOU) letter provided to the Coast Guard and DHS management.

Cause/Effect: The Coast Guard has made some progress correcting certain ITGC weaknesses identified in previous years. However, the Coast Guard was not able to effectively prioritize and implement CAPs to remediate the root cause of the ITGC weaknesses in 2007. Consequently, the corrective actions taken more often address the symptom of the problem and not the root cause. For example, workarounds are sometimes implemented so that the system can continue functioning, while more permanent solutions are developed.

Many of these weaknesses were inherited from system development activities that did not incorporate strong security controls during the initial implementation of the system more than five years ago, and will take several years to fully address. These weaknesses exist both in the documentation of processes and the implementation of adequate security controls over processes and within financial systems. Specifically, policies and procedures supporting the operation of various processes within control areas such as change control and access controls were developed without taking into account required security practices. Consequently, as policies and procedures

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

are updated, many Coast Guard components are challenged to move away from previous methodologies and fully implement and enforce these new controls in unison with other components.

The effect of these ITGC weaknesses limits Coast Guard's ability to ensure that critical financial data is reliable and is maintained in a manner to ensure confidentiality, integrity, and availability. In addition, as a result of the presence of IT weaknesses, there is added dependency on the other mitigating manual controls to be operating effectively at all times. Because mitigating controls often require more human involvement, there is an increased risk of human error that could materially affect the financial statements.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with National Institute of Standards and Technology (NIST) guidance.

OMB Circular No. A-130, *Management of Federal Information Resources,* describe specific essential criteria for maintaining effective general IT controls.

FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is 1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government, 2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities, 3) increase the accountability and credibility of federal financial management, 4) improve performance, productivity and efficiency of Federal Government financial management, and 5) establish financial management systems to support controlling the cost of Federal Government.

OMB Circular No. A-123 states, "Agency managers should continuously monitor and improve the effectiveness of internal control associated with their programs." This continuous monitoring, and other periodic evaluations, should provide the basis for the agency head's annual assessment of and report on internal control, as required by FMFIA. This Circular indicates that "control weaknesses at a service organization could have a material impact on the controls of the customer organization. Therefore, management of cross-servicing agencies will need to provide an annual assurance statement to its customer agencies in advance to allow its customer agencies to rely upon that assurance statement. Management of cross-servicing agencies shall test the controls over the activities for which it performs for others on a yearly basis. These controls shall be highlighted in management's annual assurance statement that is provided to its customers (e.g., TSA). Cross-servicing and customer agencies will need to coordinate the timing of the assurance statements."

DHS' *Sensitive Systems Policy, 4300A*, documents policies and procedures adopted by DHS intended to improve the security and operation of all DHS IT systems including the Coast Guard IT systems.

The GAO's *Federal Information System Controls Audit Manual* (FISCAM) provides a framework and recommended audit procedures that are used to conduct the IT general control test work.

Recommendations: We recommend that the DHS Office of Chief Information Officer in coordination with the Office of the Chief Financial Officer (OCFO) make the following improvements to the Coast Guard's financial management systems:

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

1. Implement the recommendations in our LOU letter provided to the Coast Guard and DHS management, to effectively address the deficiencies identified including: 1) access to key Coast Guard financial applications, 2) application change control processes, 3) entity-wide security program issues, 4) system software weaknesses involving patch management and configuration management, 5) segregation of duties involving lack of policies and procedures and excessive privilege access issues, and 6) service continuity issues involving the lack of testing of disaster recovery;
2. Design and implement plan of action and milestones that address the root cause of the weakness, to migrate away from excessive workarounds and reliance on manual mitigating controls; and
3. Develop and implement policies and procedures that appropriately consider required security practices when supporting the operation of various processes within control areas such as change control and access controls.

I-D Fund Balance with Treasury

Background: In fiscal year 2006, we reported the existence of a material weakness in Fund Balance with Treasury (FBwT) at the Coast Guard. The Coast Guard has not yet developed or implemented comprehensive FBwT CAPs, and consequently, we are repeating and expanding the conditions cited in last year's report. FBwT at the Coast Guard totaled approximately $5 billion, or approximately 10 percent of total DHS FBwT, at September 30, 2007. The majority of these funds represented appropriated amounts that were obligated, but not yet disbursed, at September 30, 2007.

Conditions: The Coast Guard:

- Did not maintain adequate supporting documentation that validated the accuracy of all of its FBwT reconciliations and the clearing of suspense items, to include posting unsupported adjustments to the Coast Guard reported general ledger activity submitted to the Treasury, and to agree Coast Guard balances to Treasury records without supporting documentation.
- Did not have an effective process for accounting for suspense account transactions related to FBwT. The Coast Guard lacks documented and effective policies and procedures, to include internal controls, to support the completeness, existence, and accuracy of recorded and subsequently posted suspense account transactions. The Coast Guard continues to be unable to produce complete and accurate populations of suspense transactions.
- Was unable to provide validated military and civilian payroll data to support payroll transactions processed through the Coast Guard's FBwT, USSGL account No. 1010. The Coast Guard did not properly report and reconcile these transactions or maintain appropriate supporting documentation.

Cause/Effect: The Coast Guard has not designed and implemented accounting processes, including a financial system that complies with federal financial system requirements, as defined in OMB Circular No. A-127 and the requirements of the *Joint Financial Management Improvement Program* (JFMIP), now administered by the *Financial Systems Integration Office* (FSIO), to fully support the fiscal year 2007 FBwT activity and balance at September 30, 2007. Failure to implement timely and effective reconciliation processes could increase the risk of fraud, abuse, undetected violations of appropriation laws, including instances of undiscovered

I.8

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

Anti-deficiency Act violations, and mismanagement of funds, which could lead to inaccurate financial reporting and affects DHS' ability to effectively monitor its budget status.

Criteria: The *Treasury Financial Manual* (TFM) states, "Federal agencies must reconcile their USSGL account No.1010, and any related subaccounts, on a monthly basis (at minimum). Federal agencies must research and resolve differences between the balances reported on their general ledger FBwT accounts and balances reported in the *Government-wide Accounting* system (GWA). In addition, Section 803(a) of FFMIA requires that Federal financial management systems comply with 1) Federal accounting standards, 2) Federal system requirements, and 3) the 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.

According to OMB Circular No. A-123, transactions should be promptly recorded, and properly classified and accounted for, in order to prepare timely and reliable financial and other reports. Documentation for transactions, management controls, and other significant events must be clear and readily available for examination.

Recommendations: We recommend that the Coast Guard:

1. Establish policies, procedures, and internal controls, including effective reconciliations and the use of a financial system that complies with federal financial system requirements, as defined in OMB Circular A-127, and the requirements of the JFMIP, to fully support the fiscal year 2007 FBwT activity and balance at September 30, 2007. These policies and procedures should allow the Coast Guard to:

   a) Perform complete and timely FBwT reconciliations using the tools provided by Treasury GWA;

   b) Better manage its suspense accounts to include researching and clearing items carried in suspense clearing accounts in a timely manner during the year, and maintaining documentation of periodic reconciliations of FBwT; and

   c) Ensure payroll data, supporting payroll transactions processed through FBwT (account 1010), is properly maintained and available for audit testwork, as needed.

I-E Capital Assets and Supplies

Background: Property, plant, and equipment (PP&E) represents approximately 15.5 percent of total DHS assets, and the Coast Guard maintains more than 60 percent of all DHS 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. Comprehensive policies and procedures are necessary to accurately and timely account for and report these assets. We reported in prior years that the Coast Guard has been unable to provide auditable documentation for certain categories of PP&E, due to a number of policy, control, and process deficiencies that will require several years to correct, and consequently, most of the conditions cited below have been repeated from our 2006 report, and have existed since the Department's inception in 2003.

Operating Materials and Supplies (OM&S) are maintained by the Coast Guard in significant quantities, and consist of tangible personal property to be consumed in normal operations to service marine equipment, aircraft, and other operating equipment. The majority of the Coast Guard's OM&S is physically located at either two Inventory Control Points (ICPs) or in the field.

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

The Coast Guard's policy requires regularly scheduled physical counts of OM&S, which are important to the proper valuation of OM&S and its safekeeping. The conditions cited below for OM&S are based on findings reported in fiscal 2006, updated as necessary to reflect the conditions noted in fiscal year 2007.

Conditions: Coast Guard has not:

Regarding PP&E:

- Consistently applied policies and procedures to ensure appropriate documentation supporting PP&E acquisitions, and their existence, is maintained to support capitalized PP&E. In cases where original acquisition documentation has not been maintained, the Coast Guard has not developed and documented methodologies and assumptions to support the value of PP&E.
- Implemented appropriate controls and related processes to accurately, consistently, and timely record additions to PP&E and construction in process (CIP), transfers from other agencies, disposals in its fixed asset system, and 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 asset system.
- Properly accounted for some improvements and impairments to buildings and structures, capital leases, and selected useful lives for depreciation purposes, consistent with GAAP.

Regarding OM&S:

- Implemented policies, procedures, and internal controls to support the completeness, accuracy, existence, valuation, ownership, and presentation assertions related to the fiscal year 2007 OM&S and related account balances.
- Fully designed and implemented policies, procedures, and internal controls over physical counts of OM&S to remediate conditions identified in previous years.
- Properly identified (bar-coded or tagged) recorded OM&S.
- Established processes and controls to fully support the calculated value of certain types of OM&S to approximate historical cost.

Cause/Effect: PP&E policies and procedures are not appropriately designed, consistently followed, or do not include sufficient controls to ensure compliance with policy or to ensure complete supporting documentation is maintained and available for audit testwork. The fixed asset module of the Coast Guard's CAS is not updated for effective tracking and reporting of PP&E. The effect of these conditions is that the Coast Guard is unable to accurately account for its PP&E, and provide necessary information to DHS OFM for consolidated financial statement purposes.

Coast Guard management deferred correction of most OM&S weaknesses reported in previous years, and acknowledged that the conditions we reported in prior years remained throughout fiscal year 2007. Lack of comprehensive and effective policies and controls over the performance of physical counts, and appropriate support for valuation, may result in errors in the physical inventory process or inventory discrepancies that could result in financial statement misstatements.

I.10

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

Criteria: Statement of Federal Financial Accounting Standard (SFFAS) No. 6, *Accounting for Property, Plant, and Equipment*, requires that:

- PP&E is recorded at historical cost with an adjustment recorded for depreciation. In the absence of such information, estimates may be used based on a comparison of similar assets with known values or inflation-adjusted current costs; and
- PP&E accounts should be adjusted for disposals, retirements, and removal of PP&E, including associated depreciation.

According to OMB Circular No. A-123, transactions should be promptly recorded, and properly classified and accounted for, in order to prepare timely and reliable financial and other reports. Documentation for transactions, management controls, and other significant events must be clear and readily available for examination.

FFMIA Section 803(a) requires each agency to implement and maintain a system that complies substantially with Federal financial management system requirements as stipulated in OMB Circular No. A-127. That Circular requires an agency's system design "to have certain characteristics that include consistent internal controls over data entry, transaction processing, and reporting throughout the system to ensure the validity of the information."

According to GAO *Standards*, assets at risk of loss or unauthorized use should be periodically counted and compared to control records. Policies and procedures should be in place for this process. The FSIO publication, *Inventory, Supplies, and Material System Requirements,* states that "the general requirements for control of inventory, supplies and materials consist of the processes of receipt and inspection. An agency's inventory, supplies and materials system must identify the intended location of the item and track its movement from the point of initial receipt to its final destination." SFFAS No. 3, *Accounting for Inventory and Related Property*, states OM&S shall be valued on the basis of historical cost.

Recommendations: We recommend that the Coast Guard:

Regarding PP&E:

1. Improve controls and related processes and procedures to ensure that documentation supporting PP&E acquisitions, to include the CIP process and existence, including additions, transfers, and disposals, is maintained to support capitalized PP&E;
2. Implement processes and controls to record PP&E transactions accurately, consistently, and timely in the fixed asset system; record an identifying number in the fixed asset system at the time of asset purchase to facilitate identification and tracking; and ensure that the status of assets is accurately maintained in the system;
3. Revise procedures for performing physical inventories of repairable items, to include procedures for resolving differences, and reporting results, to ensure that repairable PP&E is accurately and completely classified and recorded. Support the pricing methodology used to value repairable PP&E to ensure that balances, as presented in the financial statements, approximate amortized historical cost; and
4. Review policies and procedures to account for improvements and impairments to buildings and structures, capital leases, and identify proper useful lives for depreciation purposes in accordance with GAAP.

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

Regarding OM&S:

5. Update OM&S physical count policies, procedures, and controls, and provide training to personnel responsible for conducting physical inventories, and include key elements of an effective physical inventory in the policies;
6. Consider adopting a system of bar-coding or tagging OM&S as a method of tracking usage and maintaining a perpetual inventory of OM&S on hand; and
7. Establish processes and controls to support the calculated value of OM&S to ensure accounting is consistent with GAAP.

I-F Actuarial and Other Liabilities

Background: The Coast Guard maintains pension, medical, and postemployment travel benefit programs that require actuarial computations to record related liabilities for financial reporting purposes. The Military Retirement System (MRS) is a defined benefit plan that covers both retirement pay and health care benefits for all active duty and reserve military members of the Coast Guard. The medical plan covers active duty, reservists, retirees/survivors and their dependents that are provided care at Department of Defense (DoD) medical facilities. The postemployment travel benefit program pays the cost of transportation for uniformed service members upon separation from the Coast Guard. Annually, participant and cost data is extracted by the Coast Guard from its records and provided to an actuarial firm as input for the liability calculations. The accuracy of the actuarial liability as reported in the financial statements is dependent on the accuracy and completeness of the underlying participant and cost data provided to the actuary. A combined unfunded accrued liability of approximately $30 billion for the plans is reported in the DHS consolidated balance sheet at September 30, 2007.

The Coast Guard estimates accounts payable as a percentage of undelivered orders (UDOs) based on historical trends. As described in Exhibit I-G, *Budgetary Accounting*, reliable accounting processes surrounding the recording of obligations and disbursements, and tracking of UDOs, are key to the accurate reporting of accounts payable in the Coast Guard's financial statements.

The Coast Guard's environmental liabilities consist of two main types: shore facilities and vessels. Shore facilities include any facilities or property other than ships, e.g., buildings, fuel tanks, lighthouses, small arms firing ranges (SAFRs), etc.

The Coast Guard estimates its legal liabilities to include Oil Spill Liability Trust Fund claims, that are incorporated, and recorded, as part of the DHS legal liability on DHS financial statements.

Conditions: We noted the following internal control weaknesses related to actuarial and other liabilities. The Coast Guard does not:

- Have effective policies, procedures, and controls to ensure the completeness and accuracy of participant data, medical cost data, and trend and experience data provided to, and used by, the actuary for the calculation of the MRS pension, medical, and postemployment benefit liabilities. Reconciliations between subsidiary and general ledger amounts for medical expenditures are not effective.
- Have effective policies, procedures and internal controls over the Coast Guard's process for reconciling military payroll recorded in the CAS general ledger to detail payroll records. Military personnel data changes, including changes in leave balances and payroll corrections, are not processed in the appropriate payroll and/or reporting periods, and

I.12

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

consequently impact the completeness and accuracy of leave and payroll accruals as well as data used for actuarial projections.

- Use a reliable methodology to estimate accounts payable. The method used was not supported as to the validity of data, assumptions, and criteria used to develop and subsequently validate the reliability of the estimate for financial reporting.
- Support the completeness, existence, and accuracy assertions of the data utilized in developing the estimate for the FY 2007 recorded environmental liability account balance. The Coast Guard has not fully developed, documented, and implemented the policies and procedures in developing, preparing, and recording the environmental liability estimates related to vessels, shore facilities projects, lighthouses, and SAFRs.
- Use a reliable methodology to estimate their legal liabilities, to include Oil Spill Liability Trust Fund claims that are incorporated and recorded as part of the DHS contingent legal liability on DHS consolidated financial statements. The Coast Guard did implement corrective actions to support the completeness of their oil spill legal claims. However, Coast Guard policies, procedures, and internal controls were not fully effective to accurately estimate liabilities for oil spill claims.

Cause/Effect: Much of the data required by the actuary comes from personnel and payroll systems that are outside of the Coast Guard's accounting organization and are instead managed by Coast Guard's Personnel Service Center (PSC). The PSC has not substantiated the completeness and accuracy of the basic pay information provided to the actuary. Consequently, the Coast Guard management is unable to provide assurance on the completeness and accuracy of actuarially determined liabilities as stated in the DHS consolidated balance sheet at September 30, 2007. In addition, the Coast Guard does not have sufficient controls to prevent overpayments for medical services, and inaccurate medical costs submitted to the Coast Guard actuary could result in a misstatement of the actuarial medical liability and related expenses. Also, the conditions noted exist, in part, because of ineffective entity-level controls, in particular, with regard to financial management oversight – see Exhibit I-A, *Financial Management and Entity Level Controls.*

The Coast Guard has not yet developed comprehensive policies and procedures or corrective action plans to address the conditions above, and consequently, management is unable to assert to the accuracy and completeness of accounts payable, and payroll accruals recorded as of September 30, 2007.

The Coast Guard has not developed consistent, written, agency-wide policies to define the technical approach, cost estimation methodology, and overall financial management oversight of its oil spill claims and environmental remediation projects, resulting in the inability to support the completeness of the estimate and possible misstatement of the liability in its financial statements.

Criteria: According to SFFAS No. 5, *Accounting for Liabilities of the Federal Government*, paragraph 95, the employer should recognize an expense and a liability for other postemployment benefits (OPEB) when a future outflow or other sacrifice of resources is probable and measurable on the basis of events occurring on or before the reporting date. Further, the long-term OPEB liability should be measured at the present value of future payments, which requires the employer to estimate the amount and timing of future payments, and to discount the future outflow over the period for which the payments are to be made.

GAO *Standards* hold that transactions should be properly authorized, documented, and recorded accurately and timely. OMB Circular No. A-123 states that "transactions should be promptly recorded, properly classified, and accounted for in order to prepare timely accounts and reliable

I.13

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

financial and other reports." SFFAS No. 1, *Accounting for Selected Assets and Liabilities*, states, "When an entity accepts title to goods, whether the goods are delivered or in transit, the entity should recognize a liability for the unpaid amount of the goods. If invoices for those goods are not available when financial statements are prepared, the amounts owed should be estimated."

Statement on Auditing Standards (SAS) No. 57, *Auditing Accounting Estimates,* states "An entity's internal control may reduce the likelihood of material misstatements of accounting estimates. Specific relevant aspects of internal control include the following: Accumulation of relevant, sufficient, and reliable data on which to base an accounting estimate, and comparison of prior accounting estimates with subsequent results to assess the reliability of the process used to develop estimates."

Federal Accounting Standards Advisory Board (FASAB) Technical Release No. 2, *Determining Probable and Reasonably Estimable for Environmental Liabilities in the Federal Government*, states that an agency is required to recognize a liability for environmental cleanup costs as a result of past transactions or events when a future outflow or other sacrifice of resources is probable and reasonably estimable. Probable is related to whether a future outflow will be required. Reasonably estimable relates to the ability to reliably quantify in monetary terms the outflow of resources that will be required.

Recommendations: We recommend that the Coast Guard:

Regarding actuarial liabilities:

1. Establish and document policies, procedures, and effective controls to ensure the completeness and accuracy of the actuarial pension, medical, and postemployment travel benefit liabilities;
2. Establish and document policies, procedures, and effective controls to ensure the completeness and accuracy of participant data, medical cost data, and trend and experience data provided to, and used by, the actuary for the calculation of the MRS pension, medical, and postemployment travel benefit liabilities; and
3. Perform a periodic reconciliation between the medical expenditures recorded in the subsidiary ledger and those recorded in the CAS, and address differences before data is provided to the actuary. This reconciliation should be performed for all significant sources of medical actuarial data, including TriCare, and DoD Military Treatment Facilities (MTFs). In addition, this reconciliation should be reviewed by someone other than the preparer to ensure accuracy.

Regarding accounts payable and payroll:

4. Analyze and make appropriate improvements to the methodology used to estimate accounts payable and support all assumptions and criteria with appropriate documentation to develop and subsequently validate the estimate for financial reporting; and
5. Implement corrective action, including appropriately designed and implemented internal controls, to support the completeness, existence, and accuracy of changes in member personnel data records and military payroll transactions, and to include recorded accrued military leave and payroll liabilities.

I.14

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

Regarding environmental liabilities:

6. Develop consistent written agency-wide policies, procedures, processes, and controls to ensure identification of and recording of all environmental liabilities, define the technical approach, cost estimation methodology, and overall financial management oversight of its environmental remediation projects. The policies should include:

   a) Procedures to 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;

   b) Periodically validate estimates against historical costs; and

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

Regarding legal liabilities:

7. Develop, document, and implement a reliable methodology as well as formal policies and procedures, to include internal controls, to verify and support the accuracy of the legal liability estimate and related disclosures.

I-G 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 Treasury guidance. The Coast Guard has over 80 TAFS covering a broad spectrum of budget authority, including annual, multiyear, and no-year appropriations; and several revolving, special, and trust funds. In addition, the Coast Guard estimates accounts payable at year end as a percentage of UDOs based on historical trends. Reliable accounting processes surrounding obligations, UDOs and disbursements are key to the accurate reporting of accounts payable in the DHS consolidated financial statements.

Conditions: We noted the following internal control weaknesses related to budgetary accounting, many of which were repeated from our fiscal year 2006 report.

- The policies, procedures and internal controls over the Coast Guard's process for validation and verification of UDO balances are not effective to ensure that recorded obligations and UDO balances were complete, valid, accurate, and that proper approvals and supporting documentation is maintained.

- Policies were not fully implemented to ensure that contract awards, particularly related to the Deepwater Acquisition Program, were recorded in the general ledger in a timely manner, and as a result, obligations might have been temporarily understated.

- Procedures and controls are not implemented to prevent incurring a commitment/obligation in excess of established targets so that funds are not obligated in excess of the apportioned and allotted amounts. In addition, the Coast Guard did not effectively monitor unobligated commitment activity in its procurement system. As of April 2007, there were over 16,000 unobligated commitment transactions totaling approximately $516 million.

- The Coast Guard's procedures, processes, and internal controls in place to verify the completeness and accuracy of the year-end obligation pipeline adjustment to record all executed obligations were not properly designed and implemented. These deficiencies

I.15

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

affected the completeness, existence, and accuracy of the year-end "pipeline" adjustment that was made to record obligations executed before year end.

- Automated system controls are not effectively used to prevent the processing of procurement transactions by contracting officer's with expired warrant authority, and a manual compensating control was not effective since listings of warranted contracting officers were not complete.

Cause/Effect: Several of the Coast Guard's budgetary control weaknesses can be corrected by modifications or improvements to the financial accounting system, process improvements, and strengthened policies and internal controls. Weak controls in budgetary accounting, and associated contracting practices increase the risk that the Coast Guard could violate the *Anti-deficiency Act* and overspend its budget authority. The financial statements are also at greater risk of misstatement. The untimely release of commitments may prevent funds from being used timely for other purposes.

Criteria: According to the JFMIP, *Core Financial System Requirements*, an agency's core financial management system must ensure that an agency does not obligate or disburse funds in excess of those appropriated and/or authorized and specific system edits and user notifications related to funds control must be in place. The *Federal Acquisition Regulation* (FAR) Section 1.16 addresses the authorities and responsibilities granted to contracting officers. Treasury's USSGL guidance specifies the accounting entries related to budgetary transactions.

FFMIA Section 803(a) requires that each Agency to implement and maintain a system that complies substantially with Federal financial management system requirements as stipulated by OMB Circular No. A-127.

Recommendations: We recommend that the Coast Guard:

1. Improve policies, procedures, and the design and effectiveness of controls related to processing obligation transactions, including periodic review and validation of UDOs. Emphasize to all fund managers the need to perform effective reviews of open obligations, obtain proper approvals, and retain supporting documentation;
2. Fully implement policies and the design and effectiveness of controls to ensure that contract awards are recorded in the general ledger in a timely manner;
3. Improve segregation of duties for transactions related to the creation and approval of purchase requisitions, certification of funds availability, and the recording of the obligations, and record contracts timely;
4. Revise controls and related policies and procedures to periodically review commitments;
5. 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; and
6. Establish automated system controls to prevent incurring a commitment/obligation in excess of established targets so that funds are not obligated in excess of the apportioned and allotted amounts and preclude the processing of procurement transactions if the contracting officer's warrant authority had expired.

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

II-A Financial Management and Entity Level Controls (FEMA)

	2007	2006	2005
FEMA	MW	N/A	N/A
OFM	C	MW	MW
ICE	C	C	MW

Key – Trend Table

C	Corrected
SD	Significant Deficiency*
MW	Material Weakness*

* See Introduction

Background: The Federal Emergency Management Agency (FEMA)'s accounting and financial reporting requirements are very diverse supporting multifaceted operations, such as temporary assistance funds, disaster relief loans, national flood insurance programs, stockpiles of essential supplies, mission assignments to other federal agencies for restoration and reconstruction, and grants to state and local governments. These programs are sometimes subject to complicated accounting rules, as defined by the *Federal Accounting Standards Advisory Board* (FASAB), and require specialized technical knowledge to interpret and apply. FEMA has been subject to significant reorganization efforts during FY 2007 and FY 2006, while also continuing its disaster relief efforts resulting from the 2005 hurricanes affecting the Southern U.S. In addition, FEMA's accounting personnel and systems need to be ready to mobilize and support disaster operations with little advance notice, while also maintaining sound financial management standards. These circumstances place a high demand on financial management and emphasize the need for strong entity level controls throughout FEMA. Some of the conditions cited below contributed to qualifications of our Independent Auditors' Report in previous years. We believe these conditions, which include financial reporting control weaknesses, considered in aggregate, now represent a material weakness in financial management and entity level controls at FEMA.

Until 2007, the DHS OFM, within the OCFO at DHS Headquarters has not been adequately staffed with a sufficient number of management personnel who had the requisite financial accounting background, knowledge, and expertise, to both (i) set up, and (ii) effectively manage the consolidated financial reporting and internal control infrastructure of a large and complex Executive Branch agency. However, late in FY 2006 and throughout 2007, the OCFO executed a staffing plan to fill gaps in OFM skill sets. With the addition of new financial management and staff, restructuring of the OFM, development and issuance of new policies and procedures, and improved internal controls, with a focus on entity level controls, we noted that OFM has fully corrected its material weakness in *Financial Management and Entity Level Controls* reported in our FY 2006 report.

In 2006, we reported that ICE corrected its entity level control weaknesses in financial management and oversight. The corrective actions taken in 2006 continued to be effective in FY 2007.

Conditions: We noted the following internal control weaknesses related to financial management and entity level controls at FEMA, when combined with the conditions existing at the Coast Guard (see Exhibit I-A, *Financial Management and Entity Level Controls*), rise to a material weakness at the DHS consolidated financial statement level.

FEMA:

- Has not established a financial management organizational structure, with clear oversight and supervisory review functions that supports the development and implementation of effective policies, procedures, and internal controls over financial reporting, to ensure that accounting principles are correctly applied and accurate financial data is submitted to OFM for consolidation in a timely manner. For example, we noted:

II. 1

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

- The FEMA CFO does not have clearly defined and complete authority and responsibility for all financial accounting policy, processes, and control functions throughout the agency;
- Financial management oversight functions have not been clearly defined, complete with an organizational chart, job descriptions, roles and responsibilities, training requirements, and skill sets required;
- A lack of segregation of duties in financial reporting roles; and
- A lack of supervisory review in financial functions, especially over complex, nonroutine accounting estimates and adjustments, such as credit reform subsidies.

- Does not have a sufficient number of experienced financial managers and staff to expeditiously address nonroutine accounting issues. A lack of skilled accounting resources has contributed to FEMA's inability to perform important accounting functions timely. For example, we noted that FEMA did not:
  - Fully integrate certain Grants and Training (G&T) accounting processes;
  - Perform necessary procedures to completely and accurately present stockpile inventory balances in the consolidated financial statements;
  - Reevaluate the reasonableness of its allowance rates for disaster relief accounts receivable; and
  - Prepare and record adjustments for its National Flood Insurance Program accurately or timely. A material error was identified after submission of FEMA's year-end financial information to OFM.
- Has not completed and implemented a comprehensive CAP to correct internal control weaknesses that are contributing to Department-level material weaknesses, as required by OMB Circular No. A-50, *Audit Follow-up*, as revised.
- Has not documented and/or updated formal policies and procedures (including desk manuals) for many of the roles, responsibilities, processes, and functions performed within FEMA. For example, in FY 2007, we noted that improvements are needed in the formal documentation of policies and procedures related to *Anti-deficiency Act* compliance, preparation and review of the quarterly and annual financial statements; identification of and adherence to GAAP and OMB statements and guidance; policies for timely de-obligation of outstanding grant and non-grant obligations that should be closed related to the former G&T office; policies for monitoring and responding to OMB Circular No. A-133 reports, Office of Inspector General (OIG) reports, and GAO report findings and recommendations; and the quarterly process for estimating accruals (including accrual validation).
- Has not completed the placement of sufficient financial and accounting resources in its regional offices, which contributes to certain issues in Mission Assignment accounting. For example, Mission Assignment obligations are not closed out timely, and in a sample of 216 Mission Assignment payments selected for testwork, we noted that approximately 10% of the payments were not properly reviewed and approved in accordance with FEMA policy.

Cause/Effect: FEMA maintains a relatively small headquarters infrastructure and accounting staff, compared to its diverse programmatic and mission focused objectives. In addition, FEMA is dependent on timely information from other federal agencies, state governments, and grantees

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

to account for some transactions. FEMA's evaluation of internal control over financial reporting conducted pursuant to OMB Circular No. 123, *Managements Responsibility for Internal Control*, and representations made to the Secretary pursuant to the *DHS Financial Accountability Act*, stated that FEMA could not provide reasonable assurance that its internal controls over financial reporting are operating effectively to achieve desired objectives during FY 2007.

Criteria: FMFIA requires that agencies establish internal controls according to standards prescribed by the Comptroller General and specified in the GAO *Standards*. The GAO defines internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The GAO *Standards* identify the control environment, as one of the five key elements of control, which emphasizes the importance of control conscientiousness in management's operating philosophy and commitment to internal control. These standards cover controls such as human capital practices, supervisory reviews, and segregation of duties, policies, procedures, and monitoring.

Recommendations: We recommend that FEMA:

a) Provide its CFO with clear authority to develop and implement accounting and financial reporting policies, procedures, and internal controls throughout the agency. Program offices should be required to adhere to policies;

b) Evaluate the existing financial management organizational and internal control structure to determine the number of personnel and resources needed, along with the requisite skills and abilities necessary, to ensure that all significant transactions and account balances are accurately and completely recorded in FEMA's general ledger in a timely manner;

c) Assign accounting functions and responsibilities to staff to ensure proper segregation of duties;

d) Establish clear management oversight responsibilities and processes to effectively review adjustments to account balances and complex, nonroutine accounting transactions;

e) Develop and implement a comprehensive CAPs to correct conditions that contribute to the Department-level material weaknesses in internal controls, and prevented FEMA management from providing reasonable assurance on the effectiveness of internal control;

f) Fully implement plans to place comptrollers in each regional office; and

g) Ensure that procedures are in place to maintain all job-related training, and other critical personnel actions.

II-B Financial Reporting (DHS-HQ, FEMA, and TSA)

	2007	2006	2005
DHS-HQ	MW	MW	MW
FEMA*	MW	N/A	MW
TSA	SD	MW	MW
ICE	C	C	MW

* FEMA Financial Reporting conditions are combined with Comment II-A in 2007

Background: DHS-HQ (or DHS Management and Operations) is comprised of various programs, reporting entities, and offices including, the OCFO. The OCFO is primarily responsible for the financial accounting and reporting infrastructure of the Department, together with other responsibilities as defined in the *Chief Financial Officers Act of 1990*, as amended by *DHS Financial Accountability Act of 2004*. DHS' OFM is responsible for preparing the *Annual Financial Report* (AFR), including the

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

consolidated financial statements, footnote and supplementary data, from trial balances and other financial data submitted by the components to OFM through the TIER system. DHS components are responsible for providing OFM complete, accurate, and timely submission of monthly financial data and reports. The DHS CFO has authority to establish accounting policy that must be followed by components when submitting data used in the DHS consolidated financial statements, and has established *Standard Operating Procedures* (SOP)s, to perform oversight and monitoring controls over financial data submitted by the components that are properly designed and effective when fully completed. During FY 2007, the OCFO issued a component guide that describes component reporting procedures and requirements, as well as other policy memoranda, and several additional DHS-wide policies are scheduled for release in 2008.

FEMA identified a material weakness in internal control over financial reporting in its FY 2007 assurance statement sent to the Secretary, in accordance with Departmental policies requiring self evaluation of internal controls pursuant to FMFIA and OMB Circular No. A-123. The financial reporting internal control weaknesses at FEMA are included in Exhibit II-A, *Financial Management and Entity Level Controls.*

The TSA began using the Coast Guard's *Core Accounting System* (CAS) for its primary general ledger in FY 2005. The transition to a new accounting system required the development and implementation of many new accounting processes and procedures, some of which were needed to mitigate material weaknesses in internal controls that existed prior to TSA's migration to CAS and that currently exist at the Coast Guard. This process of setting up a financial accounting and reporting process interfered with TSA's ability to prepare timely and accurate financial statements through 2006, and contributed to a material weakness in internal controls over financial reporting. In FY 2007, TSA developed and implemented a CAP to address its financial reporting and other accounting internal control weaknesses. TSA has made progress toward correction of control weaknesses in financial reporting in FY 2007.

In 2006, we reported that ICE corrected its internal control weaknesses over financial reporting. The corrective actions taken in 2006 continued to be effective in FY 2007.

Conditions: We noted the following internal control weaknesses related to financial reporting at DHS-HQ and TSA:

1. DHS-HQ:

   - Has made significant progress toward the performance of responsibilities related to the consolidated financial reporting at DHS, however additional improvements are needed to fully implement a consolidated financial reporting process. This condition is supported, in part by these observations:

     - As part of the Post-Katrina reorganization, the Office of Health Affairs (OHA) was established. The accounting, reporting, and data gathering responsibilities for the new entity, including a new reporting requirement affecting the presentation of a transfer appropriation account and related activity conducted by another Federal agency and reimbursed by OHA, were not clearly established and delegated in time to be effective during the year. OHA does not have the administrative infrastructure in place to facilitate (i.e., user controls) financial reporting functions provided by its service provider (i.e., service provider controls) which changed during FY 2007. Consequently, DHS management was unable to support its implementation of a new reporting requirement of OMB Bulletin No. A-136, *Financial Reporting Requirements*, affecting the accounting and presentation of budgetary allocation transfers that occurred at OHA, and was unable to represent that the balance sheet of

II. 4

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

OHA is fairly stated in conformity with U.S. generally accepted accounting principles at September 30, 2007. Specifically, OHA did not obtain assurance that $1.4 billion of fund balance with Treasury and undelivered orders recorded as result of a budget allocation to another Federal agency, was properly stated at September 30, 2007. The total assets of OHA, as reported in the accompanying DHS balance sheet as of September 30, 2007, were $3.2 billion or 4 percent of total DHS consolidated assets.

- DHS was not able to timely or completely reconcile intragovernmental balances with other Federal entities, particularly the Department of Defense. Consequently, the DHS' *Material Difference/Status of Disposition Certification Report*, submitted to the Treasury for September 30, 2007, showed material differences attributable to accounting/reporting errors in excess of $1.5 billion FEMA, Coast Guard, TSA and CBP are DHS components that have significant intragovernmental transactions throughout the year. These conditions also impacted DHS' ability to accurately report transactions with Federal government trading partners in the financial statements as required; and

- Instances were noted where DHS components routinely provided OFM incomplete or inaccurate information, and/or did not respond timely to OFM' inquires. Consequently, OFM was often unable to fully complete its own procedures for timely review of component financial data and, therefore, are unable to resolve potential errors before the financial statements were prepared.

• Has not fully implemented recently issued policies, and we noted weaknesses in the operating effectiveness of the following established policies:

  - Beginning of the year balance reconciliations that ensure opening balances agree to the prior year ending balances. These weaknesses resulted in several material errors in the financial statements that were not identified by OFM, until questioned during our audit;

  - Interim financial statement preparation and support. During our review of the June 30, 2007, draft financial statements, we noted some errors and discrepancies that were not corrected prior to submission to the auditor. In some cases, we noted that erroneous entries were recorded to correct out-of-balance conditions in data submitted by components, without support or follow-up, and resolution with the component; and

  - Computation of abnormal or unusual account balances, including proprietary to budgetary account relationship analysis performed at the consolidated level. Currently, there is still a reliance on the external auditor to identify potential errors through proprietary to budgetary reconciliations, and refer the differences to components and OFM for investigation and resolution. Although upgrades to the existing analytical tools have been developed by OFM, they are not yet being fully utilized, with full implementation scheduled for FY 2008.

• Did not always perform key supervisory and monitoring control procedures over work prepared by accounting staff during the year. In some cases, we noted that supervisory reviews were performed and documented on incomplete information, without evidence of closure on open issues. Some reviews were not effective, e.g., did not identify material errors in the financial data. For example, some top-side (manual) adjustments to financial statements, and fluctuation and variance analysis, were not always reviewed and approved by a supervisor. In some cases, we noted that these manual adjustments also created misstatements of the financial statement balances, which were identified during our audit.

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

- Has not established Strategic Goals and the financial information systems or sufficiently documented processes to accumulate cost data by DHS strategic goal when the goals are established, as required by SFFAS No. 4, *Managerial Cost Accounting Concepts and Standards*, and does not have a current strategic plan, as required by the *Government Performance and Results Act* (GPRA) (see Exhibit III-N).

2. TSA has improved its financial reporting process in FY 2007. While TSA has made progress in addressing the conditions we identified and reported in 2006, its financial reporting CAP has not been fully implemented by the end of FY 2007. We noted that TSA:

   - Made a number of restatements to its prior year financial statements, primarily as a result prior-year data that was not previously reconciled to its general ledger.
   - Did not have certain policies and procedures in place all fiscal year.
   - Required numerous other on-top adjustments to properly close and report its monthly and annual financial results, did not consistently reverse all on-top adjustments that required reversal, and did not record all on-top adjustments properly.
   - Required significant additional human resources, to perform its year-end general ledger close, prepare financial statements, and respond to audit inquiries in a timely manner.

Cause/Effect: The OCFO adopted CAPs to address the conditions cited above; however, we continue to report that the OCFO has a material weakness in financial reporting, primarily because the OCFO has not yet fully implemented policies designed to ensure timely, accurate, and complete periodic reporting throughout the year, and developed tools to ensure that component agencies routinely respond to inquiries and actively investigate and resolve potential accounting and reporting errors in a timely manner. In some cases, newly designed centralized policies and procedures, together with effective internal controls over financial reporting, have not been fully implemented as of September 30, 2007. In addition, challenges remain in obtaining consistently complete and accurate data from DHS components, affecting OFM's ability to completely perform its responsibilities in a timely manner.

Intragovernmental out-of-balances exist in many Federal agencies and DHS is dependent on other Federal agencies maintaining accurate account balances in order to fully reconcile its balances. No government-wide system currently exists to allow for this reconciliation to be done independently by DHS. Although OFM undertook numerous corrective actions in FY 2007, including initiating a consolidated confirmation process, holding workshops to instruct components how to reconcile balances, assisting components in implementing procedures to support balances with external trading partners, and meeting with OMB and other agencies to directly reconcile differences, DHS was not able to fully reconcile its balances. OFM's process does demonstrate progress; for instance, it recently reconciled a $350 million difference with the Department of Defense.

TSA's CAP is a two-year plan to fully remediate the process and control weaknesses in financial reporting, which is not scheduled for completion until FY 2008. TSA invested substantial resources to reconcile its beginning balance sheet accounts, as necessary, to obtain an external audit of those accounts. FY 2007 was a "catch-up" year, intended to establish more efficient and effective accounting and financial reporting processes which will benefit FY 2008 and beyond.

Criteria: OMB Circular No. A-136, *Financial Reporting Requirements*, revised July 24, 2006, changed the financial reporting requirements for transferring, or allocating, budget authority from one entity to another within or to another Federal department (i.e., parent/child reporting). OMB Memorandum M-07-12 clarified the reporting requirements and emphasized that the two Federal

II. 6

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

departments may need to coordinate to ensure that parent's reporting and auditing requirements are met.

The *Treasury Federal Intragovernmental Transactions Accounting Policies Guide,* dated August 18, 2006, and OMB Circular No. A-136, require Federal CFO Act and non-CFO Act entities identified in the Treasury Financial Manual (TFM) 2006, Vol. I, Part 2-Chapter 4700, *Agency Reporting Requirements for the Financial Report of the United States Government,* to perform quarterly reconciliations of intragovernmental activity/balances. TFM, Section 4706, *Intragovernmental Requirements,* requires reporting agencies to reconcile and confirm intragovernmental activity and balances quarterly for specific reciprocal groupings. TFM Bulletin 2007-03 *Intragovernmental Business Rules*, also provides guidance to Federal agencies for standardizing the processing and recording of intragovernmental activities.

OMB Circular No. A-123 defines management's responsibility and provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control. Within the organizational structure, management must clearly: define areas of authority and responsibility; appropriately delegate the authority and responsibility throughout the agency; establish a suitable hierarchy for reporting; support appropriate human capital policies for hiring, training, evaluating, counseling, advancing, compensating, and disciplining personnel; and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties as well as understand the importance of maintaining effective internal control within the organization.

FMFIA requires that agencies establish internal controls according to standards prescribed by the Comptroller General and specified in the GAO *Standards.* The GAO defines internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The GAO *Standards* identify the control environment, as one of the five key elements of control, which emphasizes the importance of control conscientiousness in management's operating philosophy and commitment to internal control. These standards cover controls such as human capital practices, supervisory reviews, and segregation of duties, policies, procedures, and monitoring.

OMB Circular No. A-50 states that corrective action taken by management on audit findings and recommendations is essential to improving the effectiveness and efficiency of Government operations. Each agency shall establish systems to assure the prompt and proper resolution and implementation of audit recommendations. These systems shall provide for a complete record of action taken on both monetary and nonmonetary findings and recommendations.

Recommendations: We recommend that:

1. DHS-HQ (with OCFO and OFM):
   a) Develop a strategy to quickly provide full accounting and reporting services to newly created reporting entities. Identify a full-service accounting provider for OHA, that will address the allocation transfer accounting matters early in FY 2008, and make appropriate adjustments to the financial statements to accurately reflect activity and balances. Consider creating a permanent group within OCFO that will proactively identify and resolve accounting issues before they develop into significant problems, similar to the process used to assist US-Visit in FY 2007. When appropriate, and needed, this group should be directly involved in development and implementation of long-term accounting solutions, either within the Directorate or at an existing component;
   b) Fully implement a comprehensive proprietary to budgetary account analysis that is performed each month with TIER submissions, and require component entities to

II. 7

investigate and resolve differences in a timely manner. Monthly certifications received from component CFOs should specifically state the completion of this procedures, together with recording of correcting entries to the general ledger;

c) Direct component CFO leadership to improve communication and coordination on unique accounting and transactional matters, and to improve the accuracy of routine monthly data submissions. Problems with timeliness, completeness and accuracy of component data submissions, and/or responsiveness to OFM may need the support of the CFO to resolve;

d) In coordination with other DHS components, further develop policies, procedures and controls that will result in the timely reconciliation of intragovernmental activity and balances. Differences should be reconciled in a timely manner. This may involve setting up special arrangements with some trading partners, such as work OFM has begun with the Department of Defense. Procedures should include positive confirmation at least on a quarterly basis, all intragovernmental activity and balances with their intragovernmental trading partners, including other DHS component entities, as prescribed by Treasury guidance;

e) Continue with implementation of the financial reporting management directives scheduled for release in FY 2008. Once implemented, the policies should be tested for effectiveness, and when necessary, make improvement to addresses weaknesses identified;

f) Improve supervisory and monitoring control procedures over work prepared by accounting staff during the year, to ensure that they will reliably identify errors for correction, in a timely manner. Consider additional training for component accountants to improve the quality of submitted financial data, and for desk officers to improve the effectiveness of their initial reviews; and

g) OCFO and applicable component entities should develop financial information systems and document processes to accumulate and present cost data by DHS strategic goal, as required by SFFAS No. 4.

2. TSA:

a) Consistently adhere to policies and perform procedures for the preparation and approval of on-top adjustments for submission to its accounting services provider;

b) Develop and implement procedures to properly identify all on-top adjustments that require reversal in the subsequent period and to ensure the timely reversal of those adjustments; and

c) Once accounting and reporting processes stabilize in FY 2008, perform a financial organization and human resource needs assessment in coordination with its accounting services provider to determine the optimum number of accounting personnel and skill sets required and the most effective organizational structure to sustain efficient accounting operations. TSA's accounting operations should be designed and staffed to most efficiently support timely responses to auditor inquiries during the year, without also causing significant disruption to on-going accounting operations.

II-C Financial Systems Security

Background: Financial systems security is essential to achieving effective, reliable reporting of financial and performance data. As a part of the financial statement audit, we perform an

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

evaluation of the general controls over significant DHS financial IT systems. Effective general controls are typically defined by the GAO's FISCAM, in six key control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. In addition to general controls, financial systems contain application controls, which are the structure, policies, and procedures that apply to use, operability, interface, edit and monitoring controls of an application. We tested various application controls of key DHS financial systems as part of our IT audit test work.

The primary IT systems evaluated as a part of our audit are the component general ledger and subsidiary/feeder subledger or modules that support the financial statements and specific accounting processes such as grants, loans, excise tax receipts, etc.

During FY 2007, DHS Civilian Components took significant steps to improve their financial systems security, particularly the FISCAM general control areas entity-wide security program planning and management, and system software, which resulted in the closure of more than 30% of our prior year IT control findings.

Conditions: The FISCAM IT general control areas that continue to present a risk to financial systems security and data integrity include: 1) excessive access to key DHS financial applications; 2) application change control processes that are inappropriate in other locations not fully defined, followed, or effective; and 3) service continuity issues impacting DHS' ability to ensure that DHS financial data is available when needed. The conditions supporting our findings collectively limit DHS' ability to ensure that critical financial and operational data is kept secure and is maintained in a manner to ensure confidentiality, integrity, and availability. Our findings, including significant deficiencies that do not rise to the level of being a material weakness, are described in greater detail in a separate *Limited Official Use* letter provided to DHS management.

Regarding access controls – we noted:

- Excessive access existed within financial applications at two DHS components. Specifically, instances of generic shared accounts exist on the financial applications. These accounts have every privilege within the application, including the ability to create/delete/modify user accounts.
- Account management documentation did not exist, and user account lists were not periodically reviewed for appropriateness, resulting in inappropriate authorizations and excessive user access privileges across two DHS components.
- Accounts were not configured to disable upon personnel termination across two DHS components.
- Two DHS components had a large number of instances of inadequate or weak passwords that existed on key servers and databases that house financial data.
- Instances where workstations, servers, or network devices were configured without necessary security patches, inactivity time-outs, and proactive/appropriate vulnerability scanning not occurring.
- Audit logs were not reviewed at one DHS component, and the most restrictive security settings for the audit logging of highly privileged accounts and the protection of data sets were not enabled for a financial application at another DHS component.

II. 9

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

Regarding application software development and change control – we noted:

- Instances where changes made to the configuration of the system were not always documented or performed for test plans, test results, approvals or software modifications at two DHS components. Additionally, documented approval did not exist, or was not always retained, for emergency enhancements, "bug" fixes, and data fixes, and in some cases, audit logs for tracking changes to the data or systems were not activated.
- One DHS component had implemented a separate and secondary change control process outside of and conflicting with the established change control process. In another instance, changes were made prior to management approval. Instances where changes made to the configuration of the system were not always documented or performed through System Change Requests (SCRs), test plans, test results, approvals, or software modifications at two DHS components also existed.
- The contract that a DHS component has with the software vendor does not include security configuration requirements that must be adhered to during the configuration management process.
- Instances where policies and procedures regarding change controls were not in place to prevent users from having concurrent access to the development, test, and production environments of the system, or for restricting access to application system software and system support files.
- Policies and procedures surrounding the system development life cycle (SDLC) process have not been documented or adopted a finalized SDLC.

Regarding service continuity – we noted:

- The Continuity of Operations Plan (COOP) does not include an accurate listing of critical information technology systems, did not have critical data files and an alternate processing facility documented, and was not adequately tested for DHS one component. An alternate processing site is not operational for DHS one component.
- Backup tapes are not rotated off site or are not periodically tested. One DHS component did not have policy and procedures developed for testing of backups.
- Rules of Behavior forms are not consistently signed prior to gaining local area network (LAN) access for one DHS component.

Cause/Effect: Many of these weaknesses were inherited from the legacy agencies that came into DHS or system development activities that did not incorporate strong security controls from the outset and will take several years to fully address. A contributing cause to repeated findings is that DHS lacks an effective component-wide prioritization of IT systems issues, including the development of a stable centralized IT platform for the Department. Several attempts have been made, such as eMerge and eMerge 2, to centralize the financial IT platform; however, each has been halted or delayed. In addition, we found that focus is also placed on the tracking of response to audit recommendations, instead of on developing the most effective method of addressing the actual control weakness; and when weaknesses in controls or processes are identified, the corrective actions address the symptom of the problem and do not the correct root cause – amounting to a temporary fix.

The effect of the IT weaknesses identified during our testing impacts the reliability of DHS' financial data. Many of these weaknesses, especially those in the area of change controls, may result in material errors in DHS' financial data that are not detected, in a timely manner, in the

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

normal course of business. In addition, as a result of the presence of IT weaknesses there is added pressure on the other mitigating manual controls to be operating effectively at all times. Because mitigating controls often require more human involvement, there is an increased risk of human error that could materially affect the financial statements.

Criteria: The FISMA passed as part of the *E-Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with NIST guidance.

OMB Circular No. A-130 describes specific essential criteria for maintaining effective general IT controls.

FFMIA set forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government.

DHS' *Sensitive Systems Policy, 4300A*, documents policies and procedures adopted by DHS intended to improve the security and operation of all DHS IT systems.

The FISCAM provides a framework and recommended audit procedures that are used to conduct the IT general control test work.

Recommendations: We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO make the following improvements to the Departments financial management systems:

For access controls:

a) Implement an account management certification process within all the components to ensure the periodic review of user accounts for appropriate access and to ensure that generic accounts do not exist on the system;

b) Implement and appropriately implement an access authorization process that ensures that a request is completed and documented for each individual prior to granting him/her access to a financial application or database;

c) Implement a process to ensure that all accounts of terminated individuals from the system are immediately removed/end-dated/disabled upon their departure. This includes both terminated employees and contractors;

d) Enforce password controls that meet DHS' password requirements on all key financial systems. Conduct periodic vulnerability assessments, whereby systems are periodically reviewed for access controls not in compliance with DHS and Federal guidance and ensure that action is taken to remediate any security weaknesses identified;

e) Implement a patch and security configuration process, and enforce the requirement that systems are periodically tested by DHS components and the DHS Office of Chief Information Officer; and

II. 11

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

f) Develop and implement detailed procedures requiring the review of operating system logs for suspicious activity and conduct audit log reviews of the operating system on a consistent and timely basis.

For application software development and change control:

a) Further develop and enforce policies that require changes to the configuration of the system are approved and documented, and audit logs are activated and reviewed on a periodic basis;

b) Implement a single, integrated change control process over the DHS components' financial systems with appropriate internal controls to include clear lines of authority to the components' financial management personnel and to enforce responsibilities of all participants in the process and documentation requirements. Further develop and enforce policies that require changes to the configuration of the system are approved and documented, and audit logs are activated and reviewed on a periodic basis;

c) Reevaluate and revise the contract between DHS and the software vendor or otherwise ensure that the security configurations associated with the application changes and software patches are in compliance with DHS and NIST standards for financial applications;

d) Develop and implement formal policies and procedures for restricting access to DHS system software, and promulgate it to all needed personnel, to be in compliance with DHS *Sensitive Systems Policy*, 4300A;

e) Develop and implement procedures to perform a periodic review of access to financial application software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle; and

f) Remove excessive access to the all DHS financial application software and support files. Develop, document and implement a formalized SDLC process.

For service continuity:

a) Update the COOP to document and prioritize an accurate listing of critical IT systems;

b) Perform testing of key service continuity capabilities, including contingency planning;

c) Ensure that the alternate processing site is made operational;

d) Rotate backups off-site on a regular basis, implement policies and procedures developed to enforce testing of backups, and Test backups at least annually;

e) Revise the COOP to incorporate critical data files and alternate processing facility; and

f) Ensure that all employees and contractors acknowledge and sign a Rules of Behavior prior to being granted LAN access.

II-D Not Used

II-E Capital Assets and Supplies (FEMA, TSA and US-Visit)

	2007	2006	2005
FEMA	MW	N/A	N/A
TSA	SD	[illegible]	[illegible]
US-Visit	SD	[illegible]	[illegible]

Background: FEMA maintains a stockpile of inventory (e.g., blankets, bottled water, cots, tarps, plastic sheeting, Meals Ready to Eat, and ice), to be used for disaster relief if the need arises. After the 2005 hurricane season, FEMA substantially

II. 12

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

increased the amount of supplies that are stockpiled. The large increase in supplies has also increased the asset's carrying value on FEMA's and DHS' financial statements. FEMA policies require the agency to conduct an annual inventory of the supplies.

TSA maintains extensive capital assets used at airports to screen passengers and their baggage. In FY 2006, we reported accounting process and control weaknesses at TSA related to, among other things, the unreconciled Property, Plant and Equipment (PP&E) balances, and the lack of supporting documentation needed to perform our audit. These conditions also prevented TSA from asserting that its September 30, 2006 PP&E was fairly stated. During FY 2007, TSA executed a CAP to correct these deficiencies. We noted that TSA corrected the deficiencies we reported in prior years by September 30, 2007.

The mission of US-Visit is to collect, maintain, and share information on foreign nationals traveling to and from the United States in order to enhance national security, facilitate legitimate trade and travel, and contribute to the integrity of our immigration system, while deploying the program in accordance with existing privacy laws and policies. Customized software is being developed to assist with this objective.

Conditions: We noted the following internal control weaknesses related to capital assets and supplies at FEMA, TSA and US-Visit:

1. FEMA:
   - Did not fully adhere to its policies when performing its annual physical count of supplies inventory. We noted that:
     - Inventory counts were not fully reconciled to FEMA's Logistics Information Management System (LIMS), which is used to track inventory;
     - Inventory counts were not conducted in a well-controlled environment. We noted numerous weaknesses in how the procedures were conducted, which increased the likelihood of error; and
     - In some cases inventory that was in LIMS could not be located.
   - Adjustments to the stockpile inventory were not recorded in FEMA's general ledger system as they occurred throughout FY 2007.
2. TSA:
   - Did not reconcile its PP&E subsidiary ledger to its general ledger consistently and timely throughout FY 2007. However, TSA was reconciling timely by year-end.
   - Has not recorded depreciation on certain explosive detection equipment, using a method that is consistent with generally accepted accounting principles. Specifically, TSA began recording depreciation expense prior to the date the equipment was placed in service. Consequently, TSA has recorded excessive depreciation expense during FY 2007 and in previous years totaling approximately $80 million. TSA recomputed the depreciation expense, using the correct date placed in service, and adjusted its PP&E, depreciation expense, and net position balances to correct the error in its FY 2007 financial statements. The adjustment also resulted in a restatement of TSA's 2006 financial statements.
   - Uses USSGL Account No. 1890 (Other PP&E) to record all PP&E purchases, which is not compliant with the USSGL requirements of FFMIA.
   - Improperly capitalized certain advance payments to vendors as construction in progress.

II. 13

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

3. US-Visit:

   - Did not consistently apply procedures to identify and capitalize software development costs or to reclassify software placed into production from software in development; and

   - Does not have a reliable financial accounting and reporting process or system in place to routinely account for its software expenditures, capitalize appropriate amounts, and report those balances to OFM to report in the consolidated financial statements.

Cause/Effect: FEMA personnel performing the physical count of supplies lacked training in proper inventory count procedures and failed to reconcile results to the LIMS database. Without accurate physical counts and reconciliations to the perpetual records, FEMA cannot be sure supplies exist, listings of available supplies are complete, and the financial statements accurately reflect the asset values. FEMA was unable to devote sufficient human resources to properly account for its stockpile during FY 2007 (see Exhibit II-A, *Financial Management and Entity Level Controls*).

TSA personnel considered that the date of purchase and receipt of the explosive detection equipment was a reasonable approximation of the date the asset was placed in service. Verification of the reasonableness of this accounting practice was not performed, and consequently the discrepancy was not discovered until our audit of capital assets this year. Because of insufficient accounting code details on purchase orders and related system configurations, TSA's accounting services provider (Coast Guard) records PP&E purchases that do not have sufficient accounting code details to USSGL Account No. 1890 until information is available to record such purchases in the appropriate capitalized PP&E or expense account.

US-Visit has developed adequate accounting policies for tracking software development costs, these policies are not fully or adequately implemented during FY 2007. With assistance from OFM, US-Visit was able to manually compute an estimated balance, which was reclassified to capitalized software at year end for financial statement presentation purposes. A lack of sufficient personnel assigned to the financial reporting areas of US-Visit appear to have contributed to implementation delays.

Criteria: SFFAS No. 6, *Accounting for Property, Plant, and Equipment*, requires that PP&E is recorded at historical cost with an adjustment recorded for depreciation. Depreciation expense should be recognized in the financial statements beginning on the date that the asset is placed in service for its intended use.

According to GAO *Standards*, assets at risk of loss or unauthorized use should be periodically counted and compared to control records. Policies and procedures should be in place for this process. The FSIO publication, *Inventory, Supplies, and Material System Requirements,* states that the general requirements for control of inventory, supplies, and materials consist of the processes of receipt and inspection. An agency's inventory, supplies and materials system must identify the intended location of the item and track its movement from the point of initial receipt to its final destination. SFFAS No. 3, *Accounting for Inventory and Related Property*, states OM&S shall be valued on the basis of historical cost.

Per FEMA Manual 6150.1 Section 4-4g, *Annual Inventory of Accountable Property*, the designated Property Management Officers (PMO) will ensure that a complete physical inventory of FEMA property with acquisition cost of $5,000 or more, sensitive items, serialized equipment, and loaned equipment is made annually, discrepancies reconciled, and the results maintained on file for one year. The annual inventory of accountable property may be wall-to-wall (closed), cyclic (open), or special (when directed). A wall-to-wall inventory is a complete counting of all items located within the organization as of a scheduled date. A cyclic inventory is the counting of

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

a portion of the organization's property during a given period of time (monthly, quarterly, or semiannually) to cover the entire account in a one-year period. A special inventory is the counting of selected items for a specific reason.

SFFAS No. 10, *Accounting for Internal Use Software*, provides requirements for the capitalization and reporting of software development costs. GAO *Standards* require that internal control and all transactions and other significant events be clearly documented and readily available for examination. The JFMIP, *Property Management Systems Requirements,* state that the agency's property management system must create a skeletal property record or have another mechanism for capturing information on property in transit from the providing entity (e.g., vendor, donator, lender, grantor, etc.).

Recommendations: We recommend that:

1. FEMA:
   a) Devote necessary personnel to develop and implement proper accounting policies and procedures and related internal controls to ensure that its stockpiled inventory is accurately and completely accounted for in its general ledger throughout the year;
   b) Establish and implement a plan to perform a closed annual inventory count as required by FEMA Manual 6150.1 Section 4-4g, Section g., *Annual Inventory of Accountable Property*;
   c) Provide more training and detailed instruction to Logistics Center staff on performing inventory counts, including the completion of count sheets and the performance of recounts; and
   d) Reconcile the physical inventory counts, including the annual physical inventory, to the perpetual counts recorded in LIMS, and resolve related discrepancies.
2. TSA:
   a) Formally modify its policy to define the placed in service date, which then begins the process of recording periodic depreciation expense;
   b) Implement needed IT system changes to properly account for and maintain placed in service dates;
   c) Work with its accounting services provider to discontinue the use of USSGL Account No. 1890 and record PP&E to the proper general ledger account upon purchase; and
   d) Develop and implement management review controls over equipment purchase contracts to ensure that amounts advanced to vendors are properly accounted for given the terms of the underlying contract.
3. US-Visit implement procedures for developers to track and notify accounting personnel when software has been placed into production so that accounting personnel can properly classify and amortize the software costs, and appropriate and sufficient evidence is maintained to document management's decisions that lead to significant accounting transactions.

II-F Other Liabilities (FEMA, G&T, and TSA)

	2007	2006	2005
OFM	C	MW	N/A
FEMA	MW	MW	MW
G&T*	MW	MW	MW
TSA	SD	SD	MW

* G&T grants merged with FEMA in 2007

Background: In 2006, we reported that OFM and DHS General Counsel had not implemented adequate policies and procedures to accurately estimate and report an accrual for contingency legal liabilities. OFM, DHS General Counsel, and each of the DHS

II. 15

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

component entities implemented a corrective action plan in 2007, and have successfully remediated the control deficiencies we reported last year.

For the first two fiscal quarters of FY 2007, the G&T was a component of the Preparedness Directorate within DHS. During this time, accounting services for G&T were provided by the Department of Justice through an interagency agreement. These accounting services included the development and implementation of a grant accrual methodology to be used in G&T's quarterly reporting financial reporting. Effective March 31, 2007, G&T's operations were transferred to FEMA as a result of the *Post-Katrina Emergency Management Reform Act of 2006*. The financial and grant data of G&T was fully transferred to FEMA on May 15, 2007. Accordingly, FEMA is now responsible for providing accounting services for G&T, including the grant accrual methodology, and prepares its monthly financial submissions used by OFM to prepare the DHS consolidated financial statements.

A part of TSA's employee compensation package includes annual leave, which accrues at varying rates and is based on years of service, and related benefits. The annual leave liability and related benefit accruals in TSA's financial statements at September 30, 2007, totaled approximately $193 million.

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

1. FEMA:
    - Did not establish a reliable method, including validation of data and assumptions made, to estimate G&T grants payable [or advances] for accrual in the financial statements at September 30, 2007. FEMA management was unable to provide assurance that the accrued liability related to former G&T grants, was accurate, and complete at September 30, 2007.
    - Did not have sufficient policies and procedures in place to fully comply with the *Single Audit Act Amendments of 1996* and related OMB Circular No. A-133, *Audits of States, Local Governments, and Nonprofit Organizations* (see Exhibit IV-K, *Single Audit Act Amendments of 1996*).
2. TSA:
    - Has not maintained all of the necessary supporting documentation for us to complete our audit procedures over accrued annual leave. From a sample of 75 items, 13 items could not be supported and 5 contained errors.
    - Has not reconciled annual leave balances earned by employees per the payroll provider's output records to the data submitted by TSA and with the general ledger on a routine basis, which likely contributed to the errors identified in our sample.

Cause/Effect: FEMA did not have sufficient resources to perform all accounting functions related to the transfer of G&T grant administration and accounting that occurred in FY 2007. FEMA accounting staff used FEMA's historical methodology for estimating the grant liability for FEMA's grant portfolio to compute and record a grant liability at year end for the former G&T grant portfolio. However, FEMA was unable to validate this application of its methodology as appropriate and plans to perform its validation during FY 2008. Consequently, we were unable to complete our audit procedures over the accrued grant liability presented in the DHS consolidated balance sheet at September 30, 2007. Additionally, without effective procedures to timely resolve and close audit reports with identified questioned costs or other findings, the circumstances leading to the findings may continue to exist and amounts due to the government may not be received timely.

II. 16

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

The portion of TSA's annual leave liability that is in question relates to a balance that was transferred from a payroll system that has been replaced. Supporting information is not readily available to determine the correct liability at September 30, 2007.

Criteria: GAO *Standards* hold that transactions should be properly authorized, documented, and recorded accurately and timely. SFFAS No. 1, *Accounting for Selected Assets and Liabilities*, states, "When an entity accepts title to goods, whether the goods are delivered or in transit, the entity should recognize a liability for the unpaid amount of the goods. If invoices for those goods are not available when financial statements are prepared, the amounts owed should be estimated."

SAS No. 57, *Auditing Accounting Estimates*, states "An entity's internal control may reduce the likelihood of material misstatements of accounting estimates. Specific relevant aspects of internal control include the following: Accumulation of relevant, sufficient, and reliable data on which to base an accounting estimate and comparison of prior accounting estimates with subsequent results to assess the reliability of the process used to develop estimates."

OMB Circular No. A-133 states that grants should be monitored by the grant making organization.

Recommendations: We recommend that:

1. FEMA:
   a) Develop, test (e.g., validation of data and assumptions made), and implement a reliable method to periodically estimate G&T grants payable [or advances] for accrual in the financial statements during the year; and
   b) Implement policies and procedures to ensure full compliance with OMB Circular No. A-133.
2. TSA:
   a) Develop and perform procedures to enable management to assert to the appropriateness of the "beginning" accrued leave balance at a point in time (e.g., October 1, 2007). For example, these procedures may involve validating leave balances for all TSA employees at the selected point in time. These procedures should require that sufficient documentation be retained for purposes of the annual financial statement audit; and
   b) Develop and implement policies and procedures to reconcile annual leave balances per its payroll provider output records to input records submitted by TSA and to the TSA general ledger each pay period. These reconciliations should be documented, reviewed by an appropriate supervisor, and maintained.

II-G Budgetary Accounting (FEMA and TSA)

	2007	2006	2005
FEMA	MW	MW	MW
TSA	MW	MW	MW
ICE	C	SD	MW
MGMT	C	MW	N/A
US-Visit	C	SD	N/A

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. Combined, DHS has over 300 separate Treasury fund symbols (TAFS), 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, multiyear, and no-

II. 17

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

year appropriations; and several revolving, special, and trust funds. Accounting for budgetary transactions in a timely and accurate manner is essential to manage the funds of the Department and prevent overspending of allotted budgets.

Immigration and Customs Enforcement (ICE), Management Directorate, and U.S.-Visit each developed and implemented corrective action plans during FY 2007, to address the internal control weaknesses in budgetary accounting that we reported in our 2006 report.

The National Response Plan (NRP) calls for use of Other Federal Agencies (OFA) to provide goods and services to assist FEMA with its response to a disaster, as needed. The NRP defines a Mission Assignment as the vehicle used by FEMA to support Federal operations during a major disaster or emergency declaration covered under the *Stafford Act*. These work orders are issued by FEMA to OFAs to direct completion of a specific task and represent the primary documentation maintained by FEMA to support its obligations for disaster relief operations/programs being performed by OFAs.

TSA has substantial obligations and undelivered orders at year end, primarily for contract services and purchases of equipment. TSA's Office of Acquisition in coordination with TSA's Office of Financial Management monitors obligation activity and provides key input data needed to properly deobligate funds and prepare an accurate accounts payable estimate.

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

1. FEMA:
   - Did not adequately monitor the status of its obligations and ensure the timely deobligation of mission assignments resulting in a material misstatement of UDOs at the time of our testwork. We noted the following:
     - In a sample of 74 mission assignment obligations, approximately 50 percent were past their projected end dates by more than 120 days, and in some cases more than a year; and
     - Quarterly reviews of open obligations required by FEMA policies were not consistently performed or documented in the supporting records.
   - OFA's did not always provide FEMA with timely progress reports that included sufficient cost/billing data. Sufficient documentary evidence was not obtained and/or documented timely for mission assignment manager follow-up procedures with the OFAs.
2. TSA:
   - Does not have a funds control process in place to monitor outstanding obligation balances on a periodic basis (e.g., quarterly). During our interim testwork we identified 7 errors out of a sample of 75 items, and a projected overstatement undelivered orders of approximately $200 million. During our year-end testwork we identified 26 errors out of a sample of 195 items, and a projected overstatement of undelivered orders of approximately $130 million.
   - Does not have sufficient policies and procedures requiring contract officers to monitor and close-out contracts, and we noted some deficiencies in the effectiveness of TSA's validation and verification process conducted over its obligations during the second half of FY 2007.

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

- Completed an investigation over certain obligations recorded in previous years and determined that a violation of the *Anti-deficiency Act* occurred in previous years (see Exhibit IV-P, *Anti-deficiency Act*).

Cause/Effect: Although TSA has initiated a validation and verification process over its obligations, TSA was unable to complete the process before September 30, 2007.

FEMA's ability to monitor and manage mission assignments continues to be affected by resource limitations. In addition, FEMA is dependent on OFA's to provide timely information on the status of mission assignment obligations throughout the year. Lacking this information, FEMA is unable to effectively monitor and account for outstanding mission assignments, e.g., recording a proper account payable and deobligating excess funds.

Criteria: FEMA's SOP for *Processing Mission Assignment and Interagency Payments for Fund Code 06*, updated April 2007, establishes the process for mission assignment closeouts. If no activity has been recorded within the last 90 days, the Disaster Finance Branch initiates the closeout process with the Region or Headquarters.

The FEMA Form 90-129, *Mission Assignment Agreement,* states that the OFA is responsible for submitting a Mission Assignment Monthly Progress Report to FEMA to include cost data when mission assignments take more than 60 days to complete, including billing. To assist with this process, OMB issued its Memorandum – *Yearend Accounting Guidance for Disaster Relief Fund Transactions* dated September 17, 2007.

The *Anti-deficiency Act* is a series of statutes prohibiting agencies from obligating or expending funds in advance of appropriation or apportionment, OMB Circular No. A-11 has strict requirements for notification and reporting Anti-deficiency violations. GAO *Standards* hold that transactions should be properly authorized, documented, and recorded accurately and timely.

According to JFMIP's *Core Financial System Requirements*, an agency's core financial management system must ensure that an agency does not obligate or disburse funds in excess of those appropriated and/or authorized and specific system edits and user notifications related to funds control must be in place. The *Federal Acquisition Regulation* Section 1.6 addresses the authorities and responsibilities granted contracting officers. Treasury's USSGL guidance specifies the accounting entries related to budgetary transactions.

OMB Circular No. A-123 states, "Agency managers should continuously monitor and improve the effectiveness of internal control associated with their programs." This continuous monitoring, and other periodic evaluations, should provide the basis for the agency head's annual assessment of and report on internal control, as required by FMFIA. This Circular indicates that "control weaknesses at a service organization could have a material impact on the controls of the customer organization. Therefore, management of cross-servicing agencies will need to provide an annual assurance statement to its customer agencies in advance to allow its customer agencies to rely upon that assurance statement. Management of cross-servicing agencies shall test the controls over the activities for which it performs for others on a yearly basis. These controls shall be highlighted in management's assurance statement that is provided to its customers. Cross-servicing and customer agencies will need to coordinate the timing of the assurance statements."

FFMIA Section 803(a) requires that each Agency implement and maintain a system that complies substantially with Federal financial management system requirements as stipulated by OMB Circular No. A-127.

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

Recommendations: We recommend that:

1. FEMA:

   a) Require all regional offices to perform a complete UDO review, monitor timely completion of this review, and ensure that all identified mission assignment deobligations are processed in the general ledger promptly;

   b) Ensure that personnel follow the established policy for quarterly obligation reviews prior to the end of each quarter to timely determine whether the remaining balance on a mission assignment is valid, or whether a deobligation of the remaining balance is necessary;

   c) Enforce the requirement that all OFA's submit not only a progress report when the mission assignment takes more than 60 days to complete, but a progress report every additional 30 days that the project remains either programmatically or financially incomplete. The report should include an estimated completion date and, when applicable, Form 90-136 should be submitted for extension of the projected end-date whenever the estimate for programmatic completion is more than 30 days;

   d) Consider involving OMB in a permanent solution, such as Agreed-upon Procedures engagements, to ensure that FEMA receives sufficient and timely information from OFA's to properly account for obligations related to outstanding mission assignments; and

   e) Consider adding additional temporary or permanent accounting staff to improve the deobligation process (our recommendations in I-A, *Financial Management Oversight and Entity Level Controls,* will also help address these conditions).

2. TSA:

   a) Require contracting officers to review and certify whether obligations are valid or require deobligation on a periodic basis (e.g., quarterly);

   b) Refine or develop a new general ledger reporting tool that provides the contracting officers accurate information regarding outstanding obligated balances to include information related to the last activity date to assist in aging the balance;

   c) Refine existing processes by which the Business Management Office periodically examines outstanding obligations and makes recommendations (e.g., deobligation) on outstanding balances; and

   d) Develop formal policies and procedures to assist in expediting deobligations of funds associated with invalid obligations in advance of a formal contract close out.

II. 20

Independent Auditors' Report
Exhibit III – Significant Deficiency – DHS Civilian Components

III-H Custodial Revenue and Drawback

Background: CBP collects approximately $30 billion in annual import duties, taxes, and fees on merchandise arriving in the United States from foreign countries. Receipts of import duties and related refunds are presented in the statement of custodial activity in the DHS financial statements. CBP is the only DHS component with significant custodial responsibilities.

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.

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 considered outside of the CBP territory, upon activation. 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 origin.

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

Related to drawback:

- The Automated Commercial System (ACS) lacked automated controls to detect and prevent excessive drawback claims and overpayments, necessitating inefficient manual processes that do not effectively compensate for these automated controls.
- Drawback review policies did not require drawback specialists to review all or a statistically valid sample of related drawback claims against the underlying consumption entries to determine whether, in the aggregate, an excessive amount was claimed.

Related to the entry process – collection of taxes, duties and fees:

- Policies, procedures, and general guidance provided to field offices related to review procedures, and documentation requirements for the monthly review of the entry process are weak. Consequently, we noted a number of instances of noncompliance with CBP guidelines, inconsistencies in review performance, and a lack of documentation to confirm performance of the monthly reviews.

Related to BW, FTZ, and In-bond:

- We noted inconsistencies in the performance of risk assessments and compliance reviews of BWs, and FTZs, and in-bond entries in various ports. In addition, HQ review of the BW and FTZs assessment results can take up to six months to compile and analyze. Further, no policies or procedures exist to monitor the results of the in-bond audits/reviews.
- CBP is unable to determine the status of the in-bond shipments with the information available within ACS.

Cause/Effect: CBP has been challenged to balance its commitment of limited resources to two important mission objectives – trade compliance, including the collection of taxes, duties and fees owed to the Federal government, and securing the U.S. borders from potential terrorist entry. In FY 2007, CBP made significant improvements in its custodial review controls and measurement

III. 1

Independent Auditors' Report
Exhibit III – Significant Deficiency – DHS Civilian Components

processes, procedures, and policies. For drawback, much of the process is manual until planned IT system functionality improvements are made, placing an added burden on limited resources.

Criteria: Under FMFIA, management must implement cost-effective controls to safeguard assets and ensure reliable financial reporting. OMB's *Revised Implementation Guidance for FFMIA,* states that financial systems should "routinely provide reliable financial information consistently, accurately, and reported uniformly" to support management of current operations.

JFMIP publications and OMB Circular No. A-127 outlines the requirements for Federal systems. JFMIP's *Core Financial System Requirements* state that the core financial system must maintain detailed information by account sufficient to provide audit trails and to support billing and research activities. OMB Circular No. A-127 requires that the design of financial systems should eliminate unnecessary duplication of a transaction entry. Wherever appropriate, data needed by the systems to support financial functions should be entered only once, and other parts of the system should be updated through electronic means consistent with the timing requirements of normal business/transaction cycles.

The *Improper Payments Information Act of 2002*, effective in FY 2004, requires agencies to assess the risk of erroneous payments and develop a plan to correct control weaknesses. In addition to the regulatory requirements stated above, CBP's *Drawback Handbook*, dated July 2004, states that management reviews are necessary to maintain a uniform national policy of supervisory review.

Recommendations: We recommend that CBP:

Related to drawback:

a) Implement effective internal controls over drawback claims as part of any new systems initiatives, including 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; and

b) Implement automated controls within ACS to prevent overpayment of a drawback claim that is subject to deem liquidation.

Related to entry:

a) Provide additional detail in the guidelines, specifying the sample size, procedures to perform, and documentation requirements for the CM Coordinator's review of the Import Specialists' review. The guidance should also readdress the timing requirements for the monitoring reports or data queries and documentation retention; and

b) Conduct periodic training to ensure that all port personnel have comprehensive knowledge of the CM program requirements.

Related to BW, FTZ, and In-bond:

a) Ensure adequate communication of the ports requirements related to the annual risk assessments and compliance reviews and provide effective training so that all responsible personnel are aware of and can consistently execute all of the requirements; and

b) Implement a standard procedure to periodically compile the results of all In-bond audit/reviews during the year and develop an analysis function in order to evaluate the importers' compliance with regulations.

III. 2

Independent Auditors' Report
Exhibit IV – Compliance and Other Matters

(Exhibits I and II include Comments A – G, and Exhibit III presents Comment H)

All of the compliance and other matters described below are repeat conditions except IV-P *Anti-deficiency Act*, which is new finding in FY 2007.

IV-I *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 management controls; 2) assess the adequacy of management controls; 3) identify needed improvements; 4) take corresponding corrective action; and 5) report annually on management controls. During FY 2007, DHS developed a CAP titled *Internal Controls over Financial Reporting Playbook* to implement corrective actions and support management assurances by performing tests of design and operating effectiveness on entity level controls and other financial accounting and reporting processes. DHS' implementation of OMB Circular No. A-123 also facilitates compliance with FMFIA and the *DHS Financial Accountability Act of 2004*, which requires an annual audit of internal control over financial reporting.

While we noted the Department overall has taken positive steps toward full compliance with FMFIA and OMB Circular No. A-123, the Coast Guard has not fully established effective systems, processes, policies, and procedures to develop and implement internal accounting and administrative controls, and conformance of accounting systems. In addition, TSA and FEMA's control assessment processes require improvement to ensure full compliance with FMFIA.

Recommendations: We recommend that the Coast Guard, FEMA, and TSA fully implement the FMFIA process, as prescribed by the OCFO, to ensure full compliance with FMFIA and its OMB approved plan for Circular No. A-123 implementation in FY 2008. We also recommend that the OCFO consider additional training for its components, to ensure a thorough understanding of requirements.

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

Passage of the *DHS Financial Accountability Act of 2004* made DHS subject to the FFMIA, beginning in FY 2005. FFMIA Section 803(a) requires that agency Federal financial management systems comply with 1) Federal accounting standards, 2) Federal system requirements, and 3) the 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. 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 management controls; 2) assess the adequacy of management controls; 3) identify needed improvements; 4) take corresponding corrective action; and 5) report annually on management controls. During FY 2007, DHS OCFO continued with its implementation of OMB Circular No. A-123, by performing tests of design and operating effectiveness on entity level controls and other financial accounting and reporting processes as planned. DHS' implementation of OMB Circular No. A-123 also facilitates compliance with the *DHS Financial Accountability Act of 2004*, which requires an annual audit of internal control over financial reporting.

While we noted the Department overall has taken positive steps toward full compliance with FMFIA and OMB Circular No. A-123, the Coast Guard, FEMA, 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. The Secretary of DHS also has stated in the Secretary's Assurance Statements dated November 15, 2007, as listed in Management's Discussion and Analysis (MD&A) of the Department's 2007 *Annual Financial Report* (AFR), that the Department cannot provide assurance that its financial

IV.1

Independent Auditors' Report
Exhibit IV – Compliance and Other Matters

management systems are in substantial compliance with the requirements of FFMIA. The Department's remedial actions and related timeframes are also presented in that section of the 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 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 Exhibits I-C and II-C *Financial Systems Security*, which impact the Department's ability to fully comply with FISMA.

Recommendations: 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 2008.

IV-K *Single Audit Act Amendments of 1996,* and Laws and Regulations Supporting OMB Circular No. A-50, *Audit Follow-up,* as revised

During 2007, DHS' G&T Directorate merged its grants making function with FEMA. FEMA is now the only DHS component that has a significant grant making operation. OMB Circular No. A-133 requires agencies awarding grants to ensure they receive grantee reports timely and to follow-up on grantee Single Audit findings. 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 2007. We noted that FEMA does not always obtain and review grantee Single Audit reports in a timely manner, and 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.

OMB Circular No. A-50, as revised, provides guidance for use by executive agencies when considering reports issued by Inspectors General, other executive branch audit organizations, the GAO, and non-Federal auditors, where follow up is necessary. Corrective action taken by management on findings and recommendations is essential to improve the effectiveness and efficiency of government operations, and to support the objectives of sound fiscal management. The DHS OCFO has developed an extensive corrective action plan that requires each component to develop and execute corrective actions to address all material weaknesses in internal controls. This strategy is documented in the DHS Internal Controls over Financial Reporting (ICOFR) "Playbook." Progress is monitored by the CFO, and regularly reported to OMB and other outside stakeholders, such as Congressional Committees. We noted that each component has complied with the OCFO directive to develop corrective actions, and they have been reviewed and approved by the CFO. All DHS components have made progress toward remediation of material internal control weaknesses; however, as shown in described in Exhibits I, II and III, deficiencies identified in prior years have not been fully corrected in FY 2007.

Independent Auditors' Report
Exhibit IV – Compliance and Other Matters

Recommendations: We recommend that:

Regarding Single Audit Act Amendments of 1996:

1. FEMA develop 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 2008:
   a) Further develop and implement a tracking system to identify each grantee for which an OMB Circular No. A-133 Single Audit is required, and the date the audit report is due;
   b) Strengthen communication with the cognizant agencies;
   c) Use the tracking system to ensure audit and performance reports are received timely, or to follow-up when reports are overdue; and
   d) Perform reviews of grantee audit reports, issue-related management decisions, and ensure that the grantees take appropriate corrective action, on a timely basis.

Regarding OMB No. A-50, Audit Follow-up, as revised

2. DHS continue to follow and complete the actions defined in its ICOFR "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 2008.

IV-L *Improper Payments Information Act of 2002*

DHS is required to comply with the *Improper Payments Information Act of 2002* (the Act or IPIA). The Act requires agencies to review all programs and activities they administer annually and identify those that may be susceptible to significant erroneous payments. For all programs and activities where the risk of erroneous payments is significant, agencies must estimate the annual amounts of erroneous payments, and report the estimates to the President and Congress with a progress report on actions to reduce them. The agency must report a statistically valid error projection for susceptible programs in its annual Performance and Accountability Report (PAR). To facilitate the implementation of the Act, OMB issued guidance in Memorandum M-03-13, *Implementation Guide for the Improper Payments Information Act of 2002*, and in Appendix C, *Requirements for Effective Measurement and Remediation of Improper Payments*, to OMB Circular No. A-123, *Management's Responsibility for Internal Controls*, which provides a recommended process to meet the disclosure requirements.

In FY 2007, we noted the Department has taken positive steps toward full compliance with IPIA, and Appendix C of OMB Circular No. A-123, including identification of programs subject to IPIA, conducting a comprehensive process to assess the risk of programs susceptible to improper payments, and performing sample testing of programs. However, DHS did not fully comply with the Act in FY 2007. We noted that at DHS and its components:

- Some federal disbursements were excluded from the scope of DHS IPIA testwork performed.
- Some programs identified as high risk of significant improper payments during the assessment process were not tested, and some programs identified as low risk of significant improper payments were selected for testing. Accordingly, this sample testing did not meet the IPIA requirements in FY2007.
- The testing time frames selected for some components were not approved by OMB in advance, and in some cases the testing timeline did not appear to provide enough time to complete testwork over selected programs.

IV.3

Independent Auditors' Report
Exhibit IV – Compliance and Other Matters

- CAPs were not developed for all programs identified as "high risk" during the risk assessment process, if no statistical sampling was performed to validate those risks during FY2007 due to DHS' multi-year compliance plan.

Recommendation: We recommend that DHS risk assessments be completed earlier in the year so that programs identified as high risk by risk assessments are the programs that are sample tested. DHS needs to strengthen oversight of components' progress in implementing corrective action plans and in recovering improper payments for high-risk programs. Also, DHS should review sample testing procedures and begin to independently validate the results of components' sample testing.

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' OIG has engaged an independent auditor to audit the September 30, 2007 balance sheet and related statement of custodial activity. Other financial statements, including the statements of net cost, 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 corrective action plans described in DHS' ICOFR "Playbook" (see Comment IV – I, *Federal Managers' Financial Integrity Act of 1982*, above) to remediate the FY 2007 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.

IV-N *Government Performance and Results Act of 1993* (GPRA)

The *Government Performance and Results Act* requires each agency to develop a strategic plan, that includes a description of how goals and objectives are to be achieved, including a description of the operational processes, skills and technology, and the human, capital, and other resources required to meet those goals and objectives. The Department's annual performance plan and performance reports, that measure progress toward achieving strategic goals and related performance metrics are also integral to compliance with GPRA. We noted that DHS' Strategic Plan expired on October 1, 2006 and the Department has not yet provided an updated Strategic Plan as of September 30, 2007. Consequently, the Department is not in compliance with the requirements of GPRA during FY 2007. In addition, we noted that the existing (expired) strategic plan did not align all strategic objectives to performance objectives as required.

Recommendation: We recommend that DHS ensure full compliance with GPRA by completing its updated Strategic Plan and aligning all performance goals to its strategic objectives in FY 2008.

IV-O *Debt Collection Improvement Act of 1996* (DCIA)

The *DCIA of 1996* (DCIA) is intended to significantly enhance the Federal Government's ability to service and collect debts. Under the DCIA, the Treasury assumes a significant role for improving government-wide receivables management. The DCIA requires Federal agencies to refer eligible delinquent nontax debts over 180 days to U.S. Treasury for the purpose of collection by cross-servicing or the offset program. Our tests of compliance disclosed instances where DHS was not in compliance with certain provisions of the DCIA. Specifically, we noted that due process is not performed in a timely manner to ensure that some eligible debts are forwarded to

IV.4

Independent Auditors' Report
Exhibit IV – Compliance and Other Matters

the Treasury for cross-servicing or the offset program within the timeframes established by DCIA.

Recommendation: We recommend that DHS develop policies and procedures to ensure full compliance with the DCIA in FY 2008.

IV-P *Anti-deficiency Act*

DHS and TSA management notified us of an *Anti-deficiency Act* violation that occurred in the TSA, Expenses Account, Treasury Symbol – 70X0508 in an amount up to $155 million, where expenditures and obligations exceeded available funding in FY 2004. The DHS Secretary has reported the violation to the President of the United States, the President of the Senate, the Speaker of the House of Representatives, and the Comptroller General, as required by 31 U.S.C. Section 1351. After establishing certain budgetary authority within its DHS general ledger through a journal entry, the related individual purchase orders were then recorded and the journal entry reversed in March 2003. A subsequent transaction in May 2003 erroneously reversed the initial journal entry amount again. This second journal entry reversal, which led to the *Anti-deficiency Act* violation, overstated TSA's budget authority by underreporting its existing obligations. A separate notification of the final determination is still required under 31 U.S.C. section 1351.

Recommendation: We recommend that TSA continue to implement the remedial actions resulting from its internal investigation of this matter.

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

Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report		Fiscal Year 2007 Status/ Disposition
Material Weaknesses:		
A.	**Financial Management and Oversight**	
A.1	The Coast Guard had not fully implemented a financial management organizational structure that supports the development and implementation of effective policies, procedures, and internal controls to ensure data supporting financial statement assertions are complete and accurate. The Coast Guard had not established clear management oversight responsibilities and processes to review adjustments to account balances, identify the cause of abnormal balances, and account relationship discrepancies, e.g., budgetary to proprietary reconciliations, and investigate potential financial system concerns such as potential posting logic errors. The Coast Guard had not fully established management oversight functions to ensure that accounting principles are correctly applied, and to provide accounting operational guidance to other offices and facilities within the Coast Guard. The Coast Guard has not completed a comprehensive Corrective Action Plan to correct longstanding internal control weaknesses.	**Repeated** (Exhibit I-A)
A.2	The OFM did not have a sufficient number of management personnel with the requisite financial accounting background to both (i) set-up, and (ii) effectively manage the financial reporting and internal controls infrastructure of a large Executive Branch agency. The OFM had not provided effective management and oversight throughout the year to monitor the operations of DHS components to promptly identify and raise issues to the CFO that may affect the quality of the financial statements. OFM had not established a process to support the timely completion of the annual financial statement audit.	**Corrected**
B.	**Financial Reporting** *(This finding has been combined with finding J below and reported as Financial Reporting in 2007)*	
B.1	The OFM continued to have significant difficulty coordinating delivery of financial data from components and preparing financial statements and disclosures throughout the year. The OFM had not established Departmental policies and procedures, or issued timely guidance to ensure that financial statements are accurate and complete during the year. Fully documented policies and procedures for many critical activities necessary to adequately manage financial reporting processes, and monitoring controls to ensure monthly TIER submissions received from the components were prepared timely and accurately.	**Partially Repeated** (Exhibit II-B)

V.1

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
B.2	The Coast Guard had not developed and implemented an effective general ledger system. The general ledgers are not compliant with the USSGL, and TIER submissions to OFM were from a database that did not have detail back-up support for some on-top adjustments at the transaction level. The Coast Guard's financial reporting process was complex and labor-intensive, and required a significant number of "on-top" adjustments (adjustments made outside the core accounting system for presentation of financial information given to DHS for consolidation). The Coast Guard had serious deficiencies in its policies, procedures, and controls surrounding its financial reporting process, and did not record all financial transactions to the general ledger systems or have adequate beginning balance and year-end close out procedures. The Coast Guard routinely used analytical comparisons to identify adjusting entries to the financial statements, without verifying that the ending balances were properly supported at the transaction level, e.g., budgetary accounts were adjusted to equal proprietary accounts, without verifying that the underlying transactional detail supported the ending balances. The Coast Guard did not have adequate procedures and internal controls over the process of preparing and reviewing the financial statement disclosures and did not have an adequate process to record, review, and monitor accounts receivable activity.	**Repeated** (Exhibit I-B)
B.3	TSA continued to experience difficulties related to financial reporting. Specifically, we noted that certain accrual amounts were not posted and certain property amounts were misstated in the final financial data submission for the June 30, 2006 hard-close; numerous other on-top adjustments were made thereafter, account reconciliations were not performed timely or completely throughout the year, and material abnormal balances and analytical account variances were not resolved timely throughout the year. TSA did not have sufficient processes and procedures established to enable the successful completion of a financial statement audit. TSA could not provide complete supporting documentation for numerous journal vouchers.	**Corrected**
B.4	OFM and certain components did not have effective financial information systems, or sufficiently documented processes, to accumulate cost data by DHS strategic goal, as required by SFFAS No. 4, *Managerial Cost Accounting Concepts and Standards*.	**Partially Repeated** (Exhibit II-B)
C.	**Financial Systems Functionality**	
	OCFO and DHS bureaus have IT and financial system security control weaknesses in entity-wide security program planning and management, access controls, application software development and change controls, system software, segregation of duties, and service continuity.	**Partially Repeated** (Exhibits I-C and II-C)

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
D.	**Fund Balance with Treasury (FBwT)**	
	The Coast Guard did not effectively manage its suspense accounts to include accurately aging and clearing items carried in suspense clearing accounts in a timely manner during the year, and did not maintain adequate supporting documentation that validated the accuracy of the FBwT reconciliations and the clearing of suspense items.	**Repeated** (Exhibit I-D)
E.	**Property, Plant, and Equipment** *(This finding has been combined with finding F below and reported as Capital Assets and Supplies in 2007)*	
E.1	The Coast Guard had not implemented appropriate controls and related processes to accurately, consistently, and timely record PP&E, to include additions, transfers from other agencies and disposals in its fixed asset system. The Coast Guard had not consistently applied policies and procedures to ensure appropriate documentation supporting PP&E acquisitions is maintained, and readily available for audit. The Coast Guard lacked methodologies and assumptions to support the value of PP&E that is not supported by original acquisition or other documentation. The Coast Guard needed an asset identification, system mapping, and tagging processes that included sufficient detail, e.g., serial number, to clearly differentiate and accurately track assets in the fixed asset system. The Coast Guard lacked an effective physical inventory process and appropriate support for the valuation method and classification of repairable PP&E to ensure accounting and reporting for PP&E is consistent with generally accepted accounting principles.	**Repeated** (Exhibit I-E)
E.2	US-Visit did not consistently apply procedures to identify and capitalize software development costs or to reclassify software placed into production from software in development. Consequently US Visit was unable to fully support the accuracy and completeness of certain property, plant, and equipment balances, to allow us to complete our testwork, prior to the completion of DHS' 2006 PAR.	**Partially Repeated** (Exhibit II-E)
E.3	TSA did not implement adequate policies and procedures to properly account for and support property balances. Subsidiary records has not been reconciled to the general ledger timely, a sub component of the general ledger had not been updated for depreciation, additions, and disposals related to certain property and equipment, and TSA was unable to provide adequate supporting documentation to support valuation of its property.	**Corrected**

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

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
F.	**Operating Materials and Supplies** *(This finding has been combined with finding E above and reported as Capital Assets and Supplies in 2007)*	
F.1	At the Coast Guard, internal controls over physical counts at field locations were not designed and implemented to remediate conditions identified during fiscal year 2003 and 2004. OM&S items were not always properly bar-coded or tagged, on-hand quantities frequently did not agree to the perpetual inventory records, and procedures did not sufficiently address whether all inventory on hand was properly recorded in the perpetual records or require discrepancies to be resolved timely. Processes and controls were not in place to fully support the calculated value of field-held and ICP OM&S to approximate historical cost. Policies, procedures and controls designed to remediate conditions related to conducting physical inventories of OM&S at the ICPs were not completely implemented.	**Repeated** (Exhibit I-E)
G.	**Legal and Other Liabilities** *(This finding has been combined with finding H below and reported as Actuarial and Other Liabilities in 2007)*	
G.1	OFM, in association with OGC, had not implemented adequate policies and procedures to ensure that OFM is provided with sufficient information to accurately and completely present legal liabilities and related disclosures in the financial statements throughout the year.	**Corrected**
G.2	The Coast Guard did not use a reliable methodology to estimate accounts payable. The method used was not supported as to the validity of data, assumptions, and criteria used to develop and subsequently validate the reliability of the estimate for financial reporting. Did not have adequate policies, procedures and internal controls over Coast Guard's process for reconciling military payroll recorded in the CAS general ledger to detail payroll records. Military personnel data changes, including changes in leave balances and payroll corrections, are not processed to be reflected in the appropriate payroll and/or reporting periods, and consequently impact the completeness and accuracy of leave and payroll accruals as well as data used for actuarial projections. Did not have documented policies and procedures, including appropriately designed internal controls, to ensure that the Coast Guard legal liabilities, included with the Department's accrued and disclosed contingent liabilities in the balance sheet at September 30, 2006, are accurate and complete. In addition, information is not prepared on a quarterly basis as necessary to prepare accurate timely financial statements throughout the year.	**Repeated** (Exhibit I-F)
G.3	G&T did not establish a reliable method, including validity of data and assumptions made, to estimate its grants payable [or advances] for accrual in the financial statements until the end of the fourth quarter of fiscal year 2006. (G&T grants merged with FEMA during 2007)	**Repeated** (Exhibit II-F)

V.4

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
G.4	TSA did not implement a new grant accrual methodology until August 2006, and the new methodology did not consider non-reporters. Therefore, the underlying expenditure data used in the accrual percentage and the actual expenditure data subsequently used for comparison/validation purposes may not be complete (corrected). Was unable to reconcile its annual leave subsidiary ledger to the general ledger during the year, creating an out-of-balance condition in July (repeated).	**Partially Repeated** (Exhibit II-F)
G.5	FEMA did not estimate and accrue accounts payable for all material open mission assignments at year-end. FEMA only accrued for mission assignments for which a payable confirmation had been received from the other Federal agency. Did not have fully effective policies and procedures to ensure that insurance company financial data collected through a third-party service provider was accurate and complete, affecting the reliability of its accounts payable balance as of September 30, 2006.	**Partially Repeated** (Exhibit II-F)
G.6	FEMA and TSA did not have sufficient policies and procedures in place to fully comply with the OMB Circular No. A-133, *Audits of States, Local Governments, and Non-profit Organizations*, and laws and regulations supporting OMB Circular No. A-50, *Audit Follow-up*, as revised.	**Partially Repeated** (Exhibit II-F)
H.	**Actuarial Liabilities** *(This finding has been combined with finding G above and reported as Actuarial and Other Liabilities in 2007)*	
H.1	The Coast Guard was unable to fully support its assertions relating to accuracy and completeness of the underlying participant data, medical cost data, and trend and experience data provided to, and used by, the actuary for the calculation of the MRS, and post employment travel benefits liabilities. The Coast Guard did not follow established policies and procedures to accumulate data for the actuary to compute post-employment travel benefits. The Coast Guard did not perform periodic reconciliations between the medical expenditures subsidiary ledger and the general ledger. The Coast Guard did not have effective policies, procedures, and controls to monitor the expenditures for medical services to ensure they were billed at proper rates and for valid participants only, e.g., service members and their families, and retiree/survivors.	**Repeated** (Exhibit I-F)

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
I.	**Budgetary Accounting**	
I.1	Coast Guard did not have effective policies, procedures and internal controls over Coast Guard's process for validation and verification of UDO balances to ensure that recorded obligations were valid, obligations incurred were recorded timely, and that proper approvals and supporting documentation is maintained. Coast Guard has not designed or implemented a comprehensive internal control program across all components of the organization to prevent or detect and correct misstatements to UDO balances reported on the financial statements. In addition, programming logic and transaction codes used to record advances for which an obligation was not previously recorded are not operating effectively to ensure the obligation and UDO are properly recorded. Procedures and controls are not adequate to prevent a commitment or obligation of funds in excess of established appropriations. Obligations were recorded in FPD, but were not properly interfaced with the CAS, and were not supported by adequate documentation. Obligations related to post-employment permanent changes of station (PCS) were not recorded at the time orders were approved and issued. Automated system controls are not effectively used to prevent the processing of procurement transactions by contracting officer's with expired warrant authority, and a manual compensating control was not effective since listings of warranted contracting officers were not complete.	**Repeated** (Exhibit I-G)
I.2	TSA did not maintain, documentation supporting UDOs and related purchase information in a manner that is readily available to management and the auditors. Consequently, TSA was unable to provide sufficient documentation to support a sample of UDO balances at year-end prior to the completion of the DHS' 2006 PAR. Has developed, but not fully implemented, IT system programming logic which allows the accounting system to record obligations recovered at the transaction level in accordance with SGL requirements.	**Partially Repeated** (Exhibit II-G)
I.3	FEMA did not have adequate resources to monitor the status and ensure the timely deobligation of mission assignments, resulting in an overstatement of UDOs at the time of our testwork. Did not maintain adequate communications with its grants disbursements service provider regarding the reliability of its internal controls. In fiscal year 2006, FEMA's grant disbursement service provider received a qualified opinion over the effectiveness of its internal controls for the period October 1, 2005, to June 30, 2006. However, FEMA was not aware of these control deficiencies until late October 2006, and consequently, payment information from the third-party service provider used to reduce obligations in its general ledger may not be accurate	**Partially Repeated** (Exhibit II-G)
I.4	ICE has not completed its validation and verification of FPS prior year obligations, in order to determine the propriety of the completeness, existence, and accuracy of those obligations.	**Corrected**

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
I.5	Management Directorate had not established policies and procedures to ensure that obligations are recorded timely. Had not established policies and procedures to ensure that all key attributes of an obligation and purchase are recorded in the financial accounting system.	**Corrected**
I.6	US-Visit has not established policies and procedures to ensure that documentation supporting obligations and subsequent disbursements is filed and readily available for management and auditor review.	**Corrected**
J.	**Intragovermental and Intradepartmental Balances** *(This finding has been combined with finding B above and reported as Financial Reporting in 2007)*	
	OFM has not been able to reconcile intragovernmental asset, liability, and revenue amounts with trading partners, as required by OMB Circular No. A-136. OFM did not coordinate a DHS-wide reconciliation throughout the year of all intragovernmental balances. We noted that DHS, in cooperation with its components, have not developed and adopted effective policies and procedures, or established systems, to completely track, confirm, and reconcile intra-governmental balances and/or transactions with trading partners in a timely manner, which contributed to the material differences, cited below in 2006. The *Material Differences Reports* submitted to Treasury identified accounting/reporting errors of approximately $1.4 billion in both the first and second quarter 2006. These differences were primarily related to activity with the following trading partners: 96-U.S. Army Corps of Engineers and 97-Office of the Secretary of Defense-Defense Agencies. These differences were not fully reconciled/ resolved by the following quarter.	**Repeated** (Exhibit II-B)

Other Reportable Conditions:

K.	**Environmental Liabilities**	
K.1	At the Coast Guard consistent policies or procedures have not been developed for the identification, evaluation, and estimation of potential environmental remediation of Coast Guard sites, thereby resulting in different approaches by shore facility commands and ultimately varying liability estimates.	**Repeated** (Exhibit I-F)

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

	Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
K.2	FLETC had not Implemented effective policies and procedures to accurately and completely estimate its liabilities. Consequently, FLETC's liability for lead contamination at its SAFRs was substantially understated and required an adjustment to the financial statements at year-end. Implemented a process to completely identify the existence of lead-paint and asbestos contamination, and to accurately estimate the cost of clean-up for financial statement purposes. The estimation process used in fiscal year 2006 was not supported by a detailed analysis that, among other things, considered the actual square footage of the contaminated area and the type of asbestos contamination.	**Corrected**
L.	**Custodial Revenue and Drawback**	
	At CBP related to drawback the ACS lacked automated controls to detect and prevent excessive drawback claims and over-payments, necessitating inefficient manual processes that do not effectively compensate for these automated controls. ACS did not have the capability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries or export documentation upon which the drawback claim was based. ACS lacked controls to prevent overpayment of drawback claims at the summary line level that were subject to the new deem liquidation process put in place during fiscal year 2006. CBP drawback review policy and procedures allowed drawback specialists, with supervisory approval, to judgmentally decrease the number of ACS selected underlying consumption entries randomly selected for review, thus decreasing the review's effectiveness. Related to the entry process – collection of taxes, duties and fees - policies, procedures, and general guidance provided to CMP coordinators related to sampling, review procedures, and documentation requirements for the monthly review of CM results are weak. The National Analysis Specialist Division port audits were no longer performed during FY 2006. CBP lacks formal policies and procedures to ensure the CM data used for analysis and to compute the revenue gap is accurately and completely input into the IT system. Related to BW, FTZ, and In-bond we noted inconsistencies in the performance of risk assessments and compliance reviews of BWs, and FTZs, and in-bond entries in various ports.	**Repeated** (Exhibit III-H)

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

Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
Compliance and Other Matters:	
M. ***Federal Managers' Financial Integrity Act of 1982***	
DHS management's FMFIA report did not contain corrective action plans for all material weaknesses identified in the PAR. In addition, DHS and its components have not established effective systems, processes, policies and procedures to evaluate and report on FMFIA compliance.	**Repeated** (Exhibit IV-I)
N. ***Federal Financial Management Improvement Act of 1996***	
We noted that DHS and each significant component did not fully comply with at least one of the requirements of FFMIA.	**Partially Repeated** (Exhibit IV-J)
O. ***Federal Information Security Management Act (Electronic Government Act of 2002)***	
We noted instances of non-compliance with FISMA that have been reported by us in the material weakness on *Financial Systems Security*.	**Combined with FFMIA** (Exhibit IV-J)
P. ***Single Audit Act Amendments of 1996,* and Laws and Regulations Supporting OMB Circular No. A-50, *Audit Follow-up,* as revised**	
DHS did not have procedures in place to fully comply with provisions in OMB Circular No. A-133 that require them to timely obtain and review grantee Single Audit reports and follow up on questioned costs and other matters identified in these reports. DHS and its components did not fully develop and implement corrective action plans to address all material weaknesses and reportable conditions identified by previous financial statement audits within the time-frames established in OMB Circular No. A-50. We also noted that some corrective action plans lack sufficient detail, such as clearly defined roles and responsibilities, actions to be taken, time-table for completion of actions, and documented supervisory review and approval of completed actions.	**Partially Repeated** (Exhibit IV-K)
Q. ***Improper Payments Information Act of 2002***	
DHS did not properly define programs and activities, institute a systematic method of reviewing all programs and identifying those at risk of significant erroneous payments, and properly sample or compute the estimated dollar amount of improper payments.	**Repeated** (Exhibit IV-L)

V.9

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

Summary of Conditions As Reported in 2006 DHS Performance and Accountability Report	Fiscal Year 2007 Status/ Disposition
R. *DHS Financial Accountability Act of 2004 (Chief Financial Officers Act of 1990)*	
Section 3 of Public Law 108-330, *DHS Financial Accountability Act of 2004,* states that the President of the United States shall appoint a Chief Financial Officer of DHS not later than 180 days after the date of the enactment of this Act signed in October 2004, to be confirmed by the U.S. Senate. At September 30, 2005 DHS was operating with an Acting CFO, while no waiver or amendment to this law has been obtained by DHS management. The *DHS Financial Accountability Act of 2004* also 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 engaged an independent auditor to audit the September 30, 2006, consolidated balance sheet and statement of custodial activity only.	**Repeated** (Exhibit IV-M)
S. *Government Performance and Results Act of 1993*	
The validation and verification section of the fiscal year 2006 DHS *Annual Performance Plan* was incomplete and included erroneous data. In addition, no performance goals or measures were established or aligned to two of the Department's strategic objectives in the *Annual Performance Plan*. GPRA states that an agency may not omit or minimize the significance of any program activity constituting a major function or operation for the agency.	**Repeated** (Exhibit IV-N)
T. *The Debt Collection Improvement Act of 1996*	
DHS was not in compliance with certain provisions of the DCIA. Specifically, we noted that due process is not performed in a timely manner to ensure that some eligible debts are forwarded to Treasury for cross-servicing or the offset program within the timeframes established by DCIA.	**Repeated** (Exhibit IV-O)

V.10

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

Homeland Security

November 15, 2007

MEMORANDUM FOR: Richard L. Skinner, Inspector General

FROM: David L. Norquist, Chief Financial Officer

SUBJECT: FY 2007 Financial Statement Audit

This memo is our response to the Independent Public Accountant's audit of our balance sheets as of September 30, 2007 and 2006, and the related statement of custodial activities for the years then ended. We agree with the Independent Public Accountant's conclusions.

I would like to thank you for your efforts and the dedication shown by your staff and the Independent Public Accountant in working with the Department to improve financial management. Although the auditor's report on internal controls and compliance indicates that DHS still faces serious financial management challenges, I am encouraged to note that significant progress was made this year. This progress has been made possible through the tireless effort of many throughout the Department to implement meaningful corrective actions and develop strong processes and internal controls.

We are currently updating our plans to address the challenges identified by the auditors, as well as those noted by management during our A-123 assessment. Our plans will focus on sustaining progress at the components that have corrected weaknesses, as well as supporting corrective action plans in areas where weaknesses remain. Two particular challenges for the upcoming year will be the U.S. Coast Guard and the Federal Emergency Management Agency.

Financial management at DHS has come a long way. I am inspired by the extraordinary efforts of the Department's dedicated staff, and am most appreciative of the partnership we have forged with your office. Together we will continue to improve financial management and grow a cadre of leaders ready to address the mission challenges of the next decade.

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 Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative and Intergovernmental 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 Program Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

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

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

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

Financial Statements

Department of Homeland Security
Balance Sheets
As of September 30, 2007 and 2006
(In Millions)

	2007 (Unaudited)	2006 (Unaudited) (Restated)
ASSETS		
Intragovernmental		
Fund Balance with Treasury (Notes 2 and 3)	$56,185	$59,569
Investments, Net (Note 5)	2,778	634
Accounts Receivable, Net (Note 6)	278	247
Other (Note 13)		
Advances and Prepayments	2,887	2,913
Other (Note 2)	176	411
Total Intragovernmental	**$62,304**	**$63,774**
Cash and Other Monetary Assets (Notes 2 and 4)	321	99
Accounts Receivable, Net (Notes 2 and 6)	760	1,181
Taxes, Duties, and Trade Receivables, Net (Notes 2 and 7)	1,937	1,755
Direct Loans, Net (Note 8)	-	161
Inventory and Related Property, Net (Note 9)	632	677
General Property, Plant, and Equipment, Net (Notes 2 and 11)	12,275	11,151
Other (Note 13)		
Advances and Prepayments	567	551
TOTAL ASSETS	**$78,796**	**$79,349**
Stewardship Property, Plant, and Equipment (Note 12)		
LIABILITIES		
Intragovernmental		
Accounts Payable	$2,066	$1,907
Debt (Note 15)	18,153	17,446
Other (Note 18)		
Due to the General Fund	2,085	1,809
Accrued FECA Liability	355	339
Other	245	187
Total Intragovernmental	**$22,904**	**$21,688**
Accounts Payable	3,003	2,629
Federal Employee and Veterans' Benefits (Note 16)	34,910	32,278
Environmental and Disposal Liabilities (Note 17)	275	245
Other (Notes 18, 19, 20, and 21)		
Accrued Payroll and Benefits	1,553	1,362
Deferred Revenue and Advances from Others	2,727	2,188
Unliquidated Antidumping and Countervailing Duties	514	34
Insurance Liabilities	1,508	3,567

Department of Homeland Security
Balance Sheets
As of September 30, 2007 and 2006
(In Millions)

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Refunds and Drawbacks	131	5,593
Other	1,408	1,205
Total Liabilities	**$68,933**	**$70,789**
Commitments and contingencies (Notes 19, 20, and 21)		
NET POSITION		
Unexpended Appropriations		
Unexpended Appropriations-Other Funds	$49,003	$48,816
Cumulative Results of Operations		
Cumulative Results of Operations-Earmarked Funds (Note 22)	(16,236)	(19,337)
Cumulative Results of Operations-Other Funds	(22,904)	(20,919)
Total Net Position	**$9,863**	**$8,560**
TOTAL LIABILITIES AND NET POSITION	**$78,796**	**$79,349**

The accompanying notes are an integral part of these statements.

Department of Homeland Security
Statements of Net Cost
For the Years Ended September 30, 2007 and 2006
(In Millions)

Directorates and Other Components (Note 23 and 24)	2007 (Unaudited)	2006 (Unaudited) (Restated)
U.S. Customs and Border Protection		
Gross Cost	$8,198	$7,135
Less Earned Revenue	(157)	(153)
Net Cost	**8,041**	**6,982**
U.S. Coast Guard		
Gross Cost	10,564	10,011
Less Earned Revenue	(492)	(424)
Net Cost	**10,072**	**9,587**
U.S. Citizenship and Immigration Services		
Gross Cost	1,731	1,588
Less Earned Revenue	(1,659)	(1,729)
Net Cost	**72**	**(141)**
Federal Emergency Management Agency		
Gross Cost	14,272	28,845
Less Earned Revenue	(2,842)	(2,469)
Net Cost	**11,430**	**26,376**
Federal Law Enforcement Training Center		
Gross Cost	402	312
Less Earned Revenue	(40)	(33)
Net Cost	**362**	**279**
National Protection and Programs Directorate		
Gross Cost	855	743
Less Earned Revenue	-	(1)
Net Cost	**855**	**742**
U.S. Immigration and Customs Enforcement		
Gross Cost	4,891	4,500
Less Earned Revenue	(900)	(857)
Net Cost	**3,991**	**3,643**

Department of Homeland Security
Statements of Net Cost
For the Years Ended September 30, 2007 and 2006
(In Millions)

Directorates and Other Components (Note 23 and 24)	**2007 (Unaudited)**	**2006 (Unaudited) (Restated)**
Office of Health Affairs		
Gross Cost	5	53
Less Earned Revenue	-	-
Net Cost	**5**	**53**
Departmental Operations and Other		
Gross Cost	1,204	852
Less Earned Revenue	(3)	(2)
Net Cost	**1,201**	**850**
U.S. Secret Service		
Gross Cost	1,689	1,471
Less Earned Revenue	(16)	(18)
Net Cost	**1,673**	**1,453**
Science and Technology Directorate		
Gross Cost	987	843
Less Earned Revenue	(14)	-
Net Cost	**973**	**843**
Transportation Security Administration		
Gross Cost	6,439	6,001
Less Earned Revenue	(2,299)	(2,477)
Net Cost	**4,140**	**3,524**
NET COST OF OPERATIONS (Note 23 and 24)	**$42,815**	**$54,191**

The accompanying notes are an integral part of these statements.

Department of Homeland Security
Statements of Changes in Net Position
For the Year Ended September 30, 2007
(In Millions)

	2007 (Unaudited)			
	Earmarked Funds	All Other Funds	Eliminations	Consolidated Total
Cumulative Results of Operations				
Beginning Balances	$(19,337)	$(20,919)	$ -	$(40,256)
Adjustments:				
Change in Accounting Method (Note 36)	693	-	-	693
Beginning Balance, as Adjusted	**(18,644)**	**(20,919)**	-	**(39,563)**
Budgetary Financing Sources				
Appropriations used	-	39,074	-	39,074
Non-exchange Revenue	3,603	6	-	3,609
Donations and Forfeitures of Cash and Cash Equivalents	2	-	-	2
Transfers in/out Without Reimbursement	(1,980)	1,855	-	(125)
Other	-	(174)	-	(174)
Other Financing Sources (Non-Exchange)				
Donations and forfeitures of property	-	4	-	4
Transfers in/out reimbursement	-	9	-	9
Imputed financing	2	848	11	839
Total Financing Sources	1,627	41,622	11	43,238
Net Cost of Operations	781	(43,607)	(11)	(42,815)
Net Change	2, 408	(1,985)	-	423
Cumulative Results of Operations	**(16,236)**	**(22,904)**	-	**(39,140)**
Unexpended Appropriations				
Beginning Balance	-	48,816	-	48,816
Adjustments:				
Adjustments (Note 37)	-	37	-	37
Beginning Balance, as Adjusted	-	**48,853**	-	**48,853**
Budgetary Financing Sources				
Appropriations Received (Note 31)	-	39,520	-	39,520
Appropriations Transferred in/out	-	295	-	295
Other Adjustments	-	(591)	-	(591)
Appropriations Used	-	(39,074)	-	(39,074)
Total Budgetary Financing Sources	-	150	-	150
Total Unexpended Appropriations	-	**49,003**	-	**49,003**
NET POSITION	**$(16,236)**	**$26,099**	**$ -**	**$9,863**

The accompanying notes are an integral part of these statements.

Department of Homeland Security
Statements of Changes in Net Position
For the Year Ended September 30, 2006
(In Millions)

	2006 (Unaudited) (Restated)		
	Earmarked Funds	All Other Funds	Consolidated Total
Cumulative Results of Operations			
Beginning Balances	$(22,715)	$(19,132)	$(41,847)
Adjustments:			
Corrections of Errors (Note 34)	-	(588)	(588)
Beginning Balance, as Adjusted	(22,715)	(19,720)	(42,435)
Budgetary Financing Sources			
Appropriations Used	-	52,872	52,872
Non-exchange Revenue	2,516	11	2,527
Donations and Forfeitures of Cash and Cash Equivalents	68	-	68
Transfers in/out without Reimbursement	(1,296)	1,657	361
Other	2	(198)	(196)
Other Financing Sources (Non-Exchange)			
Donations and Forfeitures of Property	-	6	6
Transfers in/out Reimbursement	-	30	30
Imputed Financing	2	700	702
Total Financing Sources	1,292	55,078	56,370
Net Cost of Operations	2,086	(56,277)	(54,191)
Net Change	3,378	(1,199)	2,179
Cumulative Results of Operations	**(19,337)**	**(20,919)**	**(40,256)**
Unexpended Appropriations			
Beginning Balance	-	87,131	87,131
Adjustments:			
Corrections of Errors (Note 34)	-	676	676
Beginning Balance, as Adjusted	**-**	**87,807**	**87,807**
Budgetary Financing Sources			
Appropriations Received (Note 31 and 36)	-	39,529	39,529
Appropriations Transferred in/out	-	(573)	(573)
Other Adjustments	-	(25,075)	(25,075)
Appropriations Used	-	(52,872)	(52,872)
Total Budgetary Financing Sources	-	(38,991)	(38,991)
Total Unexpended Appropriations	**-**	**48,816**	**48,816**
NET POSITION	**$(19,337)**	**$27,897**	**$8,560**

The accompanying notes are an integral part of these statements.

Department of Homeland Security
Statements of Budgetary Resources
For the Years Ended September 30, 2007 and 2006
(In Millions)

	2007 (Unaudited)		2006 (Unaudited) (Restated)	
	Budgetary	**Non-Budgetary Credit Reform Financing Accounts**	**Budgetary**	**Non-Budgetary Credit Reform Financing Accounts**
BUDGETARY RESOURCES				
Unobligated Balance, Brought Forward, October 1 (Note 37)	$17,313	$ -	$56,905	$26
Recoveries of Prior Year Unpaid Obligations	4,938	-	3,740	-
Budget Authority:				
Appropriations (Note 31)	46,491	-	45,748	-
Borrowing Authority	-	-	17,500	629
Spending Authority from Offsetting Collections:				
Earned:				
Collected	9,963	336	9,093	478
Change in Receivables from Federal Sources	(5)	-	38	-
Change in Unfilled Customer Orders:				
Advances Received	78	-	(541)	-
Without Advance From Federal Sources	707	(122)	186	481
Expenditure Transfers from Trust Funds	47	-	49	-
Subtotal	57,281	214	72,073	1,588
Non-expenditure Transfers, net; Anticipated and Actual	787	-	(228)	-
Temporarily Not Available Pursuant to Public Law	-	-	(24)	-
Permanently Not Available	(671)	(70)	(25,172)	(334)
TOTAL BUDGETARY RESOURCES	**$79,648**	**$144**	**$107,294**	**$1,280**
STATUS OF BUDGETARY RESOURCES				
Obligations Incurred: (Note 25)				
Direct	$56,669	$13	$85,503	$1,280
Reimbursable	5,320	-	4,487	-
Subtotal	61,989	13	89,990	1,280
Unobligated Balance:				
Apportioned	9,141	12	11,854	-
Exempt from Apportionment	97	-	80	-
Subtotal	9,238	12	11,934	-
Unobligated Balance Not Available	8,421	119	5,370	-
TOTAL STATUS OF BUDGETARY RESOURCES	**$79,648**	**$144**	**$107,294**	**$1,280**

Department of Homeland Security
Statements of Budgetary Resources
For the Years Ended September 30, 2007 and 2006
(In Millions)

	2007 (Unaudited)		2006 (Unaudited) (Restated)	
	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	$43,036	$642	$40,430	-
Uncollected Customer Payments from Federal Sources, Brought Forward, October 1	(2,069)	(482)	(1,845)	-
Total Unpaid Obligated Balance, net (Note 37)	40,967	160	38,585	-
Obligations Incurred, net	61,989	13	89,990	1,280
Gross Outlays	(56,293)	(175)	(83,675)	(639)
Obligated Balance Transferred, net				
Actual Transfers, Unpaid Obligations	(18)	-	-	-
Total Unpaid Obligated Balance Transferred, net	(18)	-	-	-
Recoveries of Prior Year Unpaid Obligations, Actual	(4,938)	-	(3,740)	-
Change in Uncollected Customer Payments from Federal Sources	(702)	121	(224)	(481)
Obligated Balance, net, End of Period				
Unpaid Obligations	43,775	480	43,005	642
Uncollected Customer Payments from Federal Sources	(2,770)	(361)	(2,069)	(482)
Total, Unpaid Obligated Balance, net, End of Period	**$41,005**	**$119**	**$40,936**	**$160**
NET OUTLAYS				
Gross Outlays	$56,293	$175	$83,675	$639
Offsetting Collections	(10,090)	(336)	(8,601)	(478)
Distributed Offsetting Receipts	(4,952)	-	(4,821)	-
NET OUTLAYS	**$41,251**	**$(161)**	**$70,253**	**$161**

The accompanying notes are an integral part of these statements.

Department of Homeland Security
Statements of Custodial Activity
For the Years Ended September 30, 2007 and 2006
(In Millions)

	2007 (Unaudited)	2006 (Unaudited)
Revenue Activity		
Sources of Cash Collections:		
Duties	$26,658	$24,730
User Fees	1,732	1,524
Excise Taxes	2,626	2,427
Fines and Penalties	60	64
Interest	15	12
Miscellaneous	25	178
Total Cash Collections	31,116	28,935
Accrual Adjustments	5,723	(5,371)
Total Custodial Revenue	**36,839**	**23,564**
Disposition of Collections		
Transferred to Others:		
Federal Entities:		
U.S. Department of Agriculture	148	127
U.S. Department of Labor	193	189
U.S Department of State	46	44
National Science Foundation	107	105
Treasury General Fund Accounts	23,591	27,206
Other Federal Agencies	21	17
Non-Federal Entities:		
Government of Puerto Rico	14	14
Government of the U.S. Virgin Islands	5	6
Other Non-Federal Entities	20	9
(Increase)/Decrease in Amounts Yet to be Transferred	5,712	(5,371)
Refunds and Drawbacks (Notes 18 and 32)	6,922	1,160
Retained by the Department	60	58
Total Disposition of Custodial Revenue	**36,839**	**23,564**
Net Custodial Activity	**$ -**	**$ -**

The accompanying notes are an integral part of these statements.

Notes to the Financial Statements (Unaudited)

Table of Contents for Notes to the Financial Statements (unaudited)

Notes to the Financial Statements (Unaudited)

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)*, *P.L. 107-296*, dated March 25, 2002, as an executive department of the U.S. Federal Government. DHS's mission is to lead the national effort to secure America. This mission includes the prevention and deterrence of terrorist attacks and protection against, and response to, threats and hazards to the Nation and critical infrastructure from dangerous people and goods. Additionally, DHS's mission is to ensure the safety and security of borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce. In support of DHS's mission, the Secretary has established additional goals to build a nimble, effective emergency response system and a culture of preparedness, and to strengthen and unify DHS operations and management. The Department is composed of the following financial reporting Components[1]:

- **Federal Emergency Management Agency** (**FEMA**)
- **National Protection and Programs Directorate (NPPD)**
- **Science and Technology Directorate (S&T)**
- **U.S. Citizenship and Immigration Services (USCIS)**
- **U.S. Coast Guard (USCG)**
- **U.S. Customs and Border Protection (CBP)**
- **Federal Law Enforcement Training Center (FLETC)**
- **U.S. Immigration and Customs Enforcement (ICE),** including the Federal Protective Services (FPS)
- **U.S. Secret Service (USSS)**
- **Transportation Security Administration (TSA)**
- **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), Office of Intelligence and Analysis, and the Office of Operations Coordination

On October 4, 2006, the President signed the *Post-Katrina Emergency Management Reform Act of 2006 (P.L. 109-295)* (the PKEMR Act) which is codified at Title VI of the Department's FY 2007 Appropriations Act (P.L. 109-295). The PKEMR Act established various positions within DHS, brought additional functions into FEMA, and created and reallocated functions to other Components within DHS. In addition, pursuant to the Secretary's Authority under Section 872, *Reorganization Authority of the Homeland Security Act of 2002* (the Reorganization Authority under the HSA), DHS has made certain other organizational changes outside of the PKEMR Act. All changes as a result of the PKEMR Act and the Reorganization Authority under the HSA were effective as of March 31, 2007, unless otherwise noted.

[1] Financial reporting components are to be distinguished from direct report components.

As a result of the PKEMR Act:

- FEMA was expanded to include some programs from the Preparedness Directorate, including: the Office of Grants and Training (G&T); the Radiological Emergency Preparedness Program (REPP); and the United States Fire Administration (USFA).
- A new Office of Emergency Communications (OEC) was established and reports directly to the Assistant Secretary for Cyber Security and Communication within NPPD.

Pursuant to the Reorganization Authority under the HSA:

- The Preparedness Directorate was renamed the National Protection and Programs Directorate (NPPD). The new NPPD includes the following offices: Office of the Under Secretary, Office of Infrastructure Protection, Office of Risk Management and Analysis, Office of Cyber Security and Communications, Office of Intergovernmental Programs, and the US-VISIT program.
- The Office of Health Affairs (OHA) was established and is comprised of the Office of the Chief Medical Officer and offices responsible for carrying out the Department's biodefense responsibilities.

During FY 2007, the Department began reporting the Sport Fish Restoration and Boating Trust Fund (SFRBTF) in the applicable financial statements and footnotes based on the updated A-136 requirements for the reporting of mixed funds (partially earmarked and partially non-earmarked). The SFRBTF is a Treasury managed trust fund. During FY 2006 and prior, the SFRBTF was reported by the Department of the Interior.

B. Basis of Presentation

These financial statements are prepared to report the consolidated financial position, net cost of operation, changes in net position, custodial activity, and the combined budgetary resources of the Department pursuant to the *Government Management Reform Act of 1994 (P.L. 103-356)* and *Chief Financial Officers Act of 1990 (P.L 101-576)*, as amended by the *Reports Consolidation Act of 2000 (P.L. 106-531)*.

The Department's financial statements have been prepared from the accounting records of the Department in conformity with U.S. Generally Accepted Accounting Principles (GAAP), and the Office of Management and Budget (OMB) Circular A-136, *Financial Reporting Requirements*. GAAP for Federal entities are the standards prescribed by the Federal Accounting Standards Advisory Board (FASAB), 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 accruals of revenue from other Federal entities and intragovernmental costs are payments or 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, that 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.

Reclassifications. The PKEMR Act and the Reorganization Authority under HSA caused changes affecting the definition of the Reporting Entity. Therefore, certain reclassifications were made to the FY 2006 financial statements and associated footnotes to conform with the FY 2007 presentation.

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

Management has made certain estimates and assumptions in the reporting of assets, liabilities, revenues, expenses, obligations incurred, spending authority from offsetting collections, and note disclosures in the financial statements. Actual results could differ from these 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; depreciation; subsidy re-estimates; deferred revenues; National Flood Insurance Program (NFIP) insurance liability; actuarial workers compensation assumptions; 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 that the Department has the authority to use in its operations. The authority to use funds in an entity's operations means that 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 are not available for use by the Department. An example of a non-entity asset is Fund Balance with Treasury which consists of special and deposit funds, permanent appropriations, and miscellaneous receipts that are available to pay non-entity liabilities.

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 fiscal year-end.

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 not maintain cash in commercial bank accounts. For FEMA, certain receipts are received and processed by insurance companies. The remainder of the receipts and disbursements are processed by Treasury.

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

H. Investments, Net

Investments consist of U.S. Government non-marketable 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 represent amounts due to the Department from other Federal agencies and the public. Intragovernmental accounts receivable generally 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 results from various immigration and user fees, premiums and restitution 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. Interest due on past due receivables is fully reserved until collected.

For additional information, see Note 6, Accounts Receivable, Net.

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 tasked with mission assignments.

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 and other grant activity. Advances are expensed as they are used by the recipients. At year-end, the amount, if any, of grant funding unexpended and a grant payable is estimated based on cash transactions reported by the grant administrator.

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 any local government which has suffered a substantial loss of tax and other revenues as a result of a major disaster and which demonstrates a need for Federal financial assistance in order to perform its governmental functions. Under the program, FEMA transacts direct loans to local governments who 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) (P.L. 101-508)*. Under FCRA, for direct loans disbursed during a fiscal year, the corresponding receivable is adjusted for subsidy costs. Subsidy costs are an estimated long-term cost 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 CFR Section 206.366.

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

L. Inventory and Related Property, Net

OM&S are tangible personal property consumed during normal operations. Department OM&S consists primarily of goods consumed during the service of vessels and aircraft. OM&S are valued based on an average unit cost, weighted moving average method, or on actual prices paid. OM&S are expensed when consumed or issued for use. Excess, obsolete, and unserviceable OM&S are stated at net realizable value net of an allowance, which is based on the condition of various asset categories, as well as historical experience with using and disposing of such assets.

Inventory is tangible personal property that is held for sale, in the process of production for sale, or to be consumed in the production of goods for sale, or in the provision of services for fees. Department inventories consist primarily of USCG Supply Fund’s uniform clothing, subsistence provisions, retail stores, general stores, technical material and fuel, and USCG Yard Fund’s ship repair and general inventory. Inventories on hand at year-end are stated at cost using standard price/specific identification, last acquisition price, or weighted 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.

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, including water, meals, cots, and blankets. The goods are valued at historical cost.

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

M. Seized and Forfeited Property

The Department’s prohibited seized property results primarily from criminal investigations and passenger/cargo processing. Seized property falls into two categories, prohibited and non-prohibited. Prohibited seized property includes illegal drugs, contraband, and counterfeit items that cannot legally enter into the commerce of the United States; non-prohibited 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 are 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. Non-prohibited forfeited property is transferred to the Treasury Forfeiture Fund.

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

N. General Property, Plant, and Equipment, Net

The Department's property, plant, and equipment (PP&E) consists of aircraft, vessels, vehicles, land, structures, facilities, capital leases, 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 completed, and 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 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 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 software (COTS), 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. Capitalized costs for internally developed software include the full cost (direct and indirect) incurred during the software development phase.

The schedule of capitalization thresholds shown below is a summary of the range of capitalization rules in place from the legacy agencies that comprised the Department. In accordance with DHS policy, Components were allowed to continue using their legacy thresholds and capitalization rules until a more comprehensive approach is developed that takes into account the vast differences in Component size and asset usage.

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	Regardless of cost to $100,000	Not Applicable
Improvements to Land	Regardless of cost to $100,000	3 years to 50 years
Buildings and improvement	Regardless of cost to $200,000	2 years to 50 years
Equipment and capital leases	$5,000 to $200,000	2 years to 65 years
Software	$5,000 to $750,000	2 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 and stewardship land which 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. The Department's heritage assets consist primarily of buildings and structures owned by USCG. 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 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. The Department's multi-use heritage assets consist primarily of buildings and structures owned by CBP and USCG. DHS depreciates its multi-use heritage assets.

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

P. Liabilities

Liabilities represent the probable and measurable future outflow or other sacrifice 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 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, and there is no certainty that the appropriations will be enacted. The U.S. Government, acting in its sovereign capacity, can abrogate liabilities of the Department arising from other than contracts.

Q. Contingent Liabilities

Certain conditions exist as of the date of the financial statements, which may result in a loss to the government, but which will only be resolved when one or more future events occur or fail to occur. The Department recognizes a loss contingency when the future outflow or other sacrifice of resources is probable and reasonably estimable. The Department discloses a loss contingency in the notes to the financial statements when the conditions for liability recognition are not met, but a loss from the outcome of future events is more than remote.

For more 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 at the time the cleanup requirement is identified. DHS does not prorate a cleanup cost over the life of these PP&E. However, the estimate may be subsequently adjusted for material changes due to inflation/deflation or changes in regulations, plans, or technology. The applicable costs of decommissioning DHS's existing and future vessels are considered cleanup costs.

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

R. Grants Liabilities

The Department awards grants and cooperative agreements to Federal, State, and local governments, universities, non-profit organizations, and private sector companies for the purpose of building the 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 other Department-related activities. The Department estimates the year-end grant accrual for unreported grantee expenditures using historical disbursement data. Grants 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 known as the NFIP, which is managed by FEMA. The insurance liability represents an estimate of NFIP losses that are unpaid at the Balance Sheet date. Although the insurance underwriting operations believes the liability for unpaid losses and loss adjustment expenses is reasonable and adequate in the circumstances, 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.

For more information see 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. The Department's obligations for NFIP and DADLP are financed by principal repayments, flood premiums, and map collection fees.

The Department has borrowing authority for NFIP and DADLP, and may obtain additional borrowing authority if approved.

For more information see Note 15, Debt.

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 as an accrued payroll and benefits liability. 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 non-vested leave are not earned benefits. Accordingly, non-vested leave is expensed when used.

Federal Employees Compensation Act. The *Federal Employees Compensation Act (FECA) (P.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 (Labor), which pays valid claims and subsequently seeks reimbursement from the Department for these paid claims.

The FECA liability consists of two components. The first component, accrued FECA liability, is based on actual claims paid by Labor but not yet reimbursed by the Department. The Department reimburses Labor for the amount of actual claims as funds are appropriated for this purpose. There is generally a two to three-year time period between payment by Labor and reimbursement to Labor by the Department. As a result, the Department recognizes an intragovernmental liability for the actual claims paid by Labor and to be reimbursed by the Department.

The second component, actuarial FECA liability, is the estimated liability for future benefit payments and is recorded as a component of Federal Employee and Veterans' Benefits. This liability includes death, disability, medical, and miscellaneous costs. Labor determines this component 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 ten 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. For more information on the Accrued FECA Liability, Accrued Payroll and Accrued Leave, see Note 18, Other Liabilities.

V. Federal Employee and Veterans' Benefits

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 Office of Personnel Management (OPM) rather than the Department.

Most U.S. Government employees of DHS hired prior to January 1, 1984, participate in the Civil Service Retirement System (CSRS), to which the Department contributes 7 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 11.2 percent of base pay for regular FERS employees and 23.8 percent for law enforcement agents. A primary feature of FERS is that it also offers a defined contribution plan to which the Department automatically contributes 1 percent of base pay and matches employee contributions up to an additional 4 percent of base pay. The Department also contributes the employer's Social Security matching share for FERS participants.

Similar to CSRS and FERS, OPM rather than the Department reports the liability for future payments to retired employees who participate in the Federal Employees Health Benefits Program (FEHB) and Federal Employees Group Life Insurance Program (FEGLI). The Department is required to report the full annual cost of providing these other retirement benefits (ORB) for its retired employees as well as reporting contributions made for active employees. In addition, the Department recognizes an expense and liability for other post employment benefits (OPEB), which includes 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 USCG Military Retirement System (MRS) is a defined benefit plan that covers both retirement pay and health care benefits for all retired active duty and reserve military members of the USCG. The plan is funded through annual appropriations and, as such, is a pay-as-you-go system. 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 the future cost of benefits. Current period expense is computed using the aggregate entry age normal actuarial cost method.

A portion of the accrued MRS liability is for the health care of non-Medicare eligible and Medicare eligible retirees/survivors. The Department of Defense (DOD) is the administrative entity for the Medicare eligible fund (Fund), and in accordance with SFFAS No. 5, is required to recognize the liability on the Fund's financial statements. The USCG makes annual payments to the Fund for current active duty members. Benefits for USCG members who retired prior to the establishment of the Fund are provided by payments from the Treasury to the Fund. The future cost and liability of the Fund is determined using claim factors and claims cost data developed by DOD, adjusted for USCG retiree and actual claims experience. The USCG uses the current year actual costs to project costs for all future years.

Post-employment Military Travel Benefit. USCG uniformed service members are entitled to travel and transportation allowances for travel performed or to be performed under orders upon separation from the service, including the member's termination, retirement, permanent disability, or pre-retirement death in service. These allowances are 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.

USCG recognizes an expense and a liability for this OPEB when a future outflow or other sacrifice of resources is probable and measurable on the basis of events occurring on or before the reporting date. The OPEB liability is measured at the present value of future payments, which requires USCG to estimate the amount and timing of future payments, and to discount the future outflow using the Treasury borrowing rate for securities of similar maturity to the period over which the payments are made.

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, which 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)* or other statutes authorizing reimbursement. Prices for goods and services sold to other Federal Government agencies are generally limited to the recovery of direct cost.

Allocation Transfers. The Department is a party to allocation transfers with other Federal agencies as both a transferring (parent) entity and/or 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. Generally, 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 (HHS). DHS receives allocation transfers, as the child, from the General Services Administration (GSA), the 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 (P.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 Sheets until earned. Information and specific examples of deferred revenue include:

- Fees for flood mitigation products and services, such as insurance provided through FEMA's NFIP, are established at rates necessary to sustain a self-supporting program. 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. A major portion of the revenue received for certain applicant types is deferred and not considered earned until the application is adjudicated.

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 Revenue. Non-entity revenue and refunds are reported on the Statements 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 and USCIS 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 Title 19 United States Code (U.S.C.); nonimmigrant petition fees under Title 8 U.S.C., and excise taxes under Title 26 U.S.C. CBP also enforces over 400 laws and regulations some of which require the collection of fees or the imposition of fines and penalties pursuant to other Titles within the U.S.C. or Code of Federal Regulations (C.F.R.).

CBP assesses duties, taxes, and fees on goods and merchandise brought into the United States from foreign countries. 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. The custodial revenue is recorded at the time of collection. These revenue collections primarily result from current fiscal year activities. Generally, CBP records an equal and offsetting liability due to the Treasury General Fund for amounts recognized as non-entity tax and trade receivable and custodial revenue. 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. Fees collected by USCIS for nonimmigrant petitions must be submitted with the petition. 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 Statement of Custodial Activity. 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 32, Custodial Activities.

Y. Taxes

The Department, as a Federal agency, is not subject to Federal, State, or local income taxes and accordingly, no provision for income taxes has been recorded in the accompanying financial statements.

Z. Restatements

In FY 2007, the Department restated certain FY 2006 balances. For additional information see Note 34, Restatements.

2. Non-Entity Assets

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Intragovernmental:		
Fund Balance with Treasury	$1,130	$ 5,949
Due From Treasury	176	411
Total Intragovernmental	1,306	6,360
Cash and Other Monetary Assets	48	46
Accounts Receivable, Net	17	19
Taxes, Duties, and Trade Receivables, Net	1,937	1,755
General Property, Plant, and Equipment, Net	-	3
Total Public	2,002	1,823
Total Non-Entity Assets	3,308	8,183
Total Entity Assets	75,488	71,166
Total Assets	**$78,796**	**$ 79,349**

Non-entity Fund Balance with Treasury consists of special and deposit funds, permanent and indefinite appropriations, and miscellaneous receipts that are available to pay non-entity liabilities included in the Balance Sheet. Non-entity Fund Balance with Treasury at September 30, 2007, includes (in special fund) balances for Injured Domestic Industries (IDI) as defined in Note 18. Non-entity Fund Balance with Treasury at September 30, 2006, includes (in deposit fund) approximately $5.2 billion of unliquidated duties collected by CBP on imports of Canadian Softwood lumber. During FY 2007, approximately $5 billion in refund disbursements were paid for antidumping and countervailing duties on Canadian Softwood lumber imports. All non-entity Fund Balance with Treasury is considered restricted cash. These assets offset accrued liabilities at September 30, 2007, and 2006 (see Notes 3 and 18).

Non-entity receivables due from Treasury represent an estimate of duty, tax, and/or fee refunds and drawbacks that will be reimbursed by a permanent and indefinite appropriation account and will be used to pay estimated refunds and drawbacks payable. Duties and taxes receivable from the public represents amounts due from importers for goods and merchandise imported to the United States, and upon collection, will be available to pay the accrued intragovernmental liability due to the Treasury General Fund of $2.1 billion and $1.8 billion at September 30, 2007 and 2006, respectively (see Notes 7 and 18).

3. Fund Balance with Treasury

A. Fund Balance with Treasury

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Appropriated Funds	$50,764	$50,899
Trust Funds	60	35
Revolving, Public Enterprise, and Working Capital Funds	969	216
Special Funds	3,563	2,909
Deposit Funds	829	5,510
Total Fund Balance with Treasury	**$56,185**	**$59,569**

Appropriated funds consist of amounts appropriated annually by Congress to fund the operations of the Department. Appropriated funds included clearing funds totaling $105 million and $110 million at September 30, 2007 and 2006, respectively, which represent reconciling differences with Treasury balances.

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, generally to offset the cost of expanding border and port enforcement activities and oil spill related claims and activities.

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. 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 include funds designated for specific purposes including the disbursement of non-entity monies received in connection with antidumping and countervailing duty orders due to qualifying 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. At September 30, 2006 the majority of the deposit fund balance relates to unliquidated antidumping and countervailing duties collected by CBP, mostly related to Canadian Softwood lumber. During FY 2007, the deposit fund balance related to antidumping and countervailing duties on Canadian Softwood lumber imports was liquidated, which accounts for the decrease to the deposit fund.

B. Status of Fund Balance with Treasury

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Budgetary Status		
Unobligated Balances:		
Available	$9,250	$11,934
Unavailable	8,540	5,370
Obligated Balance Not Yet Disbursed	41,124	41,096
Total Budgetary Status	58,914	58,400
Reconciling Adjustments:		
Receipt, Clearing, and Deposit Funds	941	5,629
Borrowing Authority	(3,465)	(4,230)
Investments	(2,767)	(628)
Receivable Transfers and Imprest Fund	(130)	(97)
Receipts unavailable for obligation	1,566	495
Authority Temporarily Precluded from Obligation	25	-
Accounts Payable - SFRBTF	1,101	-
Total Fund Balance with Treasury	**$56,185**	**$59,569**

Adjustments required to reconcile the budgetary status to non-budgetary Fund Balance with Treasury as reported in the accompanying Balance Sheets are as follows:

- Receipt, clearing, and deposit funds represent amounts on deposit with Treasury that have no budget status at September 30, 2007 and 2006. Included in the 2006 adjustments for deposit funds are restricted balances for unliquidated antidumping and countervailing duties non-entity funds and receipts that are not available for obligation. During FY 2007, the deposit fund balance related to antidumping and countervailing duties on Canadian Softwood lumber imports was liquidated which accounts for the decrease to the reconciling adjustment.
- Borrowing authority is in budgetary status for use by FEMA for disaster relief purposes and Community disaster loans.
- Budgetary resources have investments included; however, the money has been moved from the Fund Balance with Treasury asset account to Investments. The increase in this reconciling adjustment relates to the addition of SFRBTF investments in FY 2007, as well as the accounts payable transfers above.

- Receivable transfers of currently invested balances increase the budget authority at the time the transfer is realized and obligations may be incurred before the actual transfer of funds.
- Imprest funds represent monies moved from Fund Balance with Treasury to Cash and Other Monetary Assets with no change in the budgetary status.
- Receipts immediately upon collection are unavailable for obligation. The receipts are not available for obligation until a specified time in the future. The increase in this reconciling adjustment relates to the addition of SFRBTF.

Portions of the Unobligated Balances Available, Unavailable and Obligated Balance Not Yet Disbursed contain CBP's user fees of $730 million and $761 million at September 30, 2007 and 2006, respectively, which is restricted by law in its use to offset costs incurred by CBP. Further, the Unobligated Balances Available include appropriations received in the Disaster Relief Fund for Hurricane Katrina. As of September 30, 2007 and 2006, this fund has an unobligated balance available of $4.4 billion and $5.5 billion, respectively.

Portions of the Unobligated Balance Unavailable include amounts appropriated in prior fiscal years that are not available to fund new obligations. However, it can be used for upward and downward adjustments for existing obligations in future years. The increase in Unobligated Balances Unavailable relates to the increase in appropriations received in the Border Security Infrastructure and Technology Fund and the cancellation of a contract and a reimbursable agreement with HHS.

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.

4. Cash and Other Monetary Assets

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Cash	$282	$62
Seized Monetary Instruments	39	37
Total Cash and Other Monetary Assets	**$321**	**$99**

DHS Cash includes cash held by others, including the net balance maintained by insurance companies for flood insurance premiums received from policyholders, less amounts paid for insured losses; imprest funds; and undeposited cash, which represents fees collected but not yet deposited. An announced increase in immigration application fees and a demand for preference visa categories, which became available under the Department of State's July 2007 Visa Bulletin, combined to create a large increase in immigration applications, resulting in an increase in immigration application fees collected but not yet deposited. Seized Monetary Instruments are held until disposition and relate primarily to gold coins seized at the end of FY 2004. As of September 30, 2007 and 2006, restricted cash and other monetary assets is $48 and $46 million, respectively.

5. Investments, Net

Investments at September 30, 2007, consisted of the following (in millions) (unaudited):

Type of Investment:	Amortization Method	Cost	Amortized (Premium) Discount	Investments, Net (Unaudited)	Market Value Disclosure
Intragovernmental Securities:					
Oil Spill Liability Trust Fund	Effective interest method	$925	$(7)	$918	N/A
Sport Fish Restoration Boating Trust Fund	Effective interest method	1,841	5	1,846	N/A
Total Non-Marketable		2,766	(2)	2,764	N/A
Non-Marketable, Market-Based	Straight line method	14	-	14	14
Total Investments, Net		**$2,780**	**$(2)**	**$2,778**	**N/A**

Investments at September 30, 2006, consisted of the following (in millions) (unaudited and restated):

Type of Investment:	Amortization Method	Cost	Amortized (Premium) Discount	Investments, Net (Unaudited)	Market Value Disclosure
Intragovernmental Securities:					
Oil Spill Liability Trust Fund	Effective interest method	$610	(15)	$595	N/A
Total Non-Marketable		610	(15)	595	N/A
Non-Marketable, Market-Based	Straight line method	39	-	39	39
Total Investments, Net		**$ 649**	**($15)**	**$ 634**	**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 and General Gift Fund) for USCG. 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 USCG as evidence of its receipts. Treasury securities associated with earmarked are an asset to USCG and a liability to the Treasury. Because Treasury and DHS are both parts of the Federal Government, these assets and liabilities offset each other from the standpoint of the Federal Government as a whole. For this reason, these funds do not represent an asset or a liability in the U.S. Government-wide financial statements.

Treasury securities provide USCG with authority to draw upon the Treasury to make future benefit payments or other expenditures. When the USCG requires redemption of these securities to make expenditures, the Federal Government finances those expenditures out of accumulated cash balances, by raising taxes or other receipts, borrowing from the public or repaying less debt, or by curtailing other expenditures. This is the same way that the Federal Government finances all other expenditures.

The change in accounting method for SFRBTF, as described in Note 36, resulted in the net investments line on the September 30, 2007 Balance Sheet to increase by approximately $1.8 billion over the September 30, 2006 investments balance.

6. Accounts Receivable, Net

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Intragovernmental	$278	$247
With the Public:		
Accounts Receivable	1,229	1,639
Allowance for Doubtful Accounts	(469)	(458)
	760	**1,181**
Accounts Receivable, Net	**$1,038**	**$1,428**

Intragovernmental accounts receivable results from reimbursable work performed by the Department. Accounts receivable with the public consist of amounts due for reimbursable services and user fees. The decrease in accounts receivable with the public is primarily caused by an increase in payments to TSA received for Aviation Security Infrastructure Fees due from airline companies.

7. Taxes, Duties, and Trade Receivables, Net

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

As of September 30, 2007 (Unaudited):

Receivables Category	Gross Receivables	Allowance	Total Net Receivables
Duties	$1,694	$(116)	$1,578
Excise Taxes	127	(6)	121
User Fees	132	(5)	127
Fines/Penalties	1,260	(1,185)	75
Anti-Dumping/Countervailing Duties	314	(278)	36
Total Tax, Duties, and Trade Receivables, Net	**$3,527**	**$(1,590)**	**$1,937**

As of September 30, 2006 (Unaudited) (Restated):

Receivables Category	Gross Receivables	Allowance	Total Net Receivables
Duties	$1,601	($118)	$1,483
Excise Taxes	99	(6)	93
User Fees	120	(13)	107
Fines/Penalties	1,243	(1,187)	56
Anti-Dumping/Countervailing Duties	259	(243)	16
Total Tax, Duties, and Trade Receivables, Net	**$3,322**	**$(1,567)**	**$1,755**

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 a period of time 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 on fines and penalties of approximately 94 percent (96 percent at September 30, 2006) 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 Treasury General Fund.

8. Direct Loans, Net

DHS's loan program consists of two types of direct loans, both administered by FEMA: (1) State Share Loans: FEMA may lend or advance to a state or an eligible applicant the portion of assistance for which the applicant is responsible under cost-sharing provisions of the Stafford Act. For 1992 and beyond, the State Share Loans are obligated from the Disaster Assistance Direct

Loan Financing Account; and (2) Community Disaster Loans (CDLs): Loans 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 financial assistance in order to perform their municipal operating functions. The loans are made at the current Treasury rate for a term of five years and cannot exceed 25 percent of the annual operating budget of the local government for the fiscal year in which the major disaster occurred, with the exception of Hurricanes Katrina/Rita Special CDL. The rates for Katrina/Rita Special CDL are less than the Treasury rate and 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, in accordance with recent Stafford Act amendments (P.L. 109-88), CDLs may exceed $5 million and shall not be canceled. However, P.L. 110-28 amended the *Community Disaster Loan Act of 2005* (P.L. 109-88) by striking "Provided further, that notwithstanding section 471(c)(1) of the *Stafford Act*, such loans may not be cancelled." This resulted in a total modification cost of $327 million for the 2006 Cohort. Of this amount $207 million was transferred to the Financing account to repay funds borrowed from Treasury. The balance remains in the Programming account to cover costs of undisturbed loans for the 2006 Cohort.

Loans totaling $162 million and $629 million have been disbursed to eligible borrowers as of September 30, 2007 and 2006, respectively. 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):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
	Loans Receivable, Net	Loans Receivable, Net
Community Disaster Loans	**$ -**	**$161**

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):

At September 30, 2007 (Unaudited):	Loans Receivable, Gross	Interest Receivable	Allowance for Subsidy Cost (Present Value)	Value of Assets Related to Direct Loans
Community Disaster Loans	**$792**	**$30**	**$(822)**	**$ -**

At September 30, 2006 (Unaudited) (Restated):	Loans Receivable, Gross	Interest Receivable	Allowance for Subsidy Cost (Present Value)	Value of Assets Related to Direct Loans
Community Disaster Loans	**$631**	**$9**	**($479)**	**$161**

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

	2007 (Unaudited)	2006 (Unaudited)
Community Disaster Loans	**$161**	**$629**

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
2007 (Unaudited)	$28	$93	$121
2006 (Unaudited) (Restated)	$109	$362	$471

For the Community Disaster Loan Program there were no re-estimates or modifications to the subsidy expense.

Total Direct Loan Subsidy Expense

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Community Disaster Loans	**$329**	**$471**

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

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

	2007 (Unaudited)		2006 (Unaudited) (Restated)	
	Community Disaster Loans	State Share Loans	Community Disaster Loans	State Share Loans
Interest Subsidy Cost	4.9%	0.82%	17.4 %	(0.55) %
Default Costs	- %	- %	57.6 %	- %
Other	88.5%	0.36%	- %	0.36 %

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Beginning Balance of the Subsidy cost allowance	$479.2	$3.2
Add subsidy expense for direct loans disbursed during the reporting years by component:		
(a) Interest rate differential costs	28.2	109.3
(b) Other subsidy costs	93.3	362.1
Adjustments:		
(a) Loans written off	(1)	-
(b) Subsidy allowance amortization	15	4.6
(c) Other	207.2	-
Ending balance of the subsidy cost allowance before reestimates	821.9	479.2
Add subsidy reestimate by component		
(a) Technical/default reestimate	.4	-
Ending balance of the subsidy cost allowance	**$822.3**	**$479.2**

The amount of loans written off as of September 30, 2007 were $1 million. No write-offs were reported as of September 30, 2006.

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Community Disaster and State Share Loans	**$.5**	**$1.6**

9. Inventory and Related Property, Net

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Operating Materials and Supplies (OM&S)		
Items Held for Use	$302	$337
Items Held for Future Use	30	28
Excess, Obsolete and Unserviceable Items	149	75
Less: Allowance for Losses	(149)	(75)
Total OM&S, Net	**332**	**365**
Inventory		
Inventory Purchased for Resale	61	69
Less: Allowance for Losses	(4)	(3)
Total Inventory, Net	**57**	**66**
Stockpile Materials Held in Reserve	**243**	**246**
Total Inventory and Related Property, Net	**$632**	**$677**

10. Seized and Forfeited Property

Prohibited seized property item counts as of September 30 and activity for fiscal years 2007 and 2006 are as follows:

Seizure Activity						
Fiscal Year Ended September 30, 2007 (Unaudited)						
Seized Property Category:	Beginning Balance	New Seizures	Remissions	New Forfeitures	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	737	774,841	-	(772,729)	405	3,254
Cocaine	353	22,985	-	(23,075)	(77)	186
Heroin	20	5,459	-	(5,463)	4	20
Ecstasy	-	1,426	-	(1,393)	-	33
Steroids	-	514	(65)	(305)	(8)	136
Firearms and Explosives (in number of items)	864	1,970	(886)	(675)	(143)	1,130
Counterfeit Currency (US/Foreign, in number of items)	4,227,431	1,325,661	-	-	(1,554,722)	3,998,370
Pornography (in number of items)	101	173	(3)	(140)	(55)	76

Forfeiture Activity						
Fiscal Year Ended September 30, 2007 (Unaudited)						
Forfeited Property Category:	Beginning Balance	New Forfeitures	Transfers	Destroyed	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	97,304	772,729	(234,858)	(459,151)	(3,629)	172,395
Cocaine	19,584	23,075	(156)	(20,545)	(394)	21,564
Heroin	2,221	5,463	(4)	(1,045)	(43)	6,592
Ecstasy	-	1,393	(9)	(1,060)	1,543	1,867
Steroids	-	305	-	(314)	22	13
Firearms and Explosives (in number of items)	253	675	(607)	(2)	29	348
Pornography (in number of items)	32	140	(1)	(195)	53	29

Seizure Activity						
Fiscal Year Ended September 30, 2006 (Unaudited) (Restated)						
Seized Property Category:	Beginning Balance	New Seizures	Remissions	New Forfeitures	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	502	439,748	-	(439,597)	84	737
Cocaine	162	28,513	-	(28,289)	(33)	353
Heroin	26	1,345	-	(1,345)	(6)	20
Firearms and Explosives (in number of items)	2,021	1,362	(936)	(1,521)	(62)	864
Counterfeit Currency (US/Foreign, in number of items)	3,364,060	1,424,320	-	-	(560,949)	4,227,431
Pornography (in number of items)	141	158	-	(138)	(60)	101
Forfeiture Activity						
Fiscal Year Ended September 30, 2006 (Unaudited) (Restated)						
Forfeited Property Category	Beginning Balance	New Forfeitures	Transfers	Destroyed	Adjustments	Ending Balance
Illegal Drugs (in kilograms):						
Cannabis (marijuana)	92,834	439,597	(3,167)	(362,988)	(68,972)	97,304
Cocaine	21,513	28,289	(7)	(29,663)	(548)	19,584
Heroin	2,104	1,345	(1)	(1,242)	15	2,221
Firearms and Explosives (in number of items)	276	1,521	(1,551)	(4)	11	253
Pornography (in number of items)	39	138	-	(178)	33	32

This schedule is presented for material prohibited (non-valued) seized and forfeited property only. These items are retained and ultimately destroyed by CBP and USSS and are not transferred to the 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. Firearms, explosives, and pornography are presented in number of items, and counterfeit currency is presented in number of bills. The adjustments columns relate to prohibited property adjustments made due to items incorrectly tagged or marked as to seized or forfeited. For seizure activity the adjustments also include destroyed items.

USCG also seizes and takes temporary possession of small boats, equipment, contraband, and other illegal drugs. USCG usually disposes of these properties within three days by transfer to CBP (who transfers non-prohibited seized property to the Treasury Forfeiture Fund), the Drug Enforcement Administration, foreign governments, or by destroying it. Seized property in USCG possession at year-end is not considered material and therefore is not itemized and is not reported in the financial statements of the Department.

CBP will take into custody, without risk or expense, merchandise termed "general order property", which for various reasons cannot legally enter into the commerce of the United States. CBP's sole responsibility with general order property is to ensure the property does not enter the Nation's commerce. If general order property remains in CBP custody for a prescribed period of time, without payment of all estimated duties, storage, and other charges, the property is considered unclaimed and abandoned and may be sold by CBP at public auction, retained by CBP for its official use, or at CBP's discretion, be transferred to any other Federal, State, or local agency, destroyed, or disposed of otherwise. Auction sales revenue in excess of charges associated with the sale or storage of the item is remitted to the Treasury General Fund. In some cases, CBP incurs charges prior to the sale and funds these costs from entity appropriations. Regulations permit CBP to offset these costs of sale before returning excess amounts to Treasury.

11. General Property, Plant, and Equipment, Net

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

As of September 30, 2007 (Unaudited):	Service Life	Gross Cost	Accumulated Depreciation/ Amortization	Total Net Book Value
Land and Land Rights	N/A	$90	N/A	$90
Improvements to Land	3-50 yrs	114	49	65
Construction in Progress	N/A	4,468	N/A	4,468
Buildings, Other Structures and Facilities	2-50 yrs	4,147	1,993	2,154
Equipment:				
ADP Equipment	3-5 yrs	317	191	126
Aircraft	10-35 yrs	2,722	1,558	1,164
Vessels	5-65 yrs	4,317	2,365	1,952
Vehicles	3-8 yrs	573	448	125
Other Equipment	2-30 yrs	3,834	2,409	1,425
Assets Under Capital Lease	2-20 yrs	79	26	53

Leasehold Improvements	3-50 yrs	364	104	260
Internal Use Software	2-10 yrs	897	714	183
Internal Use Software- in Development	N/A	210	N/A	210
Total General Property, Plant, and Equipment, Net		**$22,132**	**$9,857**	**$12,275**

As of September 30, 2006 (Unaudited) (Restated):	Service Life	Gross Cost	Accumulated Depreciation/ Amortization	Total Net Book Value
Land and Land Rights	N/A	$75	N/A	$75
Improvements to Land	3-50 yrs	64	29	35
Construction in Progress	N/A	2,899	N/A	2,899
Buildings, Other Structures and Facilities	2-50 yrs	3,893	1,903	1,990
Equipment:				
ADP Equipment	3-5 yrs	349	187	162
Aircraft	10-35 yrs	2,595	1,441	1,154
Vessels	5-65 yrs	4,233	2,152	2,081
Vehicles	3-8 yrs	505	382	123
Other Equipment	2-30 yrs	3,867	2,060	1,807
Assets Under Capital Lease	2-20 yrs	79	23	56
Leasehold Improvements	3-50 yrs	381	104	277
Internal Use Software	2-10 yrs	910	567	343
Internal Use Software- in Development	N/A	149	N/A	149
Total General Property, Plant, and Equipment, Net		**$ 19,999**	**$8,848**	**$11,151**

12. Stewardship Property, Plant, and Equipment

DHS's Stewardship PP&E primarily consists of USCG's Heritage Assets, which are unique due to historical or natural significance; cultural, educational, or artistic importance; or significant architectural characteristics. USCG's Heritage Assets includes sunken craft, historical buildings, structures, artifacts, and art and display models.

USCG does not acquire or retain Heritage buildings and structures without an operational purpose. Most real property, even if designated as historical, is acquired for operational use and is transferred to other government agencies or public entities when no longer required for operations. Of the USCG buildings and structures designated as Heritage Assets, including memorials, recreational areas, and other historical areas, over two-thirds are multi-use Heritage Assets. The remainder is comprised of historical lighthouses, which are no longer in use and awaiting transfer or disposal. CBP also has four multi-use heritage assets located in Puerto Rico and FEMA has one multi-use heritage asset that is used by the U. S. Fire Administration for training in Emmitsburg, Maryland.

13. Other Assets

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Intragovernmental:		
Advances and Prepayments	$2,887	$2,913
Due from Treasury	176	411
Total Intragovernmental	3,063	3,324
Public:		
Advances and Prepayments	567	551
Total Public	567	551
Total Other Assets	**$3,630**	**$3,875**

Intragovernmental Advances and Prepayments primarily consist of FEMA's Disaster Relief Fund disaster assistance advances to other Federal agencies (principally the Department of Transportation) tasked with 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):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Intragovernmental:		
Debt (Note 15)	$17,786	$17,092
Accrued FECA Liability (Note 18)	355	323
Other	51	67
Total Intragovernmental	18,192	17,482
Public:		
Federal Employee and Veterans' Benefits:		
Actuarial FECA Liability (Note 16)	1,683	1,520
Military Service and Other Retirement Benefits (Note 16)	33,227	30,758
Environmental and Disposal Liabilities (Note 17)	254	245
Other:		
Accrued Payroll and Benefits (Note 18)	874	824
Insurance Liabilities (Note 20)	1,508	3,557
Contingent Legal Liabilities (Note 21)	90	24
Capital Lease Liability (Note 19)	107	110
Other	-	-
Total Public	37,743	37,038
Total Liabilities Not Covered by Budgetary Resources	55,935	54,520
Liabilities Covered by Budgetary Resources or Non-Entity Assets	12,998	16,269
Total Liabilities	**$68,933**	**$70,789**

The Department anticipates that the liabilities listed above will be funded from future budgetary resources when required. Budgetary resources are generally provided for unfunded leave when it is used. Unfunded leave is included in accrued payroll and benefits.

Insurance liabilities decreased in FY 2007 due to payments of flood insurance claims, primarily related to Hurricanes Katrina and Rita. The Liabilities Covered by Budgetary Resources or Non-Entity Assets decreased in FY 2007 due to Canadian Softwood lumber refunds disbursed during FY 2007.

15. Debt

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

Fiscal year ended September 30, 2007	Beginning Balance	Net Borrowing	Ending Balance (Unaudited)
Other Debt:			
Debt for the NFIP	$17,239	$663	$17,902
Debt for Credit Reform	207	44	251
Total Debt to the Treasury General Fund	$17,446	$707	$18,153
Total Debt	**$17,446**	**$707**	**$18,153**

Fiscal year ended September 30, 2006	Beginning Balance	Net Borrowing	Ending Balance (Unaudited) (Restated)
Other Debt:			
Debt for the NFIP	$225	$17,014	$17,239
Debt for Credit Reform	1	206	207
Total Debt to the Treasury General Fund	$226	$17,220	$17,446
Total Debt	**$226**	**$17,220**	**$17,446**

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 the FEMA's credit reform programs (State Share Loans and Community Disaster Loans). The Net Borrowings in FY 2006 was the result of an increase to FEMA's borrowing authority to satisfy claims as a result of the 2005 hurricane season.

NFIP loans are for a three-year term. Interest rates are obtained from the BPD and range by cohort year from 3.38 percent to 4.88 percent as of September 30, 2007 and from 4.87 percent to 6.69 percent as of September 30, 2006. Simple interest is calculated monthly – offset by an interest rebate, if applicable. The interest rebate is calculated at a rate equal to the weighted average of the interest rates of outstanding loans for the month multiplied by the "positive" daily account fund balance for the month. Interest is paid semi-annually, October 1 and April 1. 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. Flood premiums from policy holders and map collection fees are intended to repay loan principal and interest payments due to Treasury; however, due to the size of the debt incurred for damages sustained for Hurricanes Katrina and Rita, premiums received are only sufficient to cover the interest payments.

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 2007 and FY 2006 were 4.87 percent and 4.53 percent, 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):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
USCG Military Retirement and Healthcare Benefits	$29,494	$27,105
USCG Post-Employment Military Travel Benefits	133	128
USSS DC Pension Plan Benefits	3,595	3,518
Actuarial FECA Liability	1,683	1,520
Other	5	7
Total Federal Employee and Veterans' Benefits	**$34,910**	**$32,278**

A. USCG Military Retirement and Healthcare Benefits

The USCG Military Retirement System (MRS or the Plan) is a defined benefit plan that covers both retirement pay and health care benefits for all active duty and reserve military members of the USCG. The 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 and any plan assets, from the present value of the future cost of benefits. Current period expense is computed using the aggregate entry age normal actuarial cost method.

The components of the MRS expense for the years ended September 30 consisted of the following (in millions):

Defined Benefit Plan:	2007 (Unaudited)	2006 (Unaudited) (Restated)
Normal cost	$653	$589
Interest on the liability	1,417	1,376
Actuarial losses/(gains)	120	(239)
Actuarial Assumption Change	721	902
Plan Amendments	136	-
Total Defined Benefit Plan Expense	**$3,047**	**$2,628**

Post-retirement Healthcare:		
Normal cost	$151	$180
Interest on the liability	287	249
Other Actuarial (gains)/losses	(281)	48
Total Post-retirement Healthcare Expense	**157**	**477**
Total MRS Expense	**$3,204**	**$3,105**

USCG's military service members (both active duty and reservists) participate in the MRS. USCG receives an annual "Retired Pay" appropriation to fund MRS benefits. The retirement system allows voluntary retirement for active members upon credit of at least 20 years of active service at any age. Reserve members may retire after 20 years of creditable service with benefits beginning at age 60. USCG's MRS includes the USCG Military Health Services System (Health Services Plan). The Health Services Plan is a post-retirement medical benefit plan, which covers all active duty and reserve members of the USCG.

A portion of the accrued MRS liability is for the health care of non-Medicare eligible retirees and survivors. Effective October 1, 2002, USCG transferred its liability for the health care of Medicare eligible retirees/survivors to the DOD Medicare-Eligible Retiree Health Care Fund (the Fund), which was established in order to finance the health care benefits for the Medicare-eligible beneficiaries of all DOD and non-DOD uniformed services. DOD is the administrative entity for the DOD Medicare-Eligible Retiree Health Care Fund and in accordance with Statement of Federal Financial Accounting Standards (SFFAS) No. 5, is required to recognize the liability on the Fund's financial statements. USCG makes annual payments to the Fund for current active duty members. Benefits for USCG members who retired prior to the establishment of the Fund are provided by payments from the Treasury to the Fund. The future cost and liability of the Fund is determined using claim factors and claims cost data developed by the DOD, adjusted for USCG retiree and actual claims experience. USCG uses the current year actual costs to project costs for all future years.

The unfunded accrued liability, presented as a component of the liability for military service and other retirement in the accompanying Balance Sheet, represents both retired pay and health care benefits for non-Medicare eligible retirees/survivors. Valuation of the plan's liability is based on the actuarial present value of accumulated plan benefits derived from the future payments that are attributable, under the retirement plan's provisions, to a participant's credited service as of the valuation date. 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 unfunded accrued liability by subtracting the present value of future employer/employee normal contributions. USCG 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 credited service up to 75 percent of basic pay. Personnel who became members after August 1, 1986, may elect to receive a $30,000 lump sum bonus after 15 years of service and reduced benefits prior to age 62. Annual disability is equal to the retired pay base multiplied by the larger of: (1) 2.5 percent times years of service; or (2) percent disability. The benefit cannot be more than 75 percent of retired pay base. If a USCG member is disabled, the member is entitled to disability benefits, assuming the disability is at least

30 percent (under a standard schedule of rating disabilities by Veterans Affairs) and either: (1) the member has one month and one day of service; (2) the disability results from active duty; or (3) the disability occurred in the line of duty during a time of war or national emergency or certain other time periods.

The significant actuarial assumptions used to compute the MRS accrued liability are:

- life expectancy is based upon the DOD death mortality table;
- cost of living increases are 3.0 percent annually; and
- annual rate of investment return is 6.0 percent.

B. District of Columbia Police and Fireman's Retirement System for U.S. Secret Service Employees

Special agents and personnel in certain job series hired by USSS 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 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 7 percent of base pay with no matching contribution made by USSS. Annuitants of this plan receive benefit payments directly from the DC Pension Plan. The 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, *Accounting for Liabilities of the Federal Government*, requires the administrative entity (administrator) to report the actuarial liability. However, the USSS adopted the provisions of SFFAS No. 5 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 liability and expense are computed using the aggregate cost method. The primary actuarial assumptions used to determine the liability at September 30, 2007, are:

- life expectancy is based upon the 1994 Uninsured Pension (UP94) tables;
- 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.

Total expenses related to the DC Pension Plan for the fiscal years ended September 30, 2007 and 2006, were $215 million and $202 million, respectively.

C. Actuarial FECA Liability

The actuarial Federal Employees' Compensation Act (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, generated from an application of actuarial procedures developed by the DOL, for the future cost of approved compensation cases were approximately $1.7 billion and $1.5 billion at September 30, 2007 and 2006, respectively (unaudited).

17. Environmental and Disposal Liabilities

Environmental and Disposal Liabilities at September 30, 2007 and 2006, are $275 million and $245 million, respectively (unaudited). The Department is responsible to remediate its sites with environmental contamination, and is party to various administrative proceedings, legal actions, and tort claims which 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 (P.L. 96-510)* and the *Resource Conservation and Recovery Act (P.L. 94-580)*.

The liabilities are primarily due to lighthouses, light stations, fuel storage tank program, 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, and USCG. For the Plum Island Animal Disease Center, under S&T, potential environmental liabilities may exist in addition to the amounts accrued in the accompanying financial statements that are not presently estimable but could exist due to the facility's age, old building materials used, and other materials associated with the facility's past use as a U.S. Army installation for coastline defense.

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):

Fiscal year ended September 30, 2007	Current	Non-Current	(Unaudited)
Intragovernmental:			
Accrued FECA Liability	$219	$136	$355
Advances from Others	70	-	70
Employer Benefits Contributions and Payroll Taxes	118	-	118
Due to the General Fund (Note 2)	2,085	-	2,085
Other Intragovernmental Liabilities	57	-	57
Total Intragovernmental Other Liabilities	**$2,549**	**$136**	**$2,685**
Public:			
Accrued Payroll and Benefits (See B. below)	$1,534	$19	$1,553
Deferred Revenue and Advances from Others (See B. below)	1,682	1,045	2,727
Unliquidated Antidumping/Countervailing Duties (Notes 2 and 3)	514	- -	514
Injured Domestic Industries (Notes 2 and 3)	388	-	388
Insurance Liabilities (Note 20)	513	995	1,508
Contingent Legal Liabilities (Note 21)	135	1	136
Capital Lease Liability (Note 19)	50	57	107
Refunds and Drawbacks (Note 2) (See B. below)	131	-	131
Other Liabilities	777	-	777
Total Other Liabilities with the Public	**$5,724**	**$2,117**	**$7,841**
Total Other Liabilities	**$8,273**	**$2,253**	**$10,526**

Fiscal year ended September 30, 2006	Current	Non-Current	Total (Unaudited) (Restated)
Intragovernmental:			
Accrued FECA Liability	$154	$185	$339
Advances from Others	22	-	22
Employer Benefits Contributions and Payroll Taxes	150	3	153
Due to the General Fund (Note 2)	1,809	-	1,809
Other Intragovernmental Liabilities	4	8	12
Total Intragovernmental Other Liabilities	**$2,139**	**$196**	**$2,335**
Public:			
Accrued Payroll and Benefits (See B. below)	$1,173	$189	$1,362
Deferred Revenue and Advances from Others (See B. below)	1,200	988	2,188
Unliquidated Antidumping/Countervailing Duties (Notes 2 and 3)	34	-	34
Injured Domestic Industries (Notes 2 and 3)	476	-	476
Insurance Liabilities (Note 20)	1,177	2,390	3,567
Contingent Legal Liabilities (Note 21)	-	71	71
Capital Lease Liability (Note 19)	16	106	122
Refunds and Drawbacks (Note 2) (See B. below)	5,593	-	5,593
Other Liabilities	469	67	536
Total Other Liabilities with the Public	**$10,138**	**$3,811**	**$13,949**
Total Other Liabilities	**$12,277**	**$4,007**	**$16,284**

A. Intragovernmental Other Liabilities

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 on 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 $154 million and $164 million, respectively (unaudited), for the fiscal years ended September 30, 2007 and 2006.

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.

B. Other Liabilities with the Public

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Accrued Funded Payroll and Benefits	$656	$524
Accrued Unfunded Leave	852	767
Unfunded Employment Related Liabilities	22	57
Other	23	14
Total Accrued Payroll and Benefits	**$1,553**	**$1,362**

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

	2007 (Unaudited)	2006 (Unaudited) (Restated)
USCIS Application Fees	$1,132	$702
FEMA Unexpired NFIP premium	1,582	1,473
Advances from Others	13	13
Total Deferred Revenue	**$2,727**	**$2,188**

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 that are recognized over the term of the period of insurance coverage.

Unliquidated Antidumping and Countervailing Duties and Injured Domestic Industries. The *Continued Dumping and Subsidy Offset Act of 2000, P.L. 106-387, Title X*, enacted in FY 2001 calls for CBP to collect and disburse monies received in connection with antidumping and countervailing duty orders and findings to qualifying IDI. Antidumping duties are collected when it is determined that a class or kind of foreign merchandise is being released into the U.S. economy at less than its fair value to the detriment of a U.S. industry. Countervailing duties are collected when it is determined that a foreign government is providing a subsidy to its local industries to manufacture, produce, or export a class or kind of merchandise for import into the U.S. commerce to the detriment of a U.S. industry. The duties will eventually be distributed, pursuant to rulings by the Department of Commerce.

Refunds and Drawbacks. The liability for refunds and drawbacks for the fiscal years ended September 30 consisted of the following (in millions):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Canadian Softwood Lumber Duties and Accrued Interest	$ -	$5,504
Other Refunds and Drawbacks	131	89
Total Refunds and Drawbacks	**$131**	**$ 5,593**

CBP collected duties on the import of Canadian Softwood lumber which were included in non-entity fund balance with Treasury during FY 2006. During FY 2006, an agreement was reached related to the litigation for duties related to the import of Canadian Softwood lumber. As a result of this agreement, the Canadian Softwood lumber duties previously collected and accrued interest was refunded during FY 2007, which accounts for the decrease to the Refunds and Drawbacks balance.

Other Liabilities. Other public liabilities consist primarily of NFIP payable to insurance companies and the liability for deposit and suspense funds.

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, 2007, estimated future minimum lease commitments under operating leases for equipment and GSA controlled leases were as follows (in millions) (unaudited):

	GSA	Non-GSA	Total
FY 2008	$906	$115	$1,021
FY 2009	935	113	1,048
FY 2010	956	115	1,071
FY 2011	985	118	1,103
FY 2012	1,018	123	1,141
After FY 2012	2,830	356	3,186
Total Future Minimum Lease Payments	**$7,630**	**$940**	**$8,570**

The estimated future lease payments for GSA controlled leases are based on payments made during the year ended September 30, 2007.

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 may be funded from future sources.

As of September 30, 2007, estimated future minimum lease payments under capital leases, which were all non-GSA, were as follows (in millions) (unaudited):

	Total
FY 2008	$24
FY 2009	24
FY 2010	24
FY 2011	6
FY 2012	6
After FY 2012	64
Total Future Minimum Lease Payments	**148**
Less: Imputed interest and Executory costs	(41)
Total Capital Lease Liability	**$107**

20. Insurance Liabilities

Insurance liabilities for the periods ended September 30, 2007 and 2006 were $1,508 million and $3,567 million, respectively (unaudited), and consist of primarily NFIP insurance liabilities. Insurance liabilities decreased in FY 2007 due to payments of flood insurance claims, primarily related to Hurricanes Katrina and Rita.

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):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Beginning Balance	$3,567	$23,416
Change in incurred losses	(926)	(2,281)
Less: Amounts paid during current period	(1,133)	(17,568)
Total Insurance Liability at September 30	**$1,508**	**$3,567**

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 continually reviewed, and adjustments, reflected in current operations, are made as deemed necessary.

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 the 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 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 non-subsidized premium zones applicable to the community).

21. Commitments and Contingent Liabilities

A. Legal Contingent Liabilities

The estimated contingent liability recorded in the accompanying financial statements included with other liabilities for all probable and estimable litigation related claims at September 30, 2007, was $136 million, of which $46 million was funded. The range of probable and estimable litigation is $136 million to $232 million. Asserted and pending legal claims for which loss is reasonably possible is estimated to range from $124 million to $915 million at September 30, 2007.

The estimated contingent liability recorded in the accompanying financial statements included with other liabilities for all probable and estimable litigation related claims at September 30, 2006, was $71 million, of which $47 million was funded. At September 30, 2006, the range of probable and estimable litigation was $71 million to $100 million. Asserted and pending legal claims for which loss is reasonably possible was estimated to range from $68 million to $2.7 billion, at September 30, 2006.

The nature of probable and reasonably possible claims is litigation related to the *Federal Tort Claims Act (P.L. 79-601)*, Oil Spill Liability Trust Fund, and various customs laws and regulations. The Department is subject to various other legal proceedings and claims. In management's opinion, the ultimate resolution of other actions will not materially affect the Department's financial position or net costs. Contingent liabilities considered remote are generally not disclosed unless they involve guarantees, in which case the nature of the guarantee is disclosed.

DHS management and general legal counsel assess such contingent liabilities, and such assessment inherently involves an exercise of judgment. In assessing contingencies related to legal proceedings that are pending against DHS, or unasserted claims that may result in such proceedings, general legal counsel evaluates the perceived merits of any legal proceedings or unasserted claims as well as the perceived merits of the amounts of relief sought or expected to be brought therein.

If the assessment of the loss contingency indicates that it is probable that a material liability has been incurred and the amount of the liability can be estimated, then the estimated liability is accrued in the financial statements regardless of the source of funding used to pay the liability. If the assessment indicates that a potentially material contingent liability is not probable but is reasonably possible, or is probable but cannot be estimated, then the nature of the contingent liability, together with an estimate of the range of possible loss, if determinable and material, is disclosed.

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 refunds as of September 30, 2007, and 2006, 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. As of September 30, 2007 and September 30, 2006, CBP had 16 aircraft loaned from DOD with an acquisition value of $94 million (unaudited).

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. As of September 30, 2007, DHS estimates $47 million (unaudited) in obligations related to cancelled appropriations for which the Department has a contractual obligation for payment as well as an estimated $14 million (unaudited) for contractual arrangements which may require future funding. As of September 30, 2006, DHS estimated $67 million (unaudited) in obligations related to cancelled appropriations for which the Department has a contractual obligation for payment as well as an estimated $41 million (unaudited) for contractual arrangements which may require future funding.

TSA entered into a number of *Letters of Intent for Modifications to Airport Facilities* with eight major airports in which TSA may reimburse the airports for 75 percent (estimated total of $957 million) of the cost to modify the facilities for security purposes. These Letters of Intent would not obligate TSA until funds have been appropriated and obligated. TSA has received appropriations of $162 million (unaudited) in FY 2007 and $240 million (unaudited) in FY 2006 under this program, which is available for payment to the airports upon approval by TSA of an invoice for the modification costs incurred. As of September 30, 2007, TSA has received invoices or documentation for costs incurred totaling $572 million (unaudited) related to these agreements.

22. Earmarked Funds

Earmarked funds are financed by specifically identified revenues, often supplemented by other financing sources, which remain available over time. These specifically identified revenues and other financing sources are required by statute to be used for designated activities or purposes. SSFAS No. 27 defines the following three critieria for determining an earmarked fund: (1) A statute committing the Federal Government to use specifically identifed revenues and other financing sources not used in the current period for future use to finance the 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.

Earmarked Funds containing no eliminations within the earmarked funds consisted of the following (in millions) (unaudited):

	Customs User Fees	Sport Fish Restoration Boating Trust Fund	Immigration Examination Fees	National Flood Insurance Program	All Other Earmarked Funds	Total Earmarked Funds
Balance Sheet as of September 30, 2007						
ASSETS						
Fund Balance with Treasury	$730	$8	$1,245	$656	$1,061	$3,700
Investments, Net	-	1,845	-	-	933	2,778
Taxes Receivables	69	-	-	-	-	69
Other	76	19	267	497	247	1,106
Total Assets	**$875**	**$1,872**	**$1,512**	**1,153**	**$2,241**	**$7,653**
LIABILITIES						
Other Liabilities	$87	$1,101	$1,516	$21,054	$131	$23,889
Total Liabilities	**$87**	**$1,101**	**$1,516**	**$21,054**	**$131**	**$23,889**

	Customs User Fees	Sport Fish Restoration Boating Trust Fund	Immigration Examination Fees	National Flood Insurance Program	All Other Earmarked Funds	Total Earmarked Funds
NET POSITION						
Cumulative Results of Operations	$788	$771	$(4)	$(19,901)	$2,110	$(16,236)
Total Liabilities and Net Position	**$875**	**$1,872**	**$1,512**	**$1,153**	**$2,241**	**$7,653**
Statement of Net Cost for the Year Ended September 30, 2007						
Gross Program Costs	$369	$ -	$1,681	$799	$1,163	$4,012
Less: Earned Revenues	-	(76)	(1,669)	(2,622)	(426)	(4,793)
Net Cost of Operations	**$369**	**$(76)**	**$12**	**$(1,823)**	**$737**	**$(781)**
Statement of Changes in Net Position for the Year Ended September 30, 2007						
Net Position Beginning of Period	$798	$-	$8	$(21,725)	$1,582	$(19,337)
Adjustment to the Beginning Balance (Note 36)	-	693	-	-	-	693
Net Cost of Operations	(369)	76	(12)	1,823	(737)	781
Non-exchange Revenue	1,808	628	-	-	1,167	3,603
Other	(1,450)	(626)	-	1	99	(1,976)
Change in Net Position	(11)	78	(12)	1,824	529	2,408
Net Position, End of Period	$787	$771	$(4)	$(19,901)	$2,111	$(16,236)

	Customs User Fees	Immigration Examination Fees	National Flood Insurance Program	All Other Earmarked Funds	Total Earmarked Funds
Balance Sheet as of September 30, 2006 (Restated)					
ASSETS					
Fund Balance with Treasury	$761	$819	$138	$815	$ 2,533
Investments, Net	-	-	-	634	634
Taxes Receivables	61	-	-	-	61
Other	72	29	507	220	828
Total Assets	$894	$848	$645	$1,669	$4,056
LIABILITIES					
Other Liabilities	$96	$840	$22,370	$87	$23,393
Total Liabilities	$96	$840	$22,370	$87	$23,393

	Customs User Fees	Immigration Examination Fees	National Flood Insurance Program	All Other Earmarked Funds	Total Earmarked Funds
NET POSITION (Restated)					
Cumulative Results of Operations	$798	$8	$(21,725)	$,1,582	$(19,337)
Total Liabilities and Net Position	$894	$848	$645	$1,669	$4,056
Statement of Net Cost for the Year Ended September 30, 2006 (Restated)					
Gross Program Costs	$ -	$1,590	$(716)	$1,459	$2,333
Less: Earned Revenues	(1)	(1,721)	(2,321)	(376)	(4,419)
Net Cost of Operations	$(1)	$(131)	$(3,037)	$1,083	$(2,086)
Statement of Changes in Net Position for the Year Ended September 30, 2006 (Restated)					
Net Position Beginning of Period	$797	$(123)	$(24,764)	$1,375	$(22,715)
Net Cost of Operations	1	131	3,037	(1,083)	2,086
Non-exchange Revenue	-	-	-	2,516	2,516
Other	-	-	2	(1,226)	(1,224)
Change in Net Position	1	131	3,039	207	3,378
Net Position, End of Period	$798	$8	$(21,725)	$1,582	$(19,337)

Customs User Fees

In April 1986, the President signed the *Consolidated Omnibus Budget Reconciliation Act of 1985 (COBRA)*, which 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. The collection of COBRA fees for CBP services began on July 7, 1986.

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. This legislation took effect on October 1, 1990.

19 USC Section 58c contains the fees for certain customs services. The authority to use these funds is contained in the annual DHS appropriations act.

Access to COBRA surplus funds provides CBP with additional resources to assist in the accomplishment of CBP's mission. Increased staffing and equipment have enhanced the manager's flexibility in dealing with the ever-increasing demands of the trade and travel communities.

Sport Fish Restoration Boating Trust Fund

The SFRBTF, previously known as the Aquatic Resources Trust Fund (ARTF), was created by Section 1016 of the *Deficit Reduction Act of 1984 (P.L. 98-369).* Two funds were created under this act, the Boat 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 boat 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, the Fish & Wildlife Service in the Department of Interior (DOI) (14X8151), the U.S. Army Corps of Engineers (COE) (96X8333), and USCG (70X8149).

The most recent reauthorization of the SFRBTF and expenditure of Boat Safety funds for the National RBS Program was enacted in 2005 in the *Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users or SAFETEA-LU (P.L. 109-59)* and the *Sportfishing and Recreational Boating Safety Amendments Act of 2005 (P.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) provides for the collection of fees at a level that will ensure recovery of the full 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 allow the collection, safeguarding, and accounting for fees. The authority provided by section 286(m) of the INA permits USCIS to recover the full costs of providing all immigration adjudication and naturalization services, including those services provided to individuals other than those paying 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 (Treasury

Account Fund Symbol (TAFS) 70X5088). In addition, USCIS provides specific services to other Federal agencies, such as production of Border Crossing Cards for the Department of State, that result in the collection of other revenues that are the result of intragovernmental activities.

During FY 2007, two events occurred that impacted fee revenue resources, including the fee increase and the visa open window for employment benefits.

National Flood Insurance Program

The National Flood Insurance Program (NFIP) was established by the *National Flood Insurance Act of 1968*. 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* 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* 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 mandated.

The *Bunning-Bereuter-Blumenauer Flood Insurance Reform Act (FIRA) of 2004* provides additional tools for addressing the impact of repetitive loss properties on the National Flood Insurance Fund. It introduced a pilot project though fiscal year 2009 that defines severe repetitive loss properties, authorizes additional funds for mitigation projects, and mandates a 50 percent increase of premiums for property owners who decline a mitigation offer, along with an appeal process. It also modifies the Flood Mitigation Assistance (FMA) Program by doubling the annual authorized funding level and directing it to give priority to those properties that are in the best interest of 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 Bureau & Statistical Agent (B&SA) on a monthly basis. This information is reconciled and the WYO companies are required to correct any variances.

This program is an insurance program for which the Department pays claims to policyholders whose houses have been flooded. 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 to only be used to pay claims 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 our program from Congress. The resources are inflows to the Government and are not the result of intragovernmental flows.

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, Emergency Preparedness and Response, Department of Homeland Security
- 70X5089 Customs and Border Protection, Land Border Inspection Fees, Border and Transportation Security, Department of Homeland Security; 116 Stat. 2135
- 70X5087 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 Nonimmigrant Petitioner Account, US 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)
- 70X5436 Radiological Emergency Preparedness Fund, Department of Homeland Security; 116 Stat. 2135
- 70X5451 Immigration Enforcement Account, Border and Transportation Security, Department of Homeland Security; 116 Stat. 2135
- 70X5464 Flood Map Modernization Fund, Emergency Preparedness and Response, Department of Homeland Security; 116 Stat. 2135
- 70X5694 User Fees, Small Airports, U.S. Customs Service, Department of Homeland Security; 116 Stat. 2135
- 70X8149 Boat Safety, Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70X8244 Gifts and Donations, Department Management, Department of Homeland Security; 116 Stat. 2135 (FEMA REPORTED)
- 70X8312 Oil Spill Liability Trust Fund, Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70_8314 Trust Fund Share of Expenses, Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70X8349 Oil Spill Recovery, Coast Guard, Department of Homeland Security; 116 Stat. 2135
- 70X8533 General Gift Fund, 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
- 20X8185 Oil Spill Liability Trust Fund; 103 Stat. 2363, 2364
- 70_5106 H-1 B Nonimmigrant Petitioner Account, Department of Homeland Security; 116 Stat. 2135
- 70X8360 Gifts and Bequests, FLETC, Department of Homeland Security; 116 Stat. 2135

23. Intragovernmental Costs and Exchange Revenue

For the year ended September 30, 2007 (in millions) (Unaudited)

Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
U.S. Customs and Border Protection			
Gross Cost	$2,089	$6,109	$8,198
Less Earned Revenue	(46)	(111)	(157)
Net Cost	**2,043**	**5,998**	**8,041**
U.S. Coast Guard			
Gross Cost	1,188	9,376	10,564
Less Earned Revenue	(372)	(120)	(492)
Net Cost	**816**	**9,256**	**10,072**
U.S. Citizenship and Immigration Services			
Gross Cost	569	1,162	1,731
Less Earned Revenue	(13)	(1,646)	(1,659)
Net Cost	**556**	**(484)**	**72**
Federal Emergency Management Agency			
Gross Cost	2,579	11,693	14,272
Less Earned Revenue	(98)	(2,744)	(2,842)
Net Cost	**2,481**	**8,949**	**11,430**
Federal Law Enforcement Training Center			
Gross Cost	29	373	402
Less Earned Revenue	(37)	(3)	(40)
Net Cost	**(8)**	**370**	**362**
National Protection and Programs Directorate			
Gross Cost	438	417	855
Less Earned Revenue	-	-	-
Net Cost	**438**	**417**	**855**
U.S. Immigration and Customs Enforcement			
Gross Cost	1,168	3,723	4,891
Less Earned Revenue	(783)	(117)	(900)
Net Cost	**385**	**3,606**	**3,991**
Office of Health Affairs			
Gross Cost	1	4	5
Less Earned Revenue	-	-	-
Net Cost	**1**	**4**	**5**

Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
Departmental Operations and Other			
Gross Cost	$442	$762	$1,204
Less Earned Revenue	(2)	(1)	(3)
Net Cost	**440**	**761**	**1,201**
U.S. Secret Service			
Gross Cost	487	1,202	1,689
Less Earned Revenue	(16)	-	(16)
Net Cost	**471**	**1,202**	**1,673**
Science and Technology Directorate			
Gross Cost	583	404	987
Less Earned Revenue	(14)	-	(14)
Net Cost	**569**	**404**	**973**
Transportation Security Administration			
Gross Cost	1,394	5,045	6,439
Less Earned Revenue	(2)	(2,297)	(2,299)
Net Cost	**1,392**	**2,748**	**4,140**
Total Department of Homeland Security			
Gross Cost	10,967	40,270	51,237
Less Earned Revenue	(1,383)	(7,039)	(8,422)
Net Cost	**$9,584**	**$33,231**	**$42,815**

For the year ended September 30, 2006 (in millions) (Unaudited) (Restated)

Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
U.S. Customs and Border Protection			
Gross Cost	$1,787	$5,348	$7,135
Less Earned Revenue	(47)	(106)	(153)
Net Cost	**1,740**	**5,242**	**6,982**
U.S. Coast Guard			
Gross Cost	1,105	8,906	10,011
Less Earned Revenue	(332)	(92)	(424)
Net Cost	**773**	**8,814**	**9,587**
U.S. Citizenship and Immigration Services			
Gross Cost	493	1,095	1,588
Less Earned Revenue	(15)	(1,714)	(1,729)
Net Cost	**478**	**(619)**	**(141)**
Federal Emergency Management Agency			
Gross Cost	6,228	22,617	28,845
Less Earned Revenue	(120)	(2,349)	(2,469)
Net Cost	**6,108**	**20,268**	**26,376**
Federal Law Enforcement Training Center			
Gross Cost	26	286	312
Less Earned Revenue	(31)	(2)	(33)
Net Cost	**(5)**	**284**	**279**
National Protection and Programs Directorate			
Gross Cost	391	352	743
Less Earned Revenue	(1)	-	(1)
Net Cost	**390**	**352**	**742**
U.S. Immigration and Customs Enforcement			
Gross Cost	1,179	3,321	4,500
Less Earned Revenue	(757)	(100)	(857)
Net Cost	**422**	**3,221**	**3,643**
Office of Health Affairs			
Gross Cost	53	-	53
Less Earned Revenue	-	-	-
Net Cost	**53**	**-**	**53**

Directorates and Other Components	Intragovernmental Consolidated	With the Public	Total
Department Operations and Other			
Gross Cost	$288	564	$852
Less Earned Revenue	(2)	-	(2)
Net Cost	**286**	**564**	**850**
U.S. Secret Service			
Gross Cost	403	1,068	1,471
Less Earned Revenue	(18)	-	(18)
Net Cost	**385**	**1,068**	**1,453**
Science and Technology Directorate			
Gross Cost	467	376	843
Less Earned Revenue	-	-	-
Net Cost	**467**	**376**	**843**
Transportation Security Administration			
Gross Cost	1,194	4,807	6,001
Less Earned Revenue	(5)	(2,472)	(2,477)
Net Cost	**1,189**	**2,335**	**3,524**
Total Department of Homeland Security			
Gross Cost	13,614	48,740	62,354
Less Earned Revenue	(1,328)	(6,835)	(8,163)
Net Cost	**$12,286**	**$41,905**	**$54,191**

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 Goals

Operating costs are summarized in the Statement of Net Cost by responsibility segment, as applicable to the reporting period. The net cost of operations is the gross (i.e., total) cost incurred by the Department, less any exchange (i.e., earned) revenue. A responsibility segment is the component that carries out a mission or major line of activity, and whose managers report directly to Departmental Management.

To integrate performance and financial information, as required by the *President's Management Agenda* and the *Government Performance and Results Act,* a supplemental schedule of net cost is included in this note, in which costs by component are allocated to Departmental strategic goals. The Department is currently in the process of revising its strategic goals. Until the goals are finalized and approved, the Department has elected to use the Secretary's two year goals as the basis for integrating FY 2007 net costs to performance information. For FY 2006, certain amounts have been reclassified to reflect the new organization structure conforming to the PKEMR Act. However, FY 2006 net cost information is presented by FY2006 strategic goals consistent with the FY 2006 Performance and Accountability Report (PAR), and have not been reclassified to be consistent with the current year presentation based on Secretary's two year goals.

Net Costs of Department Sub-organizations by Secretary's Goals (in millions)
For the year ended September 30, 2007 (Unaudited)

	Protect our Nation from Dangerous People	Protect our Nation from Dangerous Goods	Protect Critical Infrastructure	Emergency Response System and Culture of Preparedness	Strengthen and Unify DHS Operations and Management	TOTAL
U.S. Customs and Border Protection	$8,041	$ -	$ -	$ -	$ -	**$8,041**
U.S. Coast Guard	2,798	-	5,981	1,293	-	**10,072**
U.S. Citizenship and Immigration Services	72	-	-	-	-	**72**
Federal Emergency Management Agency	-	-	-	11,430	-	**11,430**
Federal Law Enforcement Training Center	-	-	-	362	-	**362**
National Protection and Programs Directorate	285	-	539	31	-	**855**
U.S. Immigration and Customs Enforcement	4,219	-	(228)	-	-	**3,991**
Office of Health Affairs	-	2	-	3	-	**5**
Departmental Operations and Other	-	106	-	-	1,095	**1,201**
U.S. Secret Service	-	-	1,673	-	-	**1,673**
Science and Technology Directorate	30	475	157	311	-	**973**
Transportation and Security Administration	589	-	3,551	-	-	**4,140**
TOTAL Department	**$16,034**	**$583**	**$11,673**	**$13,430**	**$1,095**	**$42, 815**

Net Costs of Department Sub-organizations by Strategic Goals (in millions)
For the year ended September 30, 2006 (Unaudited) (Restated)

	Awareness	Prevention	Protection	Response	Recovery	Service	Organizational Excellence	TOTAL
U.S. Customs and Border Protection	$ -	$ 6,535	$ -	$ -	$ -	$ 447	$ -	**$ 6,982**
U.S. Coast Guard	1,055	4,184	1,552	1,231	57	1,508	-	**9,587**
U.S. Citizenship and Immigration Services	-	(40)	-	-	-	(101)	-	**(141)**
Federal Emergency Management Administration	-	-	16,621	4,509	5,246	-	-	**26,376**
Federal Law Enforcement Training Center	-	279	-	-	-	-	-	**279**
National Protection and Programs Directorate	190	144	290	-	-	118	-	**742**
U.S. Immigration and Customs Enforcement	-	3,324	319	-	-	-	-	**3,643**
Office of Health Affairs	-	-	53	-	-	-	-	**53**
Departmental Operations and Other	86	-	-	-	-	-	764	**850**
U.S. Secret Service	-	-	1,453	-	-	-	-	**1,453**
Science and Technology Directorate	133	460	78	136	36	-	-	**843**
Transportation and Security Administration	4	3,330	190	-	-	-	-	**3,524**
TOTAL Department	**$1,468**	**$18,216**	**$20,556**	**$5,876**	**$5,339**	**$1,972**	**$764**	**$54,191**

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

Apportionment categories are determined in accordance with the guidance provided in OMB Circular 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, 2007 (Unaudited):	**Apportionment Category A**	**Apportionment Category B**	**Exempt from Apportionment**	**Total**
Obligations Incurred - Direct	$30,748	$24,341	$1,593	$56,682
Obligations Incurred - Reimbursable	4,584	736	-	5,320
Total Obligations Incurred	**$35,332**	**$25,077**	**$1,593**	**$62,002**

Year Ended September 30, 2006 (Unaudited) (Restated):	**Apportionment Category A**	**Apportionment Category B**	**Exempt from Apportionment**	**Total**
Obligations Incurred - Direct	$27,786	$58,004	$993	$86,783
Obligations Incurred - Reimbursable	3,690	788	9	4,487
Total Obligations Incurred	**$31,476**	**$58,792**	**$1,002**	**$91,270**

The decrease in obligation of Apportionment Category B for Obligations Incurred - Direct was related to FEMA's payments of approved claims from Hurricane Katrina which were obligated and paid during FY 2006.

26. Available Borrowing Authority

The Department, through FEMA's NFIP, has total borrowing authority of $4.2 billion (unaudited), as of September 30, 2007, available for disaster relief purposes. The borrowing authority consists of $4.2 billion in borrowing authority carried forward from FY 2006. During FY 2007, FEMA used $695 million in borrowing authority; the remaining balance of $3.5 billion represents the total unused portion. As of September 30, 2006, FEMA used $16.8 billion in borrowing authority; the remaining balance of $4.2 billion represents the total unused portion. DADLP 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 refer to the 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 two permanent indefinite appropriations as follows:

- CBP has a permanent and indefinite appropriation, which 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 a 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. 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, which is used to reimburse the District of Columbia Police and Fireman's Retirement System (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.

These appropriations are not subject to budgetary ceilings established by Congress. CBP's refunds payable at year-end are not subject to funding restrictions.

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: (1) specifically rescinded by law; or (2) 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 $1.1 billion (unaudited) and $1.2 billion (unaudited) at September 30, 2007 and 2006, 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; 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 $758 million (unaudited) and $761 million (unaudited) at September 30, 2007 and 2006, 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 2006 Statement of Budgetary Resources (SBR) and the actual amounts reported for 2006 in the Budget of the U.S. Government. Since the FY 2007 financial statements will be reported prior to the release of the Budget of the U.S. Government, DHS is reporting for 2006 only. Typically, the Budget of the U.S. Government with the 2007 actual data is published in February of the subsequent year. Once published the 2007 actual data will be available on the OMB website, www.whitehouse.gov/omb.

(in millions)	**Budgetary Resources**	**Obligations Incurred**	**Distributed Offsetting Receipts**	**Net Outlays**
2006 Actual Balances per the 2008 President's Budget	$105,857	$89,512	$4,844	$74,103
Reconciling Items:				
Accounts that are expired that are not included in Budget of the United States.	1,494	556		
Distributed Offsetting Receipts not included in the Budget of the United States.				(4,842)
Refunds and drawbacks not included in the Budget of the United States.	891	891		891
Byrd Program not included in the Budget of the United States.	792	226		226
Timing differences related to the reporting of an Anti-Deficiency Act violation.	(248)			
Differences in reporting methodologies between the Budget of the United States and the SBR related to prior year fee collections.	(80)	(18)		
Miscellaneous Differences	(132)	103	(23)	36
Per the 2006 SBR (Unaudited) (Restated)	**$108,574**	**$91,270**	**$4,821**	**$70,414**

30. Undelivered Orders, End of Period

An 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, 2007 and 2006 were $38,435 million (unaudited) and $36,914 million (unaudited) (restated), respectively.

31. Explanation for the Difference between the Appropriations Received reported on the Statement of Budgetary Resources and on the Statement of Changes in Net Position

The Statement of Budgetary Resources (SBR) reported $46,491 million (unaudited) for appropriations received for FY 2007. This balance does not agree to the balance reported on the Statement of Changes in Net Position (SCNP) of $39,520 million (unaudited) for FY 2007. The difference is primarily related to: (1) $5,718 million in certain trust and special fund receipts not reflected in the unexpended appropriations section of the Statement of Changes in Net Position; (2) $(34) million for the decrease in amounts appropriated from certain Treasury-managed trust funds; (3) $1,611 million related to refunds and drawbacks; (4) $(324) million for receipts unavailable for obligations upon collection from certain trust and special funds; and (5) $1 million for a temporary reduction/cancellation returned by appropriation.

In FY 2006, appropriations received on the SBR of $45,748 million (unaudited) (restated) did not equal the amounts reported on the Statement of Changes in Net Position of $39,529 million (unaudited) (restated) due to: (1) $5,177 million of trust and special fund receipts that are not reflected in the unexpended appropriation section of the SCNP; (2) $(42) million for the decrease in amounts appropriated from specific Treasury-managed trust funds; (3) $974 million of refunds and drawbacks; and (4) $110 million of receipts unavailable for obligations upon collections.

32. Custodial Revenues

The Department collects revenue from a variety of duties, excise taxes, and various other fees, some of which are refunded. Refunds and drawbacks by entry year for the fiscal years ended September 30 (in millions):

Entry Year	2007 (Unaudited)	2006 (Unaudited) (Restated)
2007	$5,531	$ -
2006	222	596
2005	327	143
2004	363	90
Prior Years	479	331
Total Refunds and Drawbacks	**$6,922**	**$1,160**

Non-entity revenue reported on the Department's Statement of Custodial Activity include duties, excise taxes, and various non-exchange fees collected by CBP and USCIS that are subsequently remitted to the Treasury General Fund or to other Federal agencies. CBP assesses duties, taxes, and fees on goods and merchandise brought into the United States from foreign countries. At the time an importer's merchandise is brought into the United States, the importer is required to file entry documents. Generally, within ten working days after release of the merchandise into the United States commerce, the importer is to submit an entry document with payment of estimated duties, taxes, and fees.

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.
- **Excise taxes:** amounts collected on imported distilled spirits, wines, and tobacco products.
- **User fees:** amounts designed to maintain U.S. harbors and to defray the cost of other miscellaneous service programs. User fees include application fees collected from employers sponsoring nonimmigrant petitions.
- **Fines and penalties:** amounts collected for violations of laws and regulations.
- **Refunds:** overpayments of duties, taxes, fees, and interest to an importer/exporter for which the importer/exporter needs to reimburse the payer. Refunds include drawback remittance paid when imported merchandise, for which duty was previously paid, is exported from the United States.

Disbursements from the refunds and drawback account for the fiscal years ended September 30, 2007 and 2006, consisted of the following (in millions):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Refunds	$6,296	$646
Drawback	626	514
Total Refunds and Drawbacks	**$6,922**	**$1,160**

The increase in the disbursements for refunds from FY 2006 to FY 2007 relates to the payment of Canadian Softwood lumber duties previously collected and interest previously accrued. The disbursements include interest payments of $655 million and $111 million, for the fiscal years ended September 30, 2007 and 2006, respectively (unaudited).

The disbursement totals for refunds include antidumping and countervailing duties collected that are refunded pursuant to rulings by the Department of Commerce (DOC). These duties are refunded when the DOC issues a decision in favor of the foreign industry.

The total amounts of antidumping and countervailing duties vary from year to year depending on decisions from DOC. Antidumping and countervailing duty refunds (included in total refunds presented above) and associated interest refunded for the fiscal years ended September 30, 2007 and 2006, consisted of the following (in millions):

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Antidumping and Countervailing Duty Refunds	$5,034	$381
Interest	655	86
Total Antidumping and Countervailing Duty Refunds	**$5,689**	**$467**

33. National Disaster Medical Systems Transfer

The transfer of the National Disaster Medical Systems (NDMS) pursuant to P.L. 109-295 had an effect on all of Department's FY 2007 financial statements, except for Statement of Custodial Activity.

The following lines of the Department's Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, and Statement of Budgetary Resources include transfer of assets, liabilities, net position, and budgetary resources of the NDMS as of January 1, 2007, the date of transfer.

Balance Sheet (In Millions)	
Fund Balance with Treasury	$90
Property, Plant and Equipment	1
Total Assets	91
Accounts Payable	2
Unexpended Appropriations	88
Cumulative Results of Operations	1
Total Liabilities and Net Position	$91

Statement of Changes in Net Position (In Millions)	
Appropriations Transferred In/Out - Unexpended Appropriations	$88
Other Financing Sources/Non-Exchange: Transfers In/Out without Reimbursement	$1

Statement of Budgetary Resources (In Millions)	
Budgetary Resources - Budget Authority - Net Transfers, Current Year	$40
Budgetary Resources - Budget Authority - Net Transfers, Balances	$31
Changes in Obligated Balances, Actual transfers, unpaid obligations	$18

34. Restatements

A. TSA Restatement (Unaudited)

Aviation Security Fee Reporting. The Department has restated the FY 2006 principle statements, excluding the Statement of Custodial Activity, and related footnotes as a result of an error in the accounting for the reduction of the Aviation Security Appropriation through a return of appropriated balances to Treasury. In prior years the security fees collected to provide aviation security were recorded as revenue. At the end of each fiscal year TSA recorded a rescission in an amount equal to the security fees and were returned to the Treasury General Fund. TSA should have been returning unexpended appropriations to Treasury equivalent to the security fees collected. The accounting treatment has been updated for FY 2007.

Prior to the implementation of this accounting change the Unexpended Appropriations were understated and the Cumulative Results of Operations were overstated. In addition, smaller adjustments were made to correct incorrect data in accounts receivable and accounts payable, also resulting in an adjustment to Cumulative Results of Operations.

Accounts Payable Reporting. The Department restated the FY 2006 Balance Sheet, Statement of Changes in Net Position, and the Statement of Net Cost, and related footnotes as a result of an error in recording accounts payable during FY 2005 through FY 2006 that resulted from FY 2004 and FY 2005 estimated accruals not reversed. This error caused the Accounts Payable balance to be overstated and the Unexpended Appropriations balance to be understated.

Correction to the Statement of Budgetary Resources. During FY 2005, TSA identified $248 million of unrecorded obligations resulting in an adjustment to the FY 2004 Statement of Budgetary Resources, which incorrectly carried forward to the beginning balances of the FY 2006 Statement of Budgetary Resources. The beginning balances to FY 2006 were incorrectly carried forward and as a result required correction for FY 2007 reporting.

B. ICE, USCIS, NPPD, S&T, and MGMT Restatements (Unaudited)

During FY 2007, in conjunction with their service provider, several Components began implementation of corrective action plans to identify and correct erroneous balances attributed to legacy data. As a result of these corrective actions five Components, ICE, USCIS, NPPD, S&T, and MGMT, restated their FY 2006 financial statements to correct errors in accounting. The restatement affected accounts payable, PP&E, accrued FECA liability, net position, and the associated budgetary balances. These restatements affected each of the principal financial statements, except for the Statement of Custodial Activity.

During FY 2007, US-VISIT, reported as a part of NPPD, reviewed its internal use software inventory to identify and correct costs that should have been capitalized. The corrections resulted in restating PP&E and operating expense, and affected the Balance Sheet, Statement of Net Cost, and the Statement of Changes in Net Position.

C. FLETC Restatement (Unaudited)

The Department restated their FY 2006 financial statements due to FLETC's FY 2006 audit adjustments related to reclassifications of PP&E construction-in-progress projects and re-computations of capital lease amortization, which occurred after the Department's statements were published in accordance with OMB A-136. These restatements affected each of the principal financial statements, except for the Statement of Custodial Activity.

D. Other Restatements (Unaudited)

Based on additional information obtained in FY 2007, the Department reclassified balances for four earmarked funds reported by OIG as a part of Departmental Operations and Others and ICE. These reclassifications affected the Balance Sheet, Statement of Changes in Net Position, and the Earmarked footnote disclosure.

The Department also recorded miscellaneous restatements resulting in a reduction in the accounts receivable and an increase to Fund Balance with Treasury. These restatements affected each of the principal financial statements, except for the Statement of Net Cost and the Statement of Custodial Activity.

BALANCE SHEET, in millions	Original 2006	Effects of Restatements	Restated 2006	Description Reference
ASSETS				
Intragovernmental				
Fund Balance With Treasury	$59,568	$1	$59,569	D
Investments, Net	634	-	634	
Accounts Receivable	248	(1)	247	D
Other				
Advances and Prepayments	2,912	1	2,913	B
Due from Treasury	411		411	
Total Intragovernmental	**$63,773**	**$1**	**$63,774**	
Cash and Other Monetary Assets	$99	$ -	$99	
Accounts Receivable, Net	1,181	-	1,181	
Taxes, Duties, and Trade Receivables, Net	1,755	-	1,755	
Direct Loans, Net	161	-	161	
Inventory and Related Property, Net	677	-	677	
General Property, Plant, and Equipment, Net	11,036	115	11,151	B, C
Other				
Advances and Prepayments	551	-	551	
TOTAL ASSETS	**$79,233**	**$116**	**$79,349**	
LIABILITIES				
Intragovernmental				
Accounts Payable	$1,900	$7	$1,907	B
Debt	17,446	-	17,446	
Other				
Due to the General Fund	1,809	-	1,809	
Accrued FECA Liability	323	16	339	B
Other	187	-	187	
Total Intragovernmental	$21,665	$23	$21,688	
Accounts Payable	$2,765	$(136)	$2,629	A, B
Federal Employee and Veteran Benefits	32,278	-	32,278	
Environmental and Disposal Liabilities	245	-	245	
Other				
Accrued Payroll	1,362	-	1,362	
Deferred Revenue and Advances from Others	2,188	-	2,188	
Deposit Liability for Canadian Softwood Lumber	34	-	34	

BALANCE SHEET, in millions	Original 2006	Effects of Restatements	Restated 2006	Description Reference
Insurance Liabilities	3,567	-	3,567	
Refunds and Drawbacks	5,593	-	5,593	
Other	1,190	15	1,205	C
Total Liabilities	$70,887	$(98)	$70,789	
Net Position				
Unexpended Appropriations- Earmarked Funds	$18	$(18)	$ -	D
Unexpended Appropriations- Other Funds	48,084	732	48,816	A, B, D
Cumulative Results of Operations- Earmarked Funds	(19,328)	(9)	(19,337)	D
Cumulative Results of Operations-Other Funds	(20,428)	(491)	(20,919)	A, B, C, D
Total Net Position	8,346	214	8,560	
TOTAL LIABILITIES AND NET POSITION	**$79,233**	**$116**	**$79,349**	

STATEMENT OF NET COST, in millions	Reclassified 2006[2]	Effects of Restatements	Restated 2006	Description Reference
Directorates and Other Components				
U.S. Customs and Border Protection				
Gross Cost	$7,135	$ -	$7,135	
Less Earned Revenue	(153)	-	(153)	
Net Cost	6,982	-	6,982	
U.S. Coast Guard				
Gross Cost	10,011	-	10,011	
Less Earned Revenue	(424)	-	(424)	
Net Cost	9,587	-	9,587	
U.S. Citizenship and Immigration Services				
Gross Cost	1,609	(21)	1,588	B
Less Earned Revenue	(1,729)	-	(1,729)	
Net Cost	(120)	(21)	(141)	
Federal Emergency Management Agency				
Gross Cost	28,845	-	28,845	
Less Earned Revenue	(2,469)	-	(2,469)	
Net Cost	26,376	-	26,376	
Federal Law Enforcement Training Center				
Gross Cost	312	-	312	
Less Earned Revenue	(33)	-	(33)	
Net Cost	279	-	279	
National Protection and Preparedness Directorate				
Gross Cost	820	(77)	743	B
Less Earned Revenue	(1)	-	(1)	
Net Cost	819	(77)	742	
U.S. Immigration and Customs Enforcement				
Gross Cost	4,487	13	4,500	B
Less Earned Revenue	(857)	-	(857)	
Net Cost	3,630	13	3,643	

[2] As discussed in Note 1, Summary of Significant Accounting Policies, the FY 2006 financial statements have been reclassified to conform with the FY 2007 presentation.

STATEMENT OF NET COST, in millions	Reclassified 2006[2]	Effects of Restatements	Restated 2006	Description Reference
Department Operations and Other				
Gross Cost	852	-	852	
Less Earned Revenue	(2)	-	(2)	
Net Cost	850	-	850	
Office of Health Affairs				
Gross Cost	53	-	53	
Less Earned Revenue	-	-	-	
Net Cost	53	-	53	
U.S. Secret Service				
Gross Cost	1,471	-	1,471	
Less Earned Revenue	(18)	-	(18)	
Net Cost	1,453	-	1,453	
Science and Technology Directorate				
Gross Cost	843	-	843	
Less Earned Revenue	-	-	-	
Net Cost	843	-	843	
Transportation Security Administration				
Gross Cost	6,043	(42)	6,001	A
Less Earned Revenue	(2,477)	-	(2,477)	
Net Cost	3,566	(42)	3,524	
NET COST OF OPERATIONS	**$54,318**	**($127)**	**$54,191**	

[2] As discussed in Note 1, Summary of Significant Accounting Policies, the FY 2006 financial statements have been reclassified to conform with the FY 2007 presentation.

STATEMENT OF CHANGES IN NET POSITION, in millions	**Original 2006**	**Effects of Restatements**	**Restated 2006**	**Description Reference**
Cumulative Results of Operations				
Beginning Balances	$(41,847)	$ -	$(41,847)	
Adjustments:				
Changes in accounting principles	-	-	-	
Corrections of Errors	-	(588)	(588)	A, B, C
Beginning balance, as adjusted	**$(41,847)**	**$(588)**	**$(42,435)**	
Budgetary Financing Sources:				
Appropriations Used	$52,895	$(23)	$52,872	A, B, D
Non-Exchange Revenue	2,527	-	2,527	
Donations and Forfeitures of Cash and Cash Equivalents	68	-	68	
Transfers in/out without Reimbursement	362	(1)	361	D
Other	(181)	(15)	(196)	
Other Financing Sources (Non-Exchange):				
Donations and Forfeitures of Property	6	-	6	
Transfers in/out reimbursement	30	-	30	
Imputed Financing	702	-	702	
Total Financing Sources	56,409	(39)	56,370	
Net Cost of Operations	(54,318)	127	(54,191)	A, B, C, D
Net Change	**2,091**	**88**	**2,179**	
Cumulative Results of Operations	**$(39,756)**	**$(500)**	**$(40,256)**	
Unexpended Appropriations:				
Beginning Balance	$87,131	$ -	$87,131	
Adjustments:				
Corrections of errors	-	676	676	A, B
Beginning Balance, as adjusted	**$87,131**	**$676**	**$87,807**	
Budgetary Financing Sources:				
Appropriations Received	$39,529	$ -	$39,529	
Appropriations transferred in/out	(573)	-	(573)	
Other Adjustments	(25,090)	15	(25,075)	B, D
Appropriations Used	(52,895)	23	(52,872)	A, B, D
Total Budgetary Financing Sources	(39,029)	38	(38,991)	
Total Unexpended Appropriations	**48,102**	**714**	**48,816**	
NET POSITION	**$8,346**	**$214**	**$8,560**	

STATEMENT OF BUDGETARY RESOUCES, in millions	Original 2006		Effects of Restatements		Restated 2006		
	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Description Reference
BUDGETARY RESOURCES							
Unobligated Balance, brought forward October 1	$56,879	$26	$26	$ -	$56,905	$26	B
Recoveries of Prior Year Unpaid Obligations	3,654	-	86	-	3,740	-	B
Budget Authority:							
Appropriations	45,748	-	-	-	45,748	-	
Borrowing Authority	17,500	629	-	-	17,500	629	
Earned:							
Collected	9,092	478	1	-	9,093	478	B
Change in Receivable from Federal Sources	39	-	(1)	-	38	-	A
Change in Unfilled Customer Orders:							
Advance Received	(541)	-	-	-	(541)	-	
Without Advance From Federal Sources	186	481	-	-	186	481	
Expenditure transfers from trust funds	49	-	-	-	49	-	
Subtotal	72,073	1,588	-	-	72,073	1,588	
Non-expenditure transfers, net; anticipated and actual	(228)	-	-	-	(228)	-	
Temporarily Not Available Pursuant to Public Law	(29)	-		-	(24)	-	B
Permanently Not Available	(25,173)	(334)	1	-	(25,172)	(334)	D
TOTAL BUDGETARY RESOURCES	**$107,176**	**$1,280**	**$118**	-	**$107,294**	**$1,280**	

STATEMENT OF BUDGETARY RESOUCES, in millions	Original 2006 Budgetary	Original 2006 Non-Budgetary Credit Reform Financing Accounts	Effects of Restatements Budgetary	Effects of Restatements Non-Budgetary Credit Reform Financing Accounts	Restated 2006 Budgetary	Restated 2006 Non-Budgetary Credit Reform Financing Accounts	Description Reference
STATUS OF BUDGETARY RESOURCES							
Obligations Incurred:							
Direct	$85,843	$1,280	$(340)	-	$85,503	$1,280	A, B
Reimbursable	4,289	-	198	-	4,487	-	B
Subtotal	**90,132**	**1,280**	**(142)**	**-**	**89,990**	**1,280**	
Unobligated Balance:							
Apportioned	11,365	-	489	-	11,854	-	A, B, D
Exempt from Apportionment	80	-	-	-	80	-	
Subtotal	**11,445**	**-**	**489**	**-**	11,934	-	
Unobligated Balance Not Available	5,599	-	(229)	-	5,370	-	A, B, D
TOTAL STATUS OF BUDGETARY RESOURCES	**$107,176**	**$1,280**	**$118**	**$ -**	**$107,294**	**$1,280**	

STATEMENT OF BUDGETARY RESOUCES, in millions	Original 2006		Effects of Restatements		Restated 2006		
	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Budgetary	Non-Budgetary Credit Reform Financing Accounts	Description Reference
CHANGE IN OBLIGATED BALANCE							
Obligated Balance, Net							
Unpaid obligations brought forward, October 1	$40,456	$ -	$(26)	$ -	$40,430	$ -	B
Less: Uncollected customer payments from Federal Sources, brought forward, October 1	(1,845)	-	-	-	(1,845)	-	
Total unpaid obligated balance, net	38,611	-	(26)	-	38,585	-	
Obligations incurred, net	90,132	1,280	(142)	-	89,990	1,280	A, B
Less: Gross Outlays	(83,674)	(639)	(1)	-	(83,675)	(639)	A, B
Obligated balance transferred, net							
Actual transfers, unpaid obligations	-	-	-	-	-	-	
Total unpaid obligated balance transferred, net	-	-	-	-	-	-	
Recoveries of Prior Year Unpaid Obligations, Actual	(3,654)	-	(86)	-	(3,740)	-	B
Change in uncollected customer payments from Federal Sources	(225)	(481)	1	-	(224)	(481)	A
Obligated balance, net end of period							
Unpaid obligations	43,260	642	(255)	-	43,005	642	A, B
Less: Uncollected customer payments from Federal Sources	(2,070)	(482)	1	-	(2,069)	(482)	A
Total, unpaid obligated balance, net end of period	41,190	160	(254)	-	40,936	160	
Net Outlays							
Gross Outlays	83,674	639	1	-	83,675	639	A, B
Less: Offsetting Collections	(8,600)	(478)	(1)	-	(8,601)	(478)	B
Less: Distributed Offsetting Receipts	(4,821)	-	-	-	(4,821)	-	
NET OUTLAYS	**$70,253**	**$161**	**$ -**	**$-**	**$70,253**	**$161**	

35. Reconciliation of Net Cost of Operations (Proprietary) to Budget (Formerly the Statement of Financing)

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 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.

In accordance with Revised OMB Circular No. A-136, *Financial Reporting Requirements*, dated June 29, 2007, the Statement of Financing is presented as a footnote disclosure and is no longer a basic financial statement, as had been presented in prior years. The information provided in the FY 2006 Statement of Financing is also presented in this footnote, to provide comparative disclosures, as required. The reconciliation of net cost of operations to budget for FY 2007 and FY 2006 is as follows:

	2007 (Unaudited)	2006 (Unaudited) (Restated)
Resources Used to Finance Activities		
Budgetary Resources Obligated		
Obligations Incurred (Note 25)	$62,002	$91,270
Less: Spending Authority from Offsetting Collections and Recoveries	(15,942)	(13,524)
Obligations Net of Offsetting Collections and Recoveries	46,060	77,746
Less: Offsetting Receipts	(4,952)	(4,821)
Net Obligations	41,108	72,925
Other Resources		
Donations and Forfeiture of Property	4	6
Transfers in (out) Without Reimbursement	9	30
Imputed Financing from Costs Absorbed by Others	839	702
Net Other Resources Used to Finance Activities	852	738
Total Resources Used to Finance Activities	**$41,960**	**$73,663**
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	$512	$1,976

Resources that Fund Expenses Recognized in Prior Periods	(1,500)	19,576
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	336	(478)
Other	(2,354)	(2,433)
Resources that Finance the Acquisition of Assets	2,925	2,681
Other Resources or Adjustments to Net Obligated Resources that do not Affect Net Cost of Operations	1,733	1,669
Total Resources Used to Finance Items Not Part of the Net Cost of Operations	1,652	22,991
TOTAL RESOURCES USED TO FINANCE THE NET COST OF OPERATIONS	**$40,308**	**$50,672**

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	$85	$140
Increase in Environmental and Disposal Liability	34	66
Increase in Exchange Revenue Receivable from the Public	(1)	(182)
Other		
Increase in Insurance Liabilities	3	-
Increase in Actuarial Pension Liability	2,200	1,721
Increase in USCG Military Post Employment Benefits	6	37
Increase in Actuarial Health Insurance Liability	265	658
Other	(1,768)	366
Total Components of Net Cost of Operations that will Require or Generate Resources in Future Periods	824	2,806
Components not Requiring or Generating Resources		
Depreciation and Amortization	1,130	1,157
Revaluation of Assets or Liabilities	65	(72)
Other	488	(372)
Total Components of Net Cost of Operations that will not Require or Generate Resources	1,683	713
Total Components of Net Cost of Operations That Will Not Require or Generate Resources in the Current Period	**2,507**	**3,519**
NET COST OF OPERATIONS	**$42,815**	**$54,191**

36. Explanation for Change in Accounting Method on the Statement of Changes in Net Position

Effective October 1, 2006, DHS adopted the reporting provisions of trust funds with multiple program agencies. This change was a result of clarifying language on mixed fund reporting added to OMB Circular A-136. Under this accounting method, DHS will report TAFS 20X8147 Bureau of Public Debt (BPD) Trust Fund account balance and transaction activity for the Sport Fish Restoration Boating Trust Fund (SFRBTF). OMB Circular A-136 requires that DHS report this trust fund since the USCG is the agency that reports the trust fund activity in the President's Budget, and to which funds are appropriated for distribution to other program agencies.

In accordance with OMB Circular A-136, DHS applied the reporting provisions trust funds prospectively beginning in FY 2007. To initially record the SFRBTF balance DHS recorded assets, including fund balance with Treasury and investments totaling approximately $1.7 billion, and offsetting liabilities to other program agencies totaling approximately $1 billion. In addition, the change in accounting for the SFRBTF required an adjustment to beginning of the year cumulative results of operations totaling $693 million, as shown on the statement of Statement of Changes in Net Position. The SFRBTF is considered an earmarked fund and accordingly significant account balances and activity is reported in Note 22.

37. Explanation for Difference between the Current Year Beginning Balances and the Prior Year Ending Balances

DHS Current Year Beginning Balances and Prior Year Ending Balances have differences due to reinstatement of a TAFS at FEMA. The TAFS was reinstated in accordance with *P.L. 109-295, Section 542, Authorizes Disaster Assistance for Unmet Needs* funds provided to the City of Cuero, TX to be available for use until September 30, 2007. However, this public law was approved after FY 2006 financial reporting. In December 2006, FEMA, working with Financial Management Services, had the TAFS reinstated and the period of availability extended. Consequently, these funds were not legally available to be included in the Prior Year Ending Balances. Therefore, the Statement of Budgetary Resources has differences for the current year and prior year balances for Unobligated Balances Brought Forward of $9 million, Unpaid Obligations of $31 million, and Total Unpaid Obligations of $31 million.

Further, the current year beginning balance was adjusted for the Statement of Changes in Net Position, Unexpended Appropriations for $37 million.

Required Supplementary Information (Unaudited, see Auditors' Report)

1. Stewardship PP&E

Heritage Assets

USCG and CBP maintain Heritage Assets, located in the United States, including the Commonwealth of Puerto Rico. Heritage Assets are property, plant, and equipment that have historical or national significance; cultural, educational, or artistic importance; or significant architectural characteristics. Heritage Assets are generally expected to be preserved indefinitely. Multi-use Heritage Assets have more than one purpose such as an operational purpose and historical purpose.

The following table summarizes activity related to Heritage Assets for the fiscal years ended September 30 (in number of units).

2007 (Unaudited)	USCG	CBP	FEMA	Total
Beginning Balance	20,425	4	1	20,430
Additions	278	-	-	278
Withdrawals	(154)	-	-	(154)
Ending Balance	**20,549**	**4**	**1**	**20,554**

2006 (Unaudited) (Restated)	USCG	CBP	FEMA	Total
Beginning Balance	20,254	4	1	20,259
Additions	349	-	-	349
Withdrawals	(178)	-	-	(178)
Ending Balance	**20,425**	**4**	**1**	**20,430**

USCG possesses artifacts that can be divided into four general areas: ship's equipment, lighthouse and other aids-to-navigation items, military uniforms, and display models. Historical artifacts are also gifted to USCG. Withdrawals are made when items have deteriorated through inappropriate display, damage due to moving and transportation, or environmental degradation.

- Ship's equipment is generally acquired when the ship is decommissioned and includes small items such as sextants, ship's clocks, wall plaques, steering wheels, bells, binnacles, engine order telegraphs, and ship's name boards. Conditions will vary based upon use and age.

- Aids-to-navigation items include fog and buoy bells, lanterns, lamp changing apparatus, and lighthouse lenses. Buoy equipment is usually acquired when new technology renders the equipment obsolete. Classical lighthouse lenses can vary in condition. The condition is normally dependent on how long the item has been out of service. The lenses go to local museums or USCG bases as display items.
- Military uniforms are generally donated by retired USCG members and include clothing, as well as insignia and accessories. Most clothing is in fair to good condition, particularly full dress items.
- Display models are mostly of USCG vessels and aircraft. These are often builders' models. Display models are generally in very good condition. Builders' models are acquired by USCG as part of the contracts with the ship or aircraft builders. The withdrawal of display models normally results from excessive wear.

USCG also has non-collection type Heritage Assets, such as sunken vessels and aircraft, under the property clause of the U.S. Constitution, Articles 95 and 96 of the International Law of the Sea Convention, 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. USCG 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 which may be aboard, and to preserve culturally valuable relics of USCG's long and rich tradition of service to our Nation in harm's way.

Buildings and Structures – USCG does not acquire or retain heritage buildings and structures without an operational use. Most real property, even if designated as historical, is acquired for operational use and is transferred to other government agencies or public entities when no longer required for operations. Of USCG buildings and structures designated as Heritage, including memorials, recreational areas, and other historical areas, over two-thirds are multi-use Heritage. The remaining assets are historical lighthouses, which are no longer in use and awaiting disposal; their related assets; and a gravesite.

CBP also has four multi-use Heritage Assets located in Puerto Rico, and FEMA has one multi-use Heritage Asset that is used by the U.S. Fire Administration for training in Emmitsburg, Maryland. All multi-use Heritage Assets are reflected on the Balance Sheet and related footnotes. Deferred maintenance information for Heritage Assets and general PP&E is presented in the required supplementary information.

2. Deferred Maintenance

The Department Components use condition assessment as the method for determining 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, 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 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 percent of facilities and item of equipment in each of the good, fair, or poor categories.

Deferred maintenance as of September 30, 2007, was estimated to range from $777 million to $1,064 million on general property, plant, and equipment and Heritage Assets with a range of poor to good condition. In FY 2006, the Department reported estimated deferred maintenance of $771 million to $967 million 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 and which is delayed for a future period.

A summary of deferred maintenance at September 30, 2007, is presented below (in millions):

	Low estimate	**High estimate**	**Asset Condition**
Building & Structures	$573	$814	Good to Poor
Equipment (vehicles and vessels)	204	249	Good to Fair
Heritage assets	-	1	Fair
Total	**$777**	**$1,064**	

3. Statement of Budgetary Resources

Schedule of FY 2007 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, Oct 1	$2,297	$1,881	$419	$9,166	$90	$654	$1,468	$218	$279	$56	$408	$377	**$17,313**
Recoveries of Prior Year Obligations	199	-	59	3,022	14	215	915	42	47	14	70	341	**4,938**
Budget Authority:													
Appropriations	11,191	8,551	2,323	10,700	275	4,209	8	1,636	965	1,494	978	4,161	**46,491**
Spending Authority from Offsetting Collections:													
Earned:													
Collected	1,514	575	35	3,803	136	1,141	-	400	-	23	35	2,637	**10,299**
Change in Receivable from Federal Sources	(34)	(11)	2	9	9	(8)	-	25	-	2	2	(1)	**(5)**
Change in Unfilled Customer Orders:													
Advance Received	(3)	38	-	42	-	(1)	-	-	2	(6)	1	5	**78**
Without Advance From Federal Sources	(20)	(8)	(14)	669	(28)	(45)	1	52	1	(4)	(2)	(17)	**585**
Previously Unavailable	-	-	-	(1)	-	-	-	-	-	-	-	-	**(1)**
Expenditure transfers from trust funds	3	45	-	-	-	-	-	-	-	-	-	-	**48**
Subtotal	12,651	9,190	2,346	15,222	392	5,296	9	2,113	968	1,509	1,014	6,785	**57,495**
Non-expenditure transfers, net; anticipated and actual	373	323	-	67	-	(8)	17	6	(4)	8	-	5	**787**
Temporarily Not Available Pursuant to Public Law	-	-	-	-	-	-	-	-	-	-	-	-	-
Permanently Not Available	(102)	(222)	(12)	(135)	(3)	(28)	-	(18)	(5)	(21)	(128)	(67)	**(741)**
TOTAL BUDGETARY RESOURCES	**$15,418**	**$11,172**	**$2,812**	**$27,342**	**$493**	**$6,129**	**$2,409**	**$2,361**	**$1,285**	**$1,566**	**$1,364**	**$7,441**	**$79,792**
STATUS OF BUDGETARY RESOURCES													
Obligations Incurred:													
Direct	$11,036	$8,956	$1,939	$17,308	$289	$4,560	$966	$1,467	$908	$1,468	$1,045	$6,740	**$56,682**
Reimbursable	1,487	551	28	1,552	123	1,066	-	462	1	16	24	10	**5,320**
Subtotal	12,523	9,507	1,967	18,860	412	$5,626	966	1,929	909	1,484	1,069	6,750	**62,002**
Unobligated Balance:													
Apportioned	17	923	233	5,999	64	300	528	336	170	47	291	245	**9,153**
Exempt from Apportionment	-	92	-	5	-	-	-	-	-	-	-	-	**97**
Subtotal	17	1,015	233	6,004	64	300	528	336	170	47	291	245	**9,250**
Unobligated Balance Not Available	2,878	650	612	2,478	17	203	915	96	206	35	4	446	**8,540**
TOTAL STATUS OF BUDGETARY RESOURCES	**$15,418**	**$11,172**	**$2,812**	**$27,342**	**$493**	**$6,129**	**$2,409**	**$2,361**	**$1,285**	**$1,566**	**$1,364**	**$7,441**	**$79,792**

Schedule of FY 2007 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	$3,067	$3,144	$640	$27,673	$265	$1,649	$1,802	$758	$773	$307	$1,256	$2,344	**$43,678**
Uncollected customer payments from federal sources, brought forward, Oct 1	(375)	(233)	(25)	(981)	(153)	(484)	-	(175)	(1)	(21)	(34)	(69)	**(2,551)**
Total unpaid obligated balance, net	2,692	2,911	615	26,692	112	1,165	1,802	583	772	286	1,222	2,275	**41,127**
Obligations incurred, net	12,523	9,507	1,967	18,860	412	5,626	966	1,929	909	1,484	1,069	6,750	**62,002**
Gross Outlays	(11,356)	(8,839)	(1,814)	(18,208)	(443)	(4,889)	(3)	(1,348)	(926)	(1,444)	(1,153)	(6,045)	**(56,468)**
Obligated balance transferred, net	34	-	(34)	(18)	-	-	15	2	(12)	-	(5)	-	**(18)**
Recoveries of Prior Year Unpaid Obligations	(199)	-	(59)	(3,022)	(14)	(215)	(915)	(42)	(47)	(14)	(70)	(341)	**(4,938)**
Change in uncollected customer payments from Federal Sources	55	20	12	(679)	19	54	-	(81)	(1)	2	-	18	**(581)**
Obligated balance, net end of Period													
Unpaid Obligations	4,070	3,813	700	25,285	220	2,172	1,865	1,296	697	333	1,097	2,707	**44,255**
Uncollected customer payments from Federal Sources	(321)	(214)	(13)	(1,660)	(134)	(431)	-	(253)	(2)	(19)	(34)	(50)	**(3,131)**
Total, unpaid obligated balance, net, end of period	3,749	3,599	687	23,625	86	1,741	1,865	1,043	695	314	1,063	2,657	**41,124**
NET OUTLAYS													
Net Outlays													
Gross Outlays	11,356	8,839	1,814	18,208	443	4,889	3	1,348	926	1,444	1,153	6,045	**56,468**
Offsetting collections	(1,515)	(657)	(35)	(3,846)	(135)	(1,140)	-	(400)	(2)	(18)	(36)	(2,642)	**(10,426)**
Distributed offsetting receipts	(2,361)	(23)	(2,080)	(61)	(1)	(155)	(1)	2	-	-	1	(273)	(4,952)
Net Outlays	**$7,480**	**$8,159**	**$(301)**	**$14,301**	**$307**	**$3,594**	**$2**	**$950**	**$924**	**$1,426**	**$1,118**	**$3,130**	**$41,090**

Schedule of FY 2006 Budgetary Resources by Responsibility Segments (in millions) (Restated) (page 1 of 2)

	CBP	USCG	USCIS	FEMA	FLETC	ICE	OHA	DepOps	NPPD	USSS	S&T	TSA	TOTAL
BUDGETARY RESOURCES													
Unobligated balance, brought forward, October 1	$1,724	$1,254	$318	$49,285	$76	$425	$2,324	$170	$284	$79	$276	$716	**$56,931**
Recoveries of Prior Year Obligations	217	-	155	2,565	55	348	-	43	44	-	179	134	**3,740**
Budget Authority:													
Appropriations	9,254	8,762	1,813	12,556	308	3,743	-	960	982	1,436	1,502	4,432	**45,748**
Borrowing Authority	-	-	-	18,129	-	-	-	-	-	-	-	-	**18,129**
Spending Authority from Offsetting Collections:													
Earned:													
Collected	1,291	561	25	3,912	87	1,271	-	426	9	18	10	1,961	**9,571**
Change in Receivable from Federal Sources	9	18	1	2	2	3	-	(1)	-	3	2	(1)	**38**
Change in Unfilled Customer Orders:													
Advance Received	1	30	(5)	(524)	-	(14)	-	-	-	(2)	(18)	(9)	**(541)**
Without Advance From Federal Sources	42	33	13	441	109	(2)	-	(6)	(5)	9	32	1	**667**
Expenditure transfers from trust funds	3	46	-	-	-	-	-	-	-	-	-	-	**49**
Subtotal	10,600	9,450	1,847	34,516	506	5,001	-	1,379	986	1,464	1,528	6,384	**73,661**
Non-expenditure transfers, net; anticipated and actual	244	280	-	(750)	-	16	-	(4)	-	-	(14)	-	**(228)**
Temporarily Not Available Pursuant to Public Law	-	-	-	(24)	-	-	-	-	-	-	-	-	**(24)**
Permanently Not Available	(160)	(485)	(11)	(23,865)	(7)	(39)	-	(35)	(25)	(49)	(35)	(795)	**(25,506)**
TOTAL BUDGETARY RESOURCES	**$12,625**	**$10,499**	**$2,309**	**$61,727**	**$630**	**$5,751**	**$2,324**	**$1,553**	**$1,289**	**$1,494**	**$1,934**	**$6,439**	**$108,574**
STATUS OF BUDGETARY RESOURCES													
Obligations Incurred:													
Direct	$9,033	$8,027	$1,868	$52,033	$308	$3,826	$856	$906	$1,008	$1,409	$1,491	$6,018	**$86,783**
Reimbursable	1,295	591	22	535	233	1,275	-	428	2	29	35	42	**4,487**
Subtotal	10,328	8,618	1,890	52,568	541	5,101	856	1,334	1,010	1,438	1,526	6,060	**91,270**
Unobligated Balance:													
Apportioned	293	1,271	107	7,001	73	275	1,468	161	246	5	404	550	**11,854**
Exempt from Apportionment	-	66	-	14	-	-	-	-	-	-	-	-	**80**
Subtotal	293	1,337	107	7,015	73	275	1,468	161	246	5	404	550	**11,934**
Unobligated Balance Not Available	2,004	544	312	2,144	16	375	-	58	33	51	4	(171)	**5,370**
TOTAL STATUS OF BUDGETARY RESOURCES	**$12,625**	**$10,499**	**$2,309**	**$61,727**	**$630**	**$5,751**	**$2,324**	**$1,553**	**$1,289**	**$1,494**	**$1,934**	**$6,439**	**$108,574**

Schedule of FY 2006 Budgetary Resources by Responsibility Segments (in millions) (Restated) (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	$2,398	$3,061	$636	$27,010	$114	$1,273	$999	$550	$915	$243	$952	$2,279	**$40,430**
Uncollected customer payments from federal sources, brought forward, October 1	(323)	(182)	(11)	(538)	(42)	(483)	-	(182)	(6)	(9)	-	(69)	**(1,845)**
Total unpaid obligated balance, net	2,075	2,879	625	26,472	72	790	999	368	909	234	952	2,210	**38,585**
Obligations incurred, net	10,328	8,618	1,890	52,568	541	5,101	856	1,334	1,010	1,438	1,526	6,060	**91,270**
Gross Outlays	(9,441)	(8,535)	(1,731)	(49,372)	(335)	(4,372)	(53)	(1,084)	(1,107)	(1,374)	(1,044)	(5,866)	**(84,314)**
Recoveries of Prior Year Unpaid Obligations	(218)	-	(156)	(2,565)	(55)	(348)	-	(43)	(43)	-	(178)	(134)	**(3,740)**
Change in uncollected customer payments from Federal Sources	(52)	(51)	(14)	(443)	(111)		-	7	5	(12)	(34)	-	**(705)**
Obligated balance, net end of Period													
Unpaid Obligations	3,067	3,144	639	27,642	265	1,654	1,802	757	775	307	1,256	2,339	**43,647**
Uncollected customer payments from Federal Sources	(375)	(233)	(25)	(982)	(153)	(483)	-	(175)	(1)	(21)	(34)	(69)	**(2,551)**
Total, unpaid obligated balance, net, end of period	2,692	2,911	614	26,660	112	1,171	1,802	582	774	286	1,222	2,270	**41,096**
NET OUTLAYS													
Net Outlays													
Gross outlays	9,441	8,535	1,731	49,372	335	4,372	53	1,084	1,107	1,374	1,044	5,866	**84,314**
Offsetting collections	(1,295)	(637)	(20)	(3,389)	(87)	(1,256)	-	(426)	(9)	(17)	8	(1,951)	**(9,079)**
Distributed offsetting receipts	(2,349)	(33)	(2,041)	(7)	(6)	(111)	-	-	-	(1)	-	(273)	**(4,821)**
Net Outlays	**$5,797**	**$7,865**	**$(330)**	**$45,976**	**$242**	**$3,005**	**$53**	**$658**	**$1,098**	**$1,356**	**$1,052**	**$3,642**	**$70,414**

4. Statement of Custodial Activity

Substantially all duty, tax, and fee revenues collected by CBP are remitted to various General Fund accounts maintained by Treasury. Treasury further distributes these revenues to other Federal agencies in accordance with various laws and regulations. CBP transfers the remaining revenue (generally less than two percent of revenues collected) directly to other Federal agencies, the Governments of Puerto Rico and the U.S. Virgin Islands, or retains funds as authorized by law or regulations. 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 all regulations are followed. If CBP believes 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 their claim of a lower amount due or to cancel the additional amount due in its entirety. Work in progress will continue until all protest options have expired or an agreement is reached. 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 2007 and FY 2006, CBP had legal right to collect \$1.9 billion and \$1.8 billion of receivables, respectively. There was an additional \$2.7 billion and \$2.4 billion representing records still in the protest phase for FY 2007 and FY 2006, respectively. CBP recognized as write-offs \$183 million and \$204 million respectively, of assessments that the Department has statutory authority to collect at September 30, 2007 and 2006, but has no future collection potential. Most of this amount represents fines, penalties, and interest.

USCG collects various fines, penalties, and miscellaneous user fees from the public that are deposited to the General Fund miscellaneous receipts of the U.S. Treasury. USCG does not collect taxes or duties. As of September 30, 2007 and 2006, USCG had outstanding general fund receipt receivables due to the Treasury General Fund of \$7 million and \$10 million, respectively.

USCIS collects user fees from employers for nonimmigrant petitions under two Congressionally mandated programs. All user fees are collected when the petition is submitted. USCIS retains a portion of the fees to fund specific program expenses and transfers the remaining balance to other Federal agencies.

5. Risk Assumed Information

The Department has performed an analysis of the contingencies associated with the unearned premium reserve for the NFIP. That analysis shows unearned premium reserve is less than the estimated present value of unpaid expected losses by $500 to $600 million. 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. The range is designed to straddle the resulting estimate.

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

Required Supplementary Stewardship Information (Unaudited, see Auditors' Report)

1. Stewardship Investments

Due to the transformational nature of DHS programs, stewardship investment information is presented only for FY 2007. 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 benefit. The Department's FY 2007 expenditures (including carryover funds expended in FY 2007) in Human Capital and Research and Development are shown below:

Summary of Stewardship Investments (in millions)

Programs	Human Capital	Research and Development
S&T – Research and Development Programs	$ -	$316.7
FEMA	101.4	-
Total	$101.4	$316.7

2. Investments in Human Capital

These investments include expenses incurred for programs for education and training of the public that are intended to increase or maintain national productive capacity and that produce outputs and outcomes that provide evidence of maintaining or increasing national productive capacity. Based on a review of the Department's programs, FEMA has made significant investments in Human Capital.

Program	Performance Measure	FY 2007 Target	FY 2007 Results
Grants Program	Percent of jurisdictions demonstrating acceptable performance on applicable critical tasks in exercises using Grants and Training approved scenarios.	40%	72%
Grants Program	Percent of State and local homeland security agency grant recipients reporting measurable progress towards identified goals and objectives to prevent and respond to terrorist attacks.	65%	67%
National Preparedness	Percent of respondents reporting they are better prepared to deal with disasters and emergencies as a result of training	91%	89%
National Preparedness	Percent of Radiological Emergency Preparedness Program communities with a nuclear power plant that are fully capable of responding to an accident originating at the site.	100%	100%

Program	Performance Measure	FY 2007 Target	FY 2007 Results
National Preparedness	Percent increase in knowledge, skills, and abilities (KSAs) of State and local homeland security preparedness professionals receiving training.	27%	25%
Urban Areas Security Initiative Grants - FEMA	Percent of participating urban area grant recipients reporting measurable progress made towards identified goals and objectives to prevent and respond to terrorist attacks.	65%	63% estimated

3. Investments in Research and Development

These investments represent expenses incurred to support the search for new or refined knowledge and ideas for the application or use of such knowledge for the development of new or improved products and processes with the expectation of maintaining or increasing national productive capacity or yielding other future benefits. The following table shows key FY 2007 targets and results for research and development.

Program	Performance Measure	FY 2007 Target	FY 2007 Results
Border and Maritime Security	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	100%	80%
Border and Maritime Security	Percentage of transition program funding dedicated to developing technologies in direct response to DHS Components' requirements.	94%	98%
Chemical and Biological	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	88%	89%
Chemical and Biological	Percent completion of an effective restoration technology to restore key infrastructure to normal operation after a chemical attack.	35%	30%
Command, Control and Interoperability	Percent of States that have initiated or completed a statewide interoperability plan, such as the Statewide Communications Interoperability Plan.	36%	89%
Command, Control and Interoperability	Cumulative number of cyber security data sets contained in protected repository.	85	263
Command, Control and Interoperability	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	75%	75%
Explosives	Number of new or improved technologies available for transition to the customers at a Technology Readiness Level (TRL) six or above.	2	0
Explosives	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	80%	61%

Program	Performance Measure	FY 2007 Target	FY 2007 Results
Human Factors	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	90%	73%
Infrastructure and Geophysical	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	90%	69%
Infrastructure and Geophysical	Number of scenarios completed on the Critical Infrastructure Protection-Decision Support System that provide actionable information to help protect U.S. critical infrastructure.	8	4
Innovation	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	45%	83%
Laboratory Facilities	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	100%	93%
Testing and Evaluation and Standards	Number of Department of Homeland Security official technical standards introduced.	20	19
Testing and Evaluation and Standards	Percent of standards introduced that are adopted by Department of Homeland Security and partner agencies.	85%	84%
Testing and Evaluation and Standards	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	70%	88%
Transition	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	80%	100%
SAFETY Act	Percentage of full SAFETY Act applications that have been processed and feedback provided to applicant when package has been disapproved.	100%	100%
University Programs	Percent of peer review adjectival ratings on University Programs' management and research and education programs that are "very good" or "excellent."	60%	N/A – No reviews conducted
University Programs	Percentage of milestones that are met, as established in the fiscal year's budget execution plan.	80%	60%

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 a Management Response.

Tax Burden/Tax Gap

Revenue Gap

The Compliance Measurement Program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations, and agreements, and it estimates the revenue gap.

The revenue gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and agreements using a statistically valid sample of the revenue losses and overpayments detected during Compliance Measurement entry summary reviews conducted throughout the year.

For FY 2006 and 2005, the actual revenue gap was $450 and $470 million, respectively. CBP calculated the preliminary FY 2007 and 2006 revenue gap to be $374 and $314 million, respectively. The projected over-collection and under-collection amounts due to noncompliance for FY 2007 were $61.6 million and $435 million, respectively. The projected over-collection and under-collection amounts due to noncompliance for FY 2006 were $128 million and $442 million, respectively. The preliminary overall trade compliance rate for FY 2007 and 2006 is 98.1 and 96.6 percent, respectively. With overall compliance at a high level, CBP has been able to emphasize matters of significant trade risk.

The final overall trade compliance rate and estimated revenue gap for FY 2007 will be issued in January, 2008.

Summary of Financial Statement Audit and Management Assurances

Table 16 and Table 17 provide a summary of the financial statement audit and management assurances for FY 2007.

Table 16. Summary of Financial Statement Audit Material Weaknesses

Audit Opinion	Disclaimer					
Restatement	Yes					
Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Financial Management and Entity Level Controls	1					1
Financial Reporting	1					1
Financial Systems Security	1					1
Fund Balance with Treasury	1					1
Property, Plant and Equipment	1					1
Operating Materials and Supplies	1			✓		0
Legal and Other Liabilities	1					1
Budgetary Accounting	1					1
Actuarial Liabilities	1			✓		0
Intragovernmental Balances	1			✓		0
Total Material Weaknesses	10	0	0	(3)	0	7

The Department's Independent Public Accountant reported seven material weakness conditions at the Department level in FY 2007, which is reduced from ten reported in FY 2006. The reduction is attributed to the consolidation of the prior year Intragovernmental Balances, Operating Materials and Supplies, and Actuarial Liabilities conditions into the Financial Reporting and Capital Assets and Supplies, and Other Liabilities material weaknesses, respectively. Finally, the Legal Liability portion of the Other Liabilities material weakness condition displayed above was corrected.

Table 17. Summary of Management Assurances

Effectiveness of Internal Control Over Financial Reporting (Federal Managers' Financial Integrity Act § 2 and the Department of Homeland Security Financial Accountability Act)						
Statement of Assurance	No Assurance					
Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Entity Level Controls	1					1
General Ledger Management	1					1
Fund Balances with Treasury Management	1					1
Financial System Security	1					1
Budget Resource Management	1					1
Property Management	1					1
Operating Materials and Supplies Management	1			✓		0
Grants Management	1					1
Insurance Management	0	✓				1
Human Resource and Payroll Management	1					1
Intragovernmental and Intradepartmental Balances	1			✓		0
Total Material Weaknesses	10	1	0	(2)	0	9

Effectiveness of Internal Controls Over Operations (Federal Managers' Financial Integrity Act § 2)						
Statement of Assurance	Qualified					
Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Implementing and Transforming DHS	1				✓	0
Establishing Appropriate and Effective Information Sharing Mechanisms	1				✓	0
National Flood Insurance Program	1				✓	0
Entity Level Controls	0	✓				1
Improper Payments Information Act Noncompliance	0	✓				1
Anti-Deficiency Act Controls	0	✓				1
Security Controls over Collection and Depositing of Fees	0	✓				1
Federal Protective Service Transformation	0	✓				1
DHS Headquarters Consolidation	0	✓				1
Acquisition Management	0	✓				1
Human Capital Management	0	✓				1
Information Technology Management	0	✓				1
Long Term Strategic Planning and Outcome Based Management	0	✓				1
Total Material Weaknesses	3	10	0	0	(3)	10

Conformance with Financial Management Systems Requirements (Federal Managers' Financial Integrity Act § 4)						
Statement of Assurance	No Assurance					
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
Integrated Financial Management Systems	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	

Effectiveness of Internal Control Over Financial Reporting

Pursuant to the *Department of Homeland Security Financial Accountability Act*, the Department focused its efforts on corrective actions to design and implement Department-wide internal controls. Although the Secretary made no assertion about the operating effectiveness of internal controls over financial reporting, a qualified assurance on the design effectiveness was provided to appropriately represent the status of DHS's corrective action efforts and to facilitate implementation of the Act's audit opinion requirement.

The Secretary reported nine material weakness conditions at the Department level in FY 2007, which is reduced from ten reported in FY 2006. The reduction is attributed to the consolidation of the prior year Intragovernmental/Intradepartmental Balances and Operating Materials and Supplies conditions into the General Ledger Management and Property Management material weaknesses, respectively. Differences between conditions reported by DHS Management and the Independent Public Accountant (IPA) is largely due to the Department's grouping of material weakness conditions by financial management processes as defined by the General Services Administration's Financial Systems Integration Office (FSIO). For example, the material weakness definition used by the IPA for Actuarial and Other Liabilities contains similar conditions as the Grants Management and Human Resource Management material weaknesses reported by DHS Management. The FSIO process definitions aid corrective actions and facilitate development of standard business processes. In FY 2006, Legal Liabilities was included as a portion of the Grants Management material weakness condition reported in Table 17 above. Legal Liabilities was corrected as reported by the Department's IPA in FY 2007.

On March 1, 2007, the Department issued the inaugural version of the Internal Controls Over Financial Reporting (ICOFR) Playbook. The ICOFR Playbook outlines the Department's strategy and process to correct material weakness conditions and build management assertions for internal controls. Since the ICOFR Playbook's publication, the Secretary and the Department's Chief Financial Officer have monitored the ICOFR Playbook's implementation on a monthly basis.

The ICOFR Playbook includes two tracks. The first track focuses on executing corrective actions to eliminate material weakness conditions. Highlights of significant Component level corrective actions executed during FY 2007 include the following:

- Strengthened the control environment and bolstered Office of the Chief Financial Officer oversight functions with the strong support of the Department's Secretary and Under Secretary for Management;
- Executed year two of the Department's multi-year plan for OMB Circular No. A-123, resulting in the Secretary's first ever assurance statement on the design effectiveness of internal controls over financial reporting;
- Partnered with the Under Secretary for Management, Chief Information Officer, and Chief Information Security Officer, to achieve compliance with the *Federal Information Security Management Act*;
- Corrected material weakness conditions for Legal Liabilities and reduced the severity of Capitalization of Internal Use Software to a significant deficiency condition;
- Corrected TSA's Financial Reporting material weakness condition and reduced the severity of TSA's Capital Assets and Other Liabilities conditions to significant deficiencies;

- Sustained FY 2006 progress at ICE and eliminated all remaining ICE material weakness conditions;
- Designed Department-wide financial reporting process improvements; and
- Developed Department-wide financial management policies and procedures.

The second track of the ICOFR Playbook focuses on building support for the Secretary's assurance statement through management-performed testing on areas without auditor-identified material weakness conditions. In FY 2007, DHS achieved a breakthrough milestone by implementing corrective actions to remediate pervasive material weakness conditions. As a result, DHS is achieving the intended outcome of the *Department of Homeland Security Financial Accountability Act* by designing and implementing internal controls to support the DHS mission.

Significant internal control challenges remain largely at USCG and FEMA. To support these Components, the Department's Chief Financial Officer will conduct monthly corrective action meetings with Senior Management and weekly working group meetings with Senior Staff. Table 18 below summarizes material weaknesses in internal controls as well as planned corrective actions with estimated target correction dates.

Table 18. Material Weaknesses in Internal Controls

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
Financial Management and Entity Level Controls: U.S. Coast Guard (USCG) and Federal Emergency Management (FEMA) have not stabilized entity level controls related to the USCG and FEMA control environment. Several key factors are needed to strengthen the control environment, including the development of human capital, cultural transformations, organizational structures, and financial management/oversight monitoring mechanisms. USCG and FEMA are responsible for the establishment, maintenance, and assessment of internal controls to meet the objectives of the Federal Managers' Financial Integrity Act (FMFIA).	USCG and FEMA	USCG will continue to develop a financial management organization to include recruiting additional skilled staff. Additionally, USCG will continue to develop an internal control program. FY 2008 will include updating to the tests of design conducted in prior fiscal years and tests of effectiveness in accordance with DHS guidance. FEMA is in the process of establishing an Internal Control Board to coordinate and manage various internal control remediation activities while measuring and reporting on tangible results toward achieving FEMA's goal for improved internal controls. In the spring of 2006 an agency wide strategic planning team was established to begin updating the current strategic plan in accordance with the Secretary's priorities, FEMA vision, Post Katrina Emergency Management Reform Act of 2006, and other internal/external drivers. In the Fall of 2006, the FEMA administrator held an agency-wide leadership conference to establish a vision and identify core competencies to support the FEMA mission. Following the conference FEMA began the implementation of the vision. A framework for the strategic plan was presented to Agency leadership at an August 2007 leadership conference. The updated strategic plan is expected to be completed and aligned to the Secretary's Near Term Goals by December 2007.	FY 2009

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
Financial Reporting: At USCG, there is a lack of noncompliance with the requirements of the Federal Financial Management Improvement Act (FFMIA) as well as the lack of policies and procedures, and controls surrounding its financial reporting process. At FEMA, the overall organizational structure continues to pose challenges surrounding management oversight, experienced financial managers and staff, noncompliance with OMB Circular No. A-50 and the lack of policies and procedures for many roles, responsibilities, processes and functions performed within FEMA. Conditions remain at DHS Headquarters (DHS HQ) and operational offices related to implementation of a consolidated financial reporting process, including Intragovernmental Account Reconciliations.	USCG, FEMA, and DHS HQ	USCG will make business process improvements and systems changes, in coordination with DHS's Oracle financial systems initiative. In addition, USCG will utilize the Department's internal control process to design and establish internal controls over its component level financial reporting process. USCG will also integrate disparate general ledgers into the single authoritative source. In addition to improving the current USCG Treasury Information Executive Repository process that consolidates three general ledger systems for financial statement reporting, evaluate use of the Informatica tool as a mechanism to facilitate a consolidated general ledger database for the review and analysis of abnormal balances and analytics. Continue operational, documentation, and control improvements surrounding abnormal account balances, budgetary to proprietary account reconciliations, suspense account activity, and liability estimates. FEMA will develop comprehensive policies and procedures to establish effective financial reporting control activities. DHS HQ will continue to formalize, publish, and implement relevant policies and procedures that clearly define the roles and responsibilities across the Department for financial reporting. In addition, DHS HQ will develop comprehensive procedures (and expand on existing standard operating procedures) ensuring accurate reporting through a management oversight function which includes various quality control identifiers within DHS HQ as well as throughout the Department. DHS HQ will establish Office of Financial Management internal staffing plans to include responsibilities based on current, back-up and future cross training responsibilities.	FY 2010
Financial Systems Security: The Department's Independent Public Accountant had identified Financial Systems Security as a material weakness in internal controls at USCG, FEMA, and TSA due to a myriad of inherited control deficiencies surrounding general computer and application controls. The Federal Information Security Management Act mandates that Federal Agencies maintain IT security programs in accordance with the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance.	FEMA, USCG, and TSA	Additional oversight will be provided by the Offices of the Chief Financial Officer (OCFO) and the Chief Information Security Officer in order to increase common FISMA and Federal Information System Controls Audit Manual security control alignment based on: Federal Information Processing Standards (FIPS) 199 Information Categories for Financial Reporting; POA&M (Plan of Action and Milestone) views to ensure Component based Financial Audit Notice of Findings and Recommendations (NFRs) are being closed in a timely manner; General security control convergence based on NIST Special Publication (SP) 800-53 and OMB Circular No. A-123 control categories for financially significant systems; Identified gaps between the A-123 requirements and existing DHS requirements (including NIST SP 800-53) and adjusting policy as appropriate; and Component OCFO Certification and Accreditation (C&A) Review and Approval for all Financial Significant Systems.	FY 2008
Fund Balance with Treasury: USCG did not implement effective internal controls to accurately clear suspense transactions in order to perform accurate and timely reconciliations of Fund Balance with Treasury (FBWT) accounts.	USCG	USCG will make systems and business process changes to enable reconciliation of FBWT for retired and annuitant pay. An interim solution will be explored to make improvements in the reconciliation of active duty and reserve pay while the new active and reserve pay system is being developed. Business process improvements and systems changes, in coordination with DHS's Oracle financial systems initiative, will be made to reduce the volume of transactions posted to suspense accounts. Documentation and control activities over suspense transactions will be improved.	FY 2010
Capital Assets and Supplies (CAS): The controls and related processes surrounding USCG CAS to accurately and consistently record CAS are either not in place or contain errors and omissions. For example, physical inventory processes for CAS and the methodologies and assumptions to support the total value of CAS are not yet fully developed and implemented. Asset identification,	USCG and FEMA	In the area of repairable spares, the USCG will develop a single set of financial policies and procedures, review the classification of repairable spares, remove excess and obsolete material from field units, and re-baseline inventory through the execution of physical inventories. In the area of real property management, the USCG will use Department of Defense's methodology to value pre-1995 assets. The Target Asset Review & Inventory Validation (TARIV) process	FY 2010

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
mapping, and tagging are also areas of weakness within CAS at the USCG. Internal controls and related policies and procedures for physical inventory counts at USCG field locations have not been completely developed and implemented. As a result, DHS has not implemented the Statement of Federal Financial Accounting Standard (SFFAS) No. 3, Accounting for Inventory and Related Property. In FY 2007, the Department's Auditor identified a new condition related to accounting for stockpiles at FEMA.		will be established and implemented to identify, accurately measure, and reclassify targeted assets. Establish policy and procedures for documenting real property additions, deletions, and changes to meet Chief Financial Officer Act requirements. In the area of personal property, the USCG will use inspection and assistance visits to units to validate internal control remediation efforts. Report annual capitalized certification letters accurately and on time. Ensure confirmation and certifications are accurate and timely to support existence and completeness of USCG inventory counts and valuation. In the area of Construction in Progress, the USCG will ensure complete policies are issued to support key assertions related to existence, completeness, and valuation for capitalized assets. Ensure policies, procedures, proper internal controls, and oversight is in place so additions, modifications, and removals are processed timely and accurately. Develop systems requests to add functionality to properly account for and track all costs for capitalized assets. Develop training for personnel responsible for capitalized assets. In the area of Operating Materials and Supplies, the USCG will re-baseline unit inventory through the execution of physical inventories, with onsite management oversight. Support the valuation of the baseline inventory and implement policies and procedures to sustain the accurate valuation. Remove excess and obsolete material from field units. FEMA will identify the root causes in order to mitigate the new material weakness based on the Auditor's recommendations by the first quarter of FY 2007.	
Budgetary Accounting: Accounts payable and obligations were identified as not recorded accurately and timely in the financial systems of DHS Components, which could lead to non-compliance with laws and regulations such as the Anti-Deficiency Act. Specifically, there is a need for overall improved recording, monitoring, reporting, and close outs over all DHS obligations and reconciling budgetary vs. proprietary account relationships.	USCG, FEMA, and TSA	USCG will implement a systems upgrade that will record prior year recoveries at the transaction level. In addition an effort is underway to revise standard operating procedures and train staff on new system capabilities. FY 2010 on-budget request submitted to substantially enhance oversight and monitoring with the addition of Full Time Equivalence (FTE) and contractor support. FEMA will implement modifications system interfaces to ensure contract obligation data is accurately and completely transferred between financial and acquisitions systems and establish a process to reconcile data, and identify key personnel to assist in facilitating the unliquidated obligations (ULO) review process for applicable budget object classes. FEMA will establish Program Office, Joint Field Office, and Regional Office Points of Contact by title with responsibility to perform the quarterly ULO reviews. Implement a process to track and monitor these reviews. Establish a FEMA Budget Execution Working Group, as a sub-group of the FEMA Investment Working Group, to oversee the assessment, redesign, and implementation of the FEMA budget execution process. Transportation Security Administration (TSA) will ensure that ULO reviews are executed timely and effectively. The TSA Office of Acquisition has created a Contract Closeout Section to review and close out purchase contracts in a timely manner.	FY 2010

Effectiveness of Internal Control Over Operations

DHS efforts for effectiveness of internal control over operations focused on developing corrective action plans. Most notably, the Department expanded its financial reporting corrective action planning process to support the Under Secretary for Management organization in unifying plans to strengthen DHS operations and management in the core focus areas of:

- Acquisition Management;
- Human Capital Management;
- Security Management;
- Information Technology Management; and
- Long Term Strategic Planning and Outcome Based Management.

This effort will be another significant step in the maturation of the Department. Our FY 2008 goal for internal control over operations is to implement a single, comprehensive, and integrated management approach to organize and focus all Department-wide internal control efforts.

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 utilizes OMB guidance and considers the results of the OIG, annual financial statement audits, and Federal Information Security Management Act (FISMA) compliance reviews. As reported in the Secretary's Management Assurance Statements, DHS financial management systems do not substantially conform to government-wide requirements. However, significant consolidation efforts are in progress to modernize, certify, and accredit all financial management systems in accordance with FISMA.

Financial Management Systems Framework

The President's Management Agenda: The President's Management Agenda (PMA) specifies that a clean financial audit and timely, useful, and reliable financial information are critical to improving financial and budget management performance government-wide. In support of these PMA objectives, the DHS Office of the Chief Financial Officer (OCFO) has undertaken a Department wide initiative to consolidate the financial management systems that support the Component agencies. A top priority for the OCFO, this initiative is part of the strategic DHS financial management framework that addresses a full range of issues in the areas of people, policy, process, systems, and assurance to achieve the goals of the PMA and the Department.

Financial Management Systems Strategy and Vision: In September 2006, the Department prudently ended its previous systems improvement effort, eMerge². The Department determined that rather than build a new system from scratch (the eMerge² strategy), it should leverage existing system investments with proven audit success. This effort, called the Transformation and Systems Consolidation (TASC) initiative, plans to consolidate financial systems by migrating Components to one of the two DHS Financial System Integration Office (FSIO) certified financial systems – Oracle Federal Financials and Systems Applications Products (SAP). TASC will consolidate over 97 percent of DHS to these two baselines by FY 2011. Following completion of the consolidation plan to two systems, a single Baseline will be chosen as the Department standard. The Department is committed to a single Baseline as the end state for its financial management needs.

TASC is a joint effort between the Department's Office of the Chief Financial Officer and Office of the Chief Information Officer. OMB reviewed the TASC strategy in March, 2007 and the TASC expenditure plan was submitted to Congress in April, 2007. The Chief Financial Officer and Chief Information Officer testified before Congress regarding this initiative on June 28, 2007.

Analysis of Alternatives: The TASC approach was carefully developed after a thorough business and alternatives analysis of the five primary software applications in the Department's inventory. From this analysis, it was determined that moving to two systems - Oracle Federal Financials, used at the Transportation Security Administration (TSA), and SAP, used at Customs and Border Protection (CBP) – is the most cost-effective, strategic solution. The TASC Oracle Baseline offers a suite of industry-recognized tools including Oracle Federal Financials, Compusearch PRISM, Sunflower Assets, and 170 Systems' MarkView.

The TASC SAP Baseline similarly offers an integrated suite of tools for comprehensive financial management. SAP is widely implemented across the Federal environment including multiple implementations in the Department of Defense, NASA, and the Department of the Interior. These standards-based software applications meet financial business requirements, are scalable, and are proven within the DHS operating environment. Each Component migration brings the Department closer to achieving a clean audit opinion.

Migration Plan: The migration process involves a systematic, phased approach whereby smaller Components will migrate first. Phased migrations promote greater understanding of the Components' business processes and provide for flexibility in sequencing Component migrations. Furthermore, because the Department has already successfully migrated TSA, DNDO, and the Federal Air Marshal Service (FAMS) to Oracle, DHS will be repeating proven and successful migration processes while using lessons learned from these migrations for future migrations.

Benefits and Compliance: By consolidating to fewer systems, DHS will leverage its investment across Components to provide more robust financial management and become a more accountable steward of taxpayer dollars. The TASC initiative facilitates compliance with applicable Federal laws and regulations and satisfies the requirements of the PMA for improving financial and budget management government-wide by:

- Supporting an OMB-compliant accounting line to provide DHS decision makers with more accurate, timely, and reliable information;
- Strengthening Department-wide financial accountability, moving DHS closer to a sustainable clean audit opinion;
- Providing the foundation for effective internal controls and segregation of duties supported by a compliant software baseline;
- Eliminating reporting errors via the removal of manual processes and controls;

- Utilizing real-time interoperability to streamline reporting across the financial management enterprise;
- Supporting an approved Chart of Accounts compliant with the United States Standard General Ledger (USSGL) and OMB Circular A-127;
- Ensuring compliance with the National Institute of Standards and Technology Special Publication 800-53 – Recommended Security Controls for Federal Information Systems and the GAO's Federal Information System Controls Audit Manual;
- Achieving FMLoB compliance by standardizing data collection and transaction processes throughout the organization;
- Supporting robust reporting requirements and enabling the Secretary's Priority 12.2 to unify IT infrastructure;
- Minimizing the information security risks by consolidating from seven to two financial systems. Eliminating five financial management systems will better enable the Department to meet the PMA, FISMA and FFMIA. Central control will ensure that transaction processing occurs in a secure environment;
- Supporting information security requirements through the use of a single sign-on feature (cross-functional, cross-system interactions will not require the end-user to log on to each system) with regular security upgrades/patches built into the underlying Government Off-the-Shelf and Custom Off-the-Shelf suite of applications;
- Providing optimal mission support through efficient finance, procurement, and asset management operations and business processes; and
- Integrating with Department-wide initiatives, such as the PMA's e-Gov Travel.

In support of the PMA, the OCFO is undertaking a Department-wide initiative to improve financial management operations. With the TASC Initiative, the OCFO is leveraging proven systems that currently exist in the Department to increase efficiencies, save taxpayer dollars, and support a clean audit opinion. Utilizing an effective phased and repeatable migration process that incorporates lessons learned and focuses on compliance, the OCFO is taking a proven approach to meeting the PMA and Department's goals.

Federal Information Security Management Act (FISMA)

The E-Government Act of 2002 (Public Law 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 *2007 Federal Information Security Management Act (FISMA) Report and Privacy Management Report* consolidated reports from three DHS offices:

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

In FY 2007, the Department continued to implement improvements to the DHS information system security program, and the CIO documented improvements in the following areas of FISMA:

- Department Oversight;

- Information Systems Inventory;
- Certification and Accreditation;
- Plan of Action and Milestones;
- Configuration Management;
- Incident Detection, Handling, and Analysis; and
- Security Training.

FISMA Department Oversight - Policy and Procedures

A number of policy updates to the DHS Sensitive Systems Policy Handbook (DHS 4300A) were issued over the past year and are published on the DHS intranet Web site at the CISO home page.

The Department uses two enterprise tools for facilitating agency-wide security management and compliance tracking against DHS policies and procedures, and a number of procedural updates were provided during the course of the year. These tools serve as the basis for generating monthly FISMA scorecard reports to the Components that track six compliance metrics for both classified and unclassified systems. The six compliance metrics include:

- Annual testing (system tests and evaluations (ST&E), and annual self-assessments);
- Plans of action and milestones (POA&Ms);
- Certifications and accreditation (C&A);
- Configuration management;
- Incident reporting; and
- Information security training.

The latest DHS 4300A Version 5.5, dated September, 30 2007, included additional security control tests and reporting requirements for CFO-designated financial systems that must performed annually. These additional controls and requirements were based on OMB Circular A-123, and grouped into the following control domains:

- Entity-wide Security Program Planning and Management;
- Access Controls;
- Application Software Development and Change Control;
- System Software;
- Service Continuity; and
- Segregation of Duties.

In addition, the OCIO implemented oversight procedures to more effectively tie OMB Exhibit 300s OCIO and CFO portfolios to DHS information system accreditation.

Information System Inventory

In FY 2007, DHS maintained a single inventory of its sensitive but unclassified general support systems and major applications, including contractor owned and operated systems, as illustrated below. The DHS inventory remains under strict change control processes and all additions, deletions, or changes to the Component’s inventory are tracked by the Department to ensure completeness. The Department identified 603 information systems in its FY 2007 FISMA Report, as shown in the table below.

Table 19. DHS FY 2005 - 2007 System Inventory Breakdown

Type of System	FY 2005	FY 2006	FY 2007
DHS-Owned Systems	543	486	396
Contractor Owned/Operated	221	206	207
Total	764	692	603

The Office of the Chief Information Officer's FY 2008 Performance Plan requires any changes to CFO-designated financial systems to document Component CFO approvals.

Certification and Accreditation (C&A)

As part of the Office of the Chief Information Officer's FY 2007 Performance Plan, the office raised the bar on accuracy and completeness of eleven artifacts used to support the DHS system certification and accreditation process. The eleven artifacts include:

- FIPS 199 Assessment;
- Authority to Operate Accreditation Letter;
- 800-53 Self Assessment;
- System Security Plan;
- Security Assessment Report;
- Risk Assessment;
- Security Test & Evaluation Plan;
- Contingency Plan;
- Contingency Plan Test Results;
- E-authentication Analysis; and
- Privacy Threshold Analysis.

DHS then established monthly metrics to monitor Component C&A compliance against published criteria in order to ensure the eleven C&A documents met departmental standards. The Office of the Chief Information Officer's FY 2007 Performance Plan also scorecards annual testing requirements. The Department's Chief Information Officer has documented significant improvements in producing key accreditation documentation, and continued to show improvements in the area of security control testing, as shown in the Table 20.

Table 20. DHS Certification and Accreditation Improvements

C&A Improvement	FY 2005		FY 2006		FY 2007	
	Number	Percent	Number	Percent	Number	Percent
Systems C&A'd	327	43	589	85	506	84[a]
Control Testing	397	52	613	89	579	96
Contingency Plan Testing	65	9	413	60	507	84
Total Systems	764	--	692	--	603	--

[a]One Component failed to provide completed C&A packages for 26 percent of its systems. This significantly reduced the Department's total for accredited systems

The Office of the Chief Information Officer's FY 2008 Performance Plan incorporates additional requirements to address artifact completeness and evidence of annual vulnerability scans. The department also plans to provide more continuous monitoring of key security controls including system configurations. For CFO designated Financial Systems, a Compliance Framework was published in the October 2007 DHS 4300A to identify FISMA SP 800-53 test procedures supporting OMB A-123 control tests.

Plans of Action and Milestones (POA&M)

The Department significantly improved Component POA&M oversight in FY 2007 as documented in the DHS POA&M Process Guide (Attachment H of DHS 4300A). POA&M scorecards were distributed monthly to the information system security managers and detailed completeness reports were distributed to the Component POA&M point-of-contacts every month. The POA&M scorecard measured the following key POA&M quality elements:

- Weakness;
- Point of Contact;
- Dollar Resources Required;
- Source of Funding;
- Scheduled Completion Date;
- Milestones; and
- Changes to Milestones.

The entire POA&M for each system or program failed if any one of the seven elements was flagged as incomplete. As of July 31, 2007, 98 percent (470 out of 480) of the Department's sensitive but unclassified systems had no POA&M element deficiency, as the table below indicates. In addition, POA&Ms have been developed for 100 percent of all financial statement audit findings.

Table 21. DHS POA&M Process Improvements

POA&M Improvements	FY 2005		FY 2006		FY 2007	
	Number	Percent	Number	Percent	Number	Percent
Systems Requiring POA&Ms	N/M[a]	--	388	55	480	--
POA&M Completeness	N/M	--	N/M	--	470	98

[a]N/M = Not Measured

The Office of the Chief Information Officer's FY 2008 Performance Plan addresses all of the OIG recommendations for POA&M improvements, including requirements to better address classified POA&Ms and ensure system test weaknesses are identified in POA&Ms. Additional Departmental oversight is targeted to ensure schedules are reasonable and resources are appropriate. POA&M reviews will also address POA&M closures and monitor delayed POA&Ms to evaluate the validity of the delay.

Configuration Management

In FY 2007, the Department deployed a compliance team to review configuration management at a Component level. The completion of these on-site reviews was incorporated into the Component's scorecard. The reviews focused on assessing Component-wide practices and usage of configuration guides, as well as the Component's change management and continuous monitoring processes.

The Office of the Chief Information Officer's FY 2008 Performance Plan incorporates additional requirements to further the continuous monitoring process for configuration management at the system level.

Incident Detection, Handling, and Analysis

In FY 2007, the Department increased employee understanding of incident reporting requirements through its annual security awareness program and specialized training on incident handling procedures. The DHS Security Operations Center (SOC) increased security and privacy incident detection support and improved the Department's handling and reporting procedures.

Office of the Chief Information Officer's FY 2008 Performance Plan identifies requirements for additional improvements in enterprise situational awareness, along with convergence of DHS networks and systems.

Security Training

In FY 2007, the Department reviewed all major Component training plans and 94 percent (15 out of 16) of Component plans were found compliant with DHS FISMA requirements. In addition, the Department continued to provide a high level of security awareness and specialized security training to its employees as the table below illustrates.

Table 22. DHS Security Training Improvements

Security Training	FY 2005		FY 2006		FY 2007	
	Number	Percent	Number	Percent	Number	Percent
Total Participants	188,167	--	207,776	--	220,149	--
Employees Receiving Awareness Training	105,847	88	155,212	74	209,309	95
Employees w/Specialized Security Responsibilities	1,142	--	1,277	--	1,372	--
Employees Receiving Specialized Training	1,109	97	1,283[1]	99	1,352	99

[1] One Component reported training provided to non-Federal employees.

At the 2007 DHS Security Conference and Workshop, the Chief Information Security Officer and Chief Security Officer presented the following tracks that focused on specialized information security topics:

- ISSO Roles and Responsibilities: Introductory Level;
- ISSO Roles and Responsibilities: Experienced Level;
- C&A for Designated Accreditation Authorities and Program Managers;
- DHS Security Management Tools;
- IT Security for CFO-Designated Financial Systems;
- Security Essentials;
- Information Security Policy and Architecture;
- Security Assessments;
- Identity Management;
- Operations and Security; and
- Privacy Policy.

These topics form the basis for defining DHS specific specialized training requirements. The Office of the Chief Information Officer's FY 2008 Performance Plan will incorporate additional requirements to address the OIG recommendations to track individuals and establish appropriate training.

FISMA Summary

OIG reviewed targeted samples of the Department's systems for security compliance and best practices. The OIG report, "Evaluation of DHS's Information Security Program for Fiscal Year 2007," identified five recommendations for security improvements. The C&A and POA&M recommendations have been identified by the CIO/CISO for incorporation into the Department's FY 2008 Performance Plan and for DHS Security Operations Center improvements. The OIG recognized the Department's progress in publishing their FY 2007 Performance Plan and monthly scorecards, policy and procedures updates, Security Operations Center Concepts of Operations, and improvements in data review and verification for FISMA reporting.

The Department's requirements to support privacy controls has increased. Currently, 254 systems in the DHS inventory contain personally identifiable information; 163 systems require a privacy impact assessment; and 224 systems require systems of records notice. The privacy office is working to improve compliance in these areas and has published policies to address privacy breach notifications, rules of behavior, and consequences for failures to comply. Additional plans have also been prepared to eliminate unnecessary use of social security numbers, and reduce usage of personally identifiable information.

Improper Payments Information Act

The Improper Payments Information Act (IPIA) of 2002 (P.L. No. 107-300) requires agencies to review their programs and activities to identify those susceptible to significant improper payments. In addition, the Defense Authorization Act (P.L. No. 107-107) established 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.

Compiling a DHS IPIA Program Inventory and Performing Risk Assessments

In FY 2006, DHS's assessment of the vulnerability of its programs to significant improper payments was limited to whether or not a program exceeded $100 million in disbursements. Sample testing of the programs identified as high-risk, resulted in two programs with improper payments exceeding $10 million and requiring corrective action plans. Both were FEMA programs - the Individuals and Households Program (IHP) and Disaster Relief Fund Vendor Payments. Sample testing was performed on Hurricane Katrina-related payments only.

Sample testing for FY 2007 focused on high visibility programs and programs that had not been tested in prior years. This approach identified a third high-risk program – CBP's Custodial Program.

In FY 2007, based on lessons learned and to achieve long-term IPIA success, DHS improved its program identification and risk assessment processes. High-quality risk assessments, which considered qualitative and quantitative factors, were completed for 65 DHS programs, totaling $61 billion in FY 2006 disbursements. Rather than a single quantitative risk factor, DHS Components considered several quantitative and qualitative risk factors, including the following: payment processing controls; quality of internal monitoring controls; human capital; complexity of the program; nature of payments; operating environment; and relevant program-specific factors. 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. Scoring was done on a 1 (low) to 5 (high) scale. Programs with an overall score of 3 or above were considered to be high-risk for issuing improper payments.

These risk assessments identified eleven new high-risk programs and split CBP's Custodial Program into two distinct groups. In summary, DHS has 15 high-risk programs, two identified in FY 2006 and thirteen identified in FY 2007. Primarily as a result of this effort, the Department's IPIA progress score on the President's Management Agenda went from Red to Green between the third and fourth quarter of FY 2007. Risk assessments will be updated early in FY 2008 (examining FY 2007 disbursements) and will serve as the basis for determining which programs to sample test.

Based on this year's assessment process, the following programs were deemed to be vulnerable to significant improper payments:

Table 23. Programs at High-Risk for Improper Payments Based on FY 2007 Risk Assessments

Component	Program Name	FY 2006 Disbursements ($ Millions)*
CBP	Custodial – Refund & Drawback	$1,376
CBP	Custodial – Continued Dumping & Subsidy Offset Act (CDSOA) & Payments to Wool Manufacturers	$226
FEMA	Insurance – National Flood Insurance Program (NFIP)	$17,935
FEMA	Grants – Public Assistance Programs	$5,425
G&T**	Grants – Homeland Security Grant Program (HSGP)	$2,298
G&T	Grants – Assistance to Firefighters Grants (AFG)	$203
G&T	Grants – Infrastructure Protection Program (IPP)	$92
ICE	Detention and Removal Operations (DRO)	$1,257
ICE	Investigations	$1,226
ICE	Federal Protective Service (FPS)	$961
TSA	Aviation Security – Payroll	$2,617
USCG	Military Payroll	$3,219
USCG	Contract Payments	$1,748
Total FY 2006 Disbursements		**$38,582**

* Excludes intragovernmental payments.
** G&T was an independent Component in FY 2006 and became part of FEMA in FY 2007.

Note: DHS has no programs previously identified in the former Section 57 of Circular A-11 (now located in OMB Circular A-123, Appendix C).

Statistical Sampling Process

Generally, a stratified sampling design was used to test payments based on the FY 2006 amounts disbursed and the assessed risk of the program. The design of the statistical sample plans and the extrapolation of sample errors across the payment populations was 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 guidance. An expected error rate of 5 percent of total payment dollars was used in the sample size calculation. Using the theory of stratified random sampling, 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:

- Identified large payment dollars as the certainty stratum;
- Assigned each payment a randomly generated number using a seed;
- Sorted the payments within each stratum (by ordered random numbers); and
- Selected the payments following the sample size design. For the certainty strata, all payments were selected.

To estimate improper payment dollars for the population from the sample data, the stratum specific ratio of improper dollars (gross, under, and overpayments, separately) to total payment dollars was calculated.

DHS sample test results are listed in Table 24. Payment population and sample size figures are in millions of dollars. Estimated error amounts are in actual dollars.

Statistical Sampling Results

Table 24. DHS Sample Test Results

Component	Program	FY 2006 Payment Population ($millions)	FY 2006 Sample Size ($millions)	Est Error Amount ($)	Est Error Percentage (%)
CBP	Custodial	1,602	284	18,423,545	1.150
	Secure Border Initiative (SBI) Net	155	86	2,020	0.001
FEMA	Disaster Relief Program-Hurricane Katrina Individuals and Households Program (Phase I) *	5,251*	2.5*	449,576,000	8.56
	Disaster Relief Program-Hurricane Katrina Individuals and Households Program (Phase II)**	920**	3.3**	133,734,431	14.53
	Disaster Relief Program-Individuals and Households Program (Phase III)***	150***	2.1***	2,624,656	1.75
	Disaster Relief Program-Hurricane Katrina Vendor Payments (Phase I)*	4,286*	825*	101,153,033*	2.36*
FLETC	Construction	72	61	1,495	0.002
	Salaries & Expenses	45	17	487	0.001
	Training	61	25	8,898	0.014
ICE	Federal Protective Service	713	157	4,838,585	0.679
TSA	Federal Air Marshall Service Contracts	55	26	13,095	0.024
	Federal Air Marshall Service Travel	56	0.5	40,286	0.072
USCG	ARSC Payment Center-Operating Expenses	180	72	0	0.000
	CGOF Payment Center-Acquisitions, Construction & Improvements	735	445	4,229	0.001
	CGOF Payment Center-Operating Expenses	1,253	146	60,448	0.005
	Oil Pollution Act/Environmental Compliance	102	95	0	0.000

* Phase I – Payments made between September 1, 2005 and March 1, 2006. The error estimates for Hurricane Katrina Vendor Payments were revised. See the notes to Table 29 for details.
** Phase II – Payments made between March 2, 2006 and November 30, 2006.
***Phase III – Payments made between July 1, 2006 and June 30, 2007 for disasters declared during these dates.

Based on the results of sample testing, corrective action plans are required for CBP's Custodial program, and FEMA's Disaster Relief Programs – IHP and Vendor Payments.

Corrective Action Plans for High-Risk Programs

Following are corrective actions plans for programs with estimated improper error amounts above $10 million.

CBP Custodial Program

The largest source of FY 2007 sample testing errors resulted from CBP's inability to provide supporting documentation. Documentation for several Refund and Drawback payment transactions was located offsite and could not be retrieved within scheduled test dates.

Table 25. In Process and Planned Custodial Program Corrective Actions

In Process and Planned Custodial Program Corrective Actions	Root Cause	Target Completion Date
Complete FY 2008 risk assessment on FY 2007 Custodial Payments.	Risk assessment was not completed early enough in FY 2007 to determine sample testing requirements.	January 2008
Review payment checklist procedures and update payment processing procedures to reflect checklist review results.	Payment review procedures needed to be completed and adjustments made appropriately.	April 2008
Conduct payment sample testing earlier in the fiscal year.	Documentation for many transactions were located offsite and required longer lead time to retrieve.	May 2008

FEMA IHP

Table 26. Completed IHP Corrective Actions

Completed IHP Corrective Actions	Root Cause	Completed Date
Make Ownership/Occupancy verification feature operational.	Ownership/Occupancy feature in NEMIS was not fully operational.	June 2006
Implement procedures and capability to do real-time quality control monitoring.	Procedures and capabilities related to real-time quality control monitoring needed improvement.	August 2006
Develop a performance metrics program to measure caseworker performance.	Performance metrics to measure caseworker performance on the processing requirements were needed.	October 2006
Recompete housing inspection contract.	Processes to ramp up operations in response to catastrophic disasters needed improvement.	March 2007
Enhance NEMIS to augment the existing NEMIS address capability.	Improvements needed within NEMIS to address capability.	April 2007
Improve Quality Control processes for manual reviews.	Controls to prevent duplicate payments or payments for incorrect amounts needed improvement.	July 2007
Conduct IPIA testing on Hurricane Katrina IHP payments between March and September 2006.	FEMA's management needed to determine the susceptibility of errors for payments made for the Disaster Relief Fund.	July 2007

Table 27. In Process and Planned IHP Corrective Actions

In Process and Planned IHP Corrective Actions	Root Cause	Target Completion Date
Complete the expedited assistance policy memo.	The process for policy creation and approval within IHP has not been fully developed.	December 2007
Put in place a contract for data verification and pre-population of verified data.	Processes to prevent and detect improper payments in a timely manner needed improvement. NEMIS upgrades preventing victims of disasters from receiving more than the Federal maximum assistance amount needed to be fully implemented.	December 2007
Develop IHP applicant recertification guidelines.	Processes needed improvements to prevent and detect improper payments in a timely manner needed improvement.	December 2007
Enhance training to assist FEMA personnel with the Lodging Expense Reimbursement System.	Knowledge gaps needed to be identified and relevant training developed.	February 2008
Award a contract to make available 6,000 call center agents.	Processes to ramp up operations in response to catastrophic disasters needed improvement.	March 2008
Develop a process for approving policy and guidance.	Certain functional areas lacked the policies and guidance needed to approve and make payments to affected individuals and households.	March 2008
Clarify and define the Separated Households Policy.	Controls to prevent duplicate payments or payments for incorrect amounts needed improvement. Certain functional areas lacked the policies and guidance needed to approve and make payments to affected individuals and households.	April 2008
Develop a process to ensure consistent application of all disaster-specific policy.	Controls to prevent duplicate payments or payments for incorrect amounts needed improvement.	June 2008

Vendor Payments

Table 28. In Process and Planned Vendor Payments Corrective Actions

In Process and Planned Vendor Payments Corrective Actions	Root Cause	Target Completion Date
Develop and require a standard COTR Appointment Letter identifying the COTR's authority.	Training of respective roles and responsibilities needed improvement.	November 2007
Conduct a review of policies, procedures, and job descriptions for Accounting Technicians.	FEMA's policies have evolved over time and have been impacted by major disasters. As a consequence, some policies lacked precision and formal documentation.	November 2007
Initiate a quality assurance review process for Vendor Payments to reduce improper vendor payments.	Processes to ramp up operations in response to catastrophic disasters needed improvement. Internal control gaps existed in the vendor payment process.	November 2007
Modify and update current training for Accounting Technicians to ensure it addresses identified improper payment problems.	Training of respective roles and responsibilities needed improvement.	January 2008
Document the Invoice Follow-up process responsibilities for Accounting Technicians to ensure invoices are paid in a timely manner.	FEMA's policies have evolved over time and have been impacted by major disasters. As a consequence, some policies lacked precision and formal documentation.	January 2008

Analyze results of the policies, procedures, and job descriptions for Accounting Technicians and create and implement changes in FEMA policies, procedures, and processes, as necessary.	Processes to ramp up operations in response to catastrophic disasters needed improvement	February 2008
Strengthen the process and controls for designating authorized invoice reviewers and approvers so that designated signatories and alternates are properly documented and readily accessible.	Payments of invoices were sometimes authorized without proper signature authority, supporting documentation, and quality checks.	July 2008
Review procurement contracting language and the standardization of contracts, where practical.	FEMA contracts were not consistently written for similar items, thereby creating issues with review and approval.	September 2008

Improper Payment Reduction Outlook for High-Risk DHS Programs

The table below summarizes improper payment amounts for DHS high-risk programs and projects future year improvements based on completing corrective actions. Improper payment (IP) percent and dollar figures are based on statistical estimates for FY 2006. These estimates are then projected for FY 2007 and beyond based on improvements expected from completing corrective actions.

Table 29. Improper Payment Reduction Outlook

Improper Payment Reduction Outlook
($ in millions)

Program	FY 2006 Outlays	FY 2006 IP%	FY 2006 IP$	FY 2007 Outlays	FY 2007 IP%	FY 2007 IP$	FY 2008 Est. Outlays	FY 2008 IP%	FY 2008 IP$	FY 2009 Est. Outlays	FY 2009 IP%	FY 2009 IP$	FY 2010 Est. Outlays	FY 2010 IP%	FY 2010 IP$
*Custodial (CBP)	$1,602	1.15	$18	$7,119	0.12	$9	$2,423	0.21	$5	$2,423	0.12	$3	$2,423	0.06	$1.5
**IHP (FEMA)	$3,902	9.45	$369	$932	9.45	$88	$2,228	5.00	$111	$2,228	2.00	$45	$2,228	1.50	$33
**Vendor Payments (FEMA)	$6,747	2.36	$159	$1,782	2.36	$42	$3,454	2.00	$69	$3,454	1.75	$60	$3,454	1.50	$51

The following programs (with actual FY 2006 and FY 2007 Outlays and Projected FY 2008-2010 Outlays listed in $millions less intragovernmental payments) will have measurements reported in DHS's FY 2008 AFR, if they are assessed as having significant improper payments as a result of the FY 2008 risk assessment of FY 2007 payments:
FEMA – National Flood Insurance Program (NFIP), (Outlays – FY 2006 $17,935; FY 2007 $1,456; FY 2008 $3,276; FY 2009 $2,556; and FY 2010 $1,150)
FEMA – Public Assistance Programs, (Outlays – FY 2006 $5,425; FY 2007 $5,098; FY 2008 $1,026; FY 2009 $1,524; and FY 2010 $1,589)
G&T – Homeland Security Grant Program (HSGP), (Outlays – FY 2006 $2,298; FY 2007 $826; FY 2008 $347; FY 2009 $545; and FY 2010 $667)
G&T – Assistance to Firefighters Grants (AFG), (Outlays – FY 2006 $203; FY 2007 $499; FY 2008 $658; FY 2009 $656; and FY 2010 $421)
G&T – Infrastructure Protection Program (IPP), (Outlays – FY 2006 $92; FY 2007 $120; FY 2008 $417; FY 2009 $466; and FY 2010 $460)
ICE – Detention and Removal Operations (DRO) , (Outlays – FY 2006 $1,257; FY 2007 $1,243; FY 2008 $1,678; FY 2009 $2,047; and FY 2010 $2,083)
ICE – Investigations, (Outlays – FY 2006 $1,226; FY 2007 $1,132; FY 2008 $1,354; FY 2009 $1,490; and FY 2010 $1,515)
***ICE – Federal Protective Service, (Outlays – FY 2006 $961; FY 2007 $801; FY 2008 $991; FY 2009 988; and FY 2010 $998)
TSA – Aviation Security – Payroll, (Outlays – FY 2006 $2,617; FY 2007 $2,883; FY 2008 $3,025; FY 2009 $3,117; and FY 2010 $3,213)
USCG – Military Payroll, (Outlays – FY 2006 $3,219; FY 2007 $3,519; FY 2008 $3,669; FY 2009 $3,805; and FY 2010 $3,946)
***USCG – Contract Payments, (Outlays – FY 2006 $1,748; FY 2007 $1,853; FY 2008 $1,965; FY 2009 $2,083; and FY 2010 $2,208)

Notes

*CBP's Custodial Program Group consists of two Custodial programs – Refund & Drawback and Continued Dumping and Subsidy Offset Act (CDSOA). These programs were sample tested together and joint figures are given throughout the table. If the CDSOA program had been listed separately, the estimated error amount would be below $10 million for all years. The estimated percentage error rate for FY 2007 Outlays is lower than for other years due to $5.6 billion ($5,573,970,512) of softwood lumber refunds which are not expected to have any errors due to very simple payment processing requirements.

An assumption to estimate future year outlays is embedded in Table 29. Future year outlays are dependent on many factors involving import and export activity, tariff decisions made by the U.S. Government, and the actions of foreign entities. The estimated outlay figures above were based on an average of the five most recent fiscal years (in millions of dollars - FY 2003 $995; FY 2004 $1,119; FY 2005 $1,282; FY 2006 $1,602; and FY 2007 $7,119).

**For these FEMA programs, two major assumptions are embedded in Table 29. The first assumption involves estimating future year outlays. The difficulty is that these programs do not have stable outlays from year to year because emergency response to Presidential declared disasters and other emergencies varies through time. The estimated outlay figures above were based on an average of the five most recent fiscal years (in millions of dollars for vendor payments – FY 2003 $774; FY 2004 $1,322; FY 2005 $6,645; FY 2006 $6,747; and FY 2007 $1,782; in millions of dollars for IHP payments – FY 2003 $684; FY 2004 $982; FY 2005 $4,638; FY 2006 $3,902; and FY 2007 $932).

The second assumption is the application of the estimated error percentage rates that came from the Phase I and Phase II IHP testing and Phase I vendor payment testing to the FY 2006 and FY 2007 outlay figures. For IHP, the estimated error rate for the combined Phase I and Phase II sample testing is 9.45 percent.

Although the Phase III IHP testing produced an error estimate below $10 million, DHS considers this program to still be at high-risk for improper payments. The favorable sample test result reflects additional internal controls FEMA implemented over IHP payments as well as an absence of catastrophic disasters. FEMA will continue to test the IHP program with the goals of: (1) confirming payment processing control improvements, (2) providing senior management with better information on the costs associated with temporarily suspending controls to expedite delivering aid to disaster victims, and (3) clarifying the costs and benefits of proposed financial system improvements.

FEMA reviewed its identified improper Hurricane Katrina Vendor Payments from Phase I and resolved 35 of the 60 identified improper payments. Based on this review, FEMA has revised its estimated improper payment rate for FY 2006 and FY 2007 for this program from 7.44 percent to 2.36 percent.

***These programs were risk assessed as high-risk but sample testing produced an estimated error below $10 million.

Recovery of Improper Payments

Since FY 2006, FEMA has collected $18 million of Hurricane Katrina IHP payments identified as improper as a result of payment sample testing. In January 2007, DHS published interim regulation 6 CFR Part 11 which took effect immediately and required FEMA to provide disaster applicants who were in recoupment with the opportunity for an oral hearing. This regulation applied to disasters declared on or after January 30, 2007. On June 13, 2007, the U.S. District Court in Ridgely applied the same criteria to disaster applicants from Hurricanes Katrina and Rita. The Ridgely injunction is in effect until FEMA develops its oral hearing policy.

Recovery Auditing

Last year, DHS did not report recovery audit results for Components because recovery audit efforts were not completed in time. This year, DHS is reporting recovery audit results for FY 2005 and FY 2006 disbursements. This contract work was completed for ICE, USCG, and the Components they cross-service (MGMT, NPPD, S&T, TSA, USCIS, and US-VISIT).

After consultation with OMB, CBP was granted relief by the DHS OCFO from performing recovery audit work. CBP made the request after recovery audit work conducted for Fiscal Years 2003 through 2005 produced negligible recovery amounts. The amount of effort expended by CBP and contractor personnel as compared to recoveries identified and subsequently collected clearly demonstrated that recovery auditing for CBP and contractor personnel is not cost effective. CBP validated and collected amounts identified by the contractor from prior year efforts. The prior year efforts included a review of FY 2003 and FY 2004 disbursements and a survey of major vendors to identify any amounts owed to CBP. CBP continues to work with the vendors to recover outstanding amounts. Continued granting of relief will be reviewed annually and is linked to risk assessment results and results of the test of design and test of operating effectiveness for key payment process controls.

Recovery audit results are listed in Table 30. Please note that the current year (CY) columns include figures for FY 2005 disbursement and FY 2006 disbursements as both years underwent recovery auditing in FY 2007. For TSA and USCG, recovery audit work began with these years which is why the prior year (PY) amounts identified for recovery are $0. Also, the amount recovered for USCG is relatively modest due to recovery audit work being completed late in the fiscal year.

Table 30. Recovery Audit Results

DHS Component	Amount Subject to Review for CY Reporting ($ Millions)	Actual Amount Reviewed and Reported CY ($ Millions)	Amounts Identified for Recovery CY ($000)	Amounts Recovered CY ($000)	Amounts Identified for Recovery PYs ($000)	Amounts Recovered PYs ($000)	Cumulative Amounts Identified for Recovery (CY + PYs) ($000)	Cumulative Amounts Recovered (CY + PYs) ($000)
CBP	N/A	N/A	N/A	$100	$184	$27	$184	$127
ICE	$4,183	$4,183	$611	$501	$1,216	$1,077	$1,827	$1,578
MGMT	$603	$603	$166	$42	$1	$0	$167	$42
NPPD	$337	$337	$166	$88	$37	$0	$203	$88
S&T	$646	$646	$53	$53	$0	$0	$53	$53
TSA	$4,574	$4,574	$91	$52	$0	$0	$91	$52
USCG	$4,969	$4,969	$282	$3	$0	$0	$282	$3
USCIS	$1,372	$1,372	$467	$374	$319	$296	$786	$670
US-VISIT	$515	$515	$0	$0	$0	$0	$0	$0

Management Accountability for IPIA

Managers are held accountable for reducing and recovering improper payments in a variety of ways. DHS receives quarterly grades from OMB on the President's Management Agenda (PMA) Eliminating Improper Payments scorecard. Similarly, Components receive quarterly grades from the Department. Recovery auditing progress is discussed at CFO level briefings. Managers are also held accountable for completing internal control work on payment processing as part of the Department's OMB Circular A-123 effort. Payment processing key controls were evaluated for test of design and documentation in FY 2007. In FY 2008, payment processing key controls will undergo test of operating effectiveness. The importance of improper payments was discussed regularly at DHS Senior Assessment Team meetings. Half-day workshops on improper payment topics were held in FY 2007 and will be expanded in FY 2008.

Agency Information Systems and Other Infrastructure

In September 2006, DHS ended its previous systems improvement effort, eMerge[2]. Rather than build a new system from scratch, existing systems will be leveraged. This effort, the Transformation and Systems Consolidation (TASC) initiative, is discussed further in the Financial Management Systems Framework (see page 223).

FEMA is improving its financial system interfaces to reduce improper payments in its Disaster Relief Fund high-risk programs. CBP is upgrading its financial system to automate the handling of Custodial payments.

The Department requested resources in its FY 2008 budget to hire additional staff so that it can enhance risk assessment procedures and conduct oversight and review of Component test plans.

Statutory or Regulatory Barriers to Reducing Improper Payments

None.

Additional Comments

The Department focused its FY 2007 efforts on completing risk assessments which it views as the foundation to a fully successful improper payments program. The Department has gained valuable benefits from its payment processing tests of key controls as required by OMB Circular A-123.

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 has been measured between 0.02 percent and 0.05 percent for the period of October 2006 through May 2007 (Note: MTS statistics are reported with at least a six week lag).

Debt Collection Improvement Act (DCIA)

The DHS Office of the Chief Financial Officer (CFO) is developing and implementing comprehensive debt collection regulations that would supersede Components' legacy agency regulations. The DHS-wide debt collection regulations will provide instructions to the components on meeting the reporting requirements in support of the Debt Collection Improvement Act of 1996 (DCIA). This act established the following purposes:

- To maximize collections of delinquent debts owed to the Federal Government by ensuring quick action to enforce recovery of debts and the use of all appropriate collection tools.
- To minimize the costs of debt collection by consolidating related functions and activities and utilizing interagency teams.
- To reduce losses arising from debt management activities by requiring proper screening of potential borrowers, aggressive monitoring of all accounts, and sharing of information within and among Federal agencies.
- To ensure that the public is fully informed of the Federal Government's debt collection policies and that debtors are cognizant of their financial obligations to repay amounts owed to the Federal Government.
- To ensure that debtors have appropriate due process rights, including the ability to verify, challenge, and compromise claims, and have access to administrative appeals procedures which are both reasonable and protect the interests of the United States.
- To encourage agencies, when appropriate, to sell delinquent debt, particularly debts with underlying collateral.
- To rely on the experience and expertise of private sector professionals to provide debt collection services to DHS components.

To achieve these purposes, the Department's goals are to: (1) overcome DCIA deficiencies by having fair, aggressive, and consistent internal programs to recover non-tax delinquent debt; (2) improve the Department's non-tax debt collection performance by promoting the resolution of delinquencies as quickly as possible; (3) refer all eligible non-tax delinquent debts to Treasury (for Treasury Offset and/or Cross Servicing) at the 180 day point as required by the DCIA; (4) reduce future write-offs of debt by implementing a debt collection strategy incorporating the authorities within OMB's Circular A-129, *Policies for Federal Credit Programs and Non-Tax Receivables (11/2000)*; (5) require that all DHS Components have finalized internal policies and procedures to ensure that potential debtors to the Federal Government have all appropriate due process rights; and, (6) ensure the accuracy and timeliness of reports on receivables by reporting, certifying, and verifying all required data on the Treasury Report on Receivables and Debt Collection Activities (TROR).

FY 2006 Biennial User Charges Review

The Chief Financial Officers Act of 1990 requires each agency's CFO to review, on a biennial basis, the fees, royalties, rents, and other charges imposed by the agency, for services and things of value provided to specific recipients, beyond those received by the general public. The purpose of these reviews 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.

A preliminary review of DHS user fees was conducted and reported by the CFO in FY 2006. This review was based on Component FY 2005 data and user fee structures that had been established through the legacy agencies. The next biennial review of user fees to be performed by DHS is scheduled to take place in FY 2008 and will be based on FY 2007 data.

Management Challenges

Office of Inspector General

U.S. Department of Homeland Security

Homeland Security

NOV - 2 2007

MEMORANDUM FOR: The Honorable Michael Chertoff
Secretary

FROM: Richard L. Skinner
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*. The report was included in DHS FY 2007 Annual Financial Report. The report, including the department's comments in their entirety, will be posted on our public website.

Should you have any questions, please call me, or your staff may contact James Taylor, Deputy Inspector General, at (202) 254-4100.

Attachment

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

OIG-08-11 November 2007

Office of Inspector General

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

Homeland Security

NOV - 2 2007

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.

The attached summary presents the major management challenges facing the Department of Homeland Security. For a more detailed analysis of these areas, please see our full report, which is included in DHS' FY 2007 Annual Financial Report. As required by *the Reports Consolidation Act of 2000*, we update our assessment of management challenges annually.

It is our hope that 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Office of Inspector General

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

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

Since its inception in March 2003, the Department of Homeland Security (DHS) has worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the missions of protecting the country against another terrorist attack, responding to threats and hazards, ensuring safe and secure borders, welcoming lawful immigrants and visitors, and promoting the free-flow of commerce has presented many challenges to its managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient, and effective organization.

The major management challenges we identify facing DHS, including department-wide and operational challenges, are a major factor in setting our priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the *Reports Consolidation Act of 2000*, Pub.L.No. 106-531, we update our assessment of management challenges annually. We have made recommendations in many, but not all, of these areas as a result of our reviews and audits of departmental operations. Where applicable, we have footnoted specific reports that require DHS' action.

The major management challenges we identified are:

- Catastrophic Disaster Response and Recovery
- Acquisition Management
- Grants Management
- Financial Management
- Information Technology Management
- Infrastructure Protection
- Border Security
- Transportation Security
- Trade Operations and Security

CATASTROPHIC DISASTER RESPONSE AND RECOVERY

Reports issued by the White House, Congress, federal offices of Inspector General, the Government Accountability Office (GAO), and others, have identified longstanding problems within the federal government to sufficiently mobilize a coordinated response operation in the event of a catastrophic disaster. The Department of Homeland Security's (DHS) failures after Hurricane Katrina ravaged the Gulf Coast illuminated a number of these issues, including questionable leadership decisions and capabilities, organizational failures, overwhelmed response and communications systems, and inadequate statutory authorities. In the two years since Hurricane Katrina, a number of federal agencies, private sector organizations, and public offices have issued reports addressing the Federal Emergency Management Agency's (FEMA) weaknesses in response to Katrina.

Additionally, Congress enacted six statutes that contain changes that apply to future federal emergency management actions. Most of the statutes contain relatively few changes to federal authorities related to emergencies and disasters. The Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act), Pub.L.No. 109-295,[1] however, contains many changes that will have long-term consequences for FEMA and other federal entities. That statute reorganizes FEMA, expands its statutory authority, and imposes new conditions and requirements on the operations of the agency. Although FEMA finds itself in a better position today than it did two years ago, it has not fully implemented the Post-Katrina Act. Many of the changes made as a result of the Act, as well as planned response capabilities for future catastrophic disasters, remain untested.

Many problems plaguing FEMA have existed for years, but they never received the attention needed to fix them because FEMA had never before dealt with such a devastating disaster. We are currently in the process of completing audits and reviews to help FEMA turn lessons learned into problems solved and are planning additional work in FY 2008 to assess FEMA's readiness to respond to future catastrophic disasters.

DHS' and FEMA's major management challenges in preparing to meet future catastrophic disasters relate to the following areas: (1) coordination of disaster response efforts, (2) catastrophic planning, (3) logistics, (4) acquisitions, (5) housing, and (6) evacuation. These six critical areas are discussed in detail below.

Coordination of disaster response efforts. When a catastrophic event occurs, disaster response and recovery efforts are not solely a FEMA responsibility – they are inherently the nation's responsibility. Therefore, a successful response to and subsequent recovery from a catastrophic event can be tied directly to the resources and capabilities of citizens, local and state governments, the federal government, nongovernmental organizations, and the private sector. FEMA is the face of our nation's response to large-scale disasters and is charged with coordinating the deployment of our nation's resources and capabilities, but success can only be realized when all stakeholders are fully prepared and willing to contribute.

[1] Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act) Pub.L.No. 109-295, Title VI, 120 Stat.1394.

FEMA's initial response to Hurricane Katrina was significantly impeded by the adjustments it was making in implementing its responsibilities under DHS' National Response Plan (NRP), which was published in December 2004. Moreover, DHS had previously published the National Incident Management System (NIMS) in March 2004. The NIMS, along with the NRP, restructured how federal, state, and local government agencies and emergency responders conduct disaster preparation, response, and recovery activities. Changes needed to implement both plans, however, were still underway when Hurricane Katrina made landfall. Unfortunately, two years later, DHS and FEMA have yet to finalize and issue the National Response Framework, the successor to the NRP, mandated in Title VI of the Post-Katrina Act. Notwithstanding that FEMA provided record levels of support to Hurricane Katrina victims, states, and emergency responders, the response to Katrina demonstrated areas where FEMA and DHS headquarters must make adjustments relating to the use of incident designations, the role of the Principal Federal Official, and the responsibilities of emergency support function coordinators.

Since FEMA is responsible for providing the necessary emergency management leadership to other federal departments, agencies, and other organizations when responding to major disasters, it is largely dependent on other agencies and outside resources to execute many activities that take place. Therefore, departments and agencies need to allocate personnel and funding to train, exercise, plan, and staff disaster response activities to enable better execution of their roles and responsibilities and plans and procedures. Specific contingency plans must be developed and integrated so that capabilities and gaps are identified and addressed.

Hurricane Katrina also highlighted the need for data sharing among federal agencies following a catastrophic disaster. However, data-sharing arrangements between FEMA and other federal agencies to safeguard against fraud and promote the delivery of disaster assistance are not in place. Critical tasks, from locating missing children and registered sex offenders to identifying duplicate assistance payments and fraudulent applications, have all been hindered because mechanisms and agreements to foster interagency collaboration did not exist prior to Hurricane Katrina.

Catastrophic Planning. Attempts to plan for an event such as Hurricane Katrina had been ongoing since 1998, but were never completed for a variety of reasons, including a lack of federal funding, other natural disasters occurring, and the terrorist attacks of September 11, 2001. According to FEMA officials, the major challenge in conducting catastrophic planning is the lack of funding. The GAO reported that requests from FEMA for $100 million for catastrophic planning and an additional $20 million for catastrophic housing planning in fiscal years 2004 and 2005, respectively, were denied by DHS.[2]

The integration of FEMA all hazards preparedness and disaster response and recovery capabilities within DHS requires additional attention. Although an "all-hazards" approach can address preparedness needs common to both man-made and natural events, DHS must ensure that all four phases of emergency management – preparedness, response, recovery, and mitigation – are managed throughout the department on an all-hazards basis. Coordination and

[2] *Hurricanes Katrina and Rita: Unprecedented Challenges Exposed the Individuals and Households Program to Fraud and Abuse; Actions Needed to Reduce Such Problems in the Future,* GAO-06-1013, September 2006.

consultation among DHS components and with state and local governments is essential to guide, advise, develop, and monitor all-hazards capabilities and responder effectiveness.

Planning and exercises also are critical to prepare for and respond to catastrophic events. FEMA recognized the need for catastrophic planning and requested resources for a number of scenarios, including earthquakes in California and along the New Madrid Seismic Zone, hurricanes along the gulf coast, and terrorist attacks. While Congress has appropriated $20 million recently for catastrophic planning, to be successful, FEMA needs to plan and conduct exercises with its federal, state, and local partners. FEMA needs to continue to develop plans and exercises for high risk scenarios and include all its emergency management partners.

Logistics. FEMA is responsible for coordinating the delivery of commodities, equipment, personnel, and other resources to support emergency or disaster response efforts, and therefore, FEMA's ability to track resources is key to fulfilling its mission. In response to Hurricane Katrina, state officials expressed frustration with the lack of asset visibility in the logistics process. FEMA used an inconsistent process involving multiple, independent computer and paper-based systems, many of which generated numerous, unique tracking numbers and few of which were cross-referenced. A White House report revealed a highly bureaucratic federal supply process that was not sufficiently flexible or efficient to meet requirements, and that failed to leverage the private sector and 21st Century advances in supply chain management.

After Hurricane Katrina, FEMA's Logistics Inventory Management System (LIMS) did not track essential commodities, such as food and water. As a result, FEMA could not readily determine its effectiveness in achieving DHS' specific disaster response goals or whether there was a need to improve the system. FEMA's disaster response culture has supported the agency through many crisis situations, such as the 2004 hurricanes. However, FEMA's reactive approach encourages short-term fixes rather than long-term solutions, contributing to the difficulties it encountered in supporting response and recovery operations after Hurricane Katrina. Without taking the time to fully define and document systems requirements, it is difficult for FEMA to evaluate viable alternatives to its custom-designed systems. Also, the reactive manner in which information technology systems are funded and implemented has left little time for testing before they are deployed.

In 2004, FEMA Logistics began testing a total asset visibility pilot program that involved putting tracking units on selected trucks to monitor their movement. In response to Hurricane Katrina, FEMA could only equip about one third of the trucks with tracking units because funds were not available to purchase units for all trucks. In addition, FEMA could not determine whether a truck had been offloaded or had changed cargo once it left its point of origin because of software limitations of the equipment.

Another logistics issue is the use of mission assignments. In response to of Hurricane Katrina, FEMA issued approximately 2,700 mission assignments totaling about $8.7 billion to other federal agencies to acquire goods and services needed for disaster response activities. Historically, FEMA's guidance on mission assignments has been vague and agencies' accounting practices have varied significantly. As a result, FEMA has had difficulty issuing, tracking, monitoring, and closing mission assignments and reconciling agencies' records to FEMA records. FEMA has developed new pre-defined mission assignments to streamline some of the initial recurring response activities. In addition, FEMA's Disaster Finance Center is working with other federal agencies on appropriate supporting documentation for billings.

Since Hurricane Katrina, FEMA has identified five major commodity storage sites for water, meals, tarps, sheeting, blankets, cots and generators, and has expanded its asset visibility to all regions. Reporting capabilities have been enhanced to allow for more comprehensive and real time reporting from the field. FEMA has interagency agreements with key partners at the Defense Logistics Agency, U.S. Army Corps of Engineers, the Department of Transportation, and the American Red Cross, and is pursuing one with the General Services Administration, to sustain efforts at 100 percent of requirements within 72 hours. These interagency agreements will provide FEMA with essential disaster response commodities, such as meals-ready-to-eat, fuel, ice, medical supplies, water, cots, blankets, tarps, and rental equipment. Each agency will be responsible for tracking its assets and working closely with FEMA and its total asset visibility staff.

Because it is essential to its mission to track assets real-time across federal, state, and local organizations, FEMA has made improvements to LIMS, and has called on the expertise of the private sector to improve total asset visibility. The actions to improve logistical capability are steps in the right direction. Recent events, including the Kansas tornado, indicate improvements in FEMA's response and logistics capabilities. However, whether these improvements will work for a catastrophic event are largely untested.

Acquisitions. In the aftermath of Hurricane Katrina, FEMA was not prepared to provide the kind of acquisition support needed for a catastrophic disaster. Specifically, FEMA lacked (1) sufficient acquisition planning and preparation for many crucial acquisitions needed immediately after the disaster; (2) clearly communicated acquisition responsibilities among FEMA, other federal agencies, and state and local governments; and (3) sufficient numbers of acquisition personnel to manage and oversee contracts.

Pursuant to the Post-Katrina Act, FEMA has undergone significant reorganization, including in its acquisition function. Major concerns for the acquisition program include the need for: (1) an integrated acquisition system; (2) a full partnership of FEMA's acquisition office with other functions; (3) comprehensive program management policies and processes; (4) appropriate staffing levels and trained personnel; (5) reliable and integrated financial and information systems; and (6) timely corrective actions in response to many OIG and GAO report recommendations.

FEMA has recognized the need to improve acquisition outcomes and has taken positive steps that include:

- Using a hurricane gap analysis tool to identify potential disaster response gaps;
- Executing pre-negotiated or "readiness" contracts in advance of disasters;
- Working with DHS' Disaster Response/Recovery Internal Control Oversight Board to address response problems; and

- Continuing its aggressive hiring of highly trained acquisition professionals.

Despite these positive steps, a number of acquisition readiness concerns remain, including the following:

- FEMA has yet to finalize an established process to ensure that federal pre-negotiated contracts for goods and services are coordinated with federal, state, and local governments;
- FEMA has not fully strategized and identified the goods and services for which pre-negotiated contracting may be needed in a catastrophic event; and
- FEMA and other federal agencies may not have enough trained and experienced acquisitions personnel to manage and oversee the vast number of acquisitions that follow major and catastrophic events.

Housing. Possibly the largest problem FEMA faced in the aftermath of Hurricane Katrina was providing financial assistance, sheltering, and housing to evacuees. Because FEMA lacked a catastrophic disaster housing strategy and had never before been faced with meeting the short- and long-term housing needs of hundreds of thousands of disaster victims, it relied on shelters, hotels, motels, cruise ships, and tents, as well as any other available housing resources to meet sheltering and housing needs. FEMA also worked with the Department of Housing and Urban Development (HUD) to implement additional programs to provide housing assistance vouchers to eligible disaster victims. After approximately two years, FEMA has executed an Interagency Agreement with HUD to handle long-term Gulf Coast housing issues.

FEMA's existing programs were inadequate to handle the magnitude of housing requirements after Hurricane Katrina. Also, the number of victims overwhelmed FEMA's system for verifying victim identities and providing individual assistance payments. Consequently, FEMA lessened system controls to accelerate individual assistance payments, resulting in widespread fraud. While FEMA subsequently improved its intake process and the system's capacity, the changes remain untested.

FEMA's efforts to house victims in travel trailers and mobile homes were not well planned, coordinated, or managed, and some outcomes were not anticipated. FEMA purchased mobile homes without a plan for how the homes would be used. As a result, FEMA now has thousands of surplus mobile homes.

The Post-Katrina Act requires FEMA to develop a National Disaster Housing Strategy. The strategy will focus on sheltering, interim and permanent housing, and the various populations to be served, and will guide FEMA and other federal agencies during disasters. The strategy also will identify gaps, such as additional authorities required to deal with sheltering and housing operations, as well as provide flexibility and scalability to meet the unique needs of individual disasters. FEMA has coordinated with other federal agencies and the National Council on Disability to develop a strategy to address housing needs for future disasters. The strategy includes a Joint Housing Task Force that consists of other federal agencies, state, local, tribal governments, and volunteer agencies. The task force will convene immediately after a Presidential disaster declaration to work with FEMA to coordinate resources and implement housing programs. However, FEMA is looking to other federal and state partners to take a bigger role in disaster housing.

While lessons learned from Hurricane Katrina have improved housing coordination, FEMA needs to develop and test new and innovative catastrophic disaster housing plans to deal with large-scale displacement of citizens for extended periods. Traditional housing programs for non-traditional disaster events have been shown to be inefficient, ineffective, and costly.

Evacuations. Lessons learned from Hurricane Katrina have caused FEMA to take a more active role in evacuating victims during major and catastrophic disasters. While the Department of Transportation has retained responsibility for some transportation functions, FEMA has taken over the standby contracts for air/bus/rail support when state and local governments cannot handle the evacuation process. FEMA is also working closely with states to ensure that evacuation plans are in place. It is critical that FEMA and its federal partners coordinate with state and local governments since catastrophic disaster events will likely exceed their capabilities to handle mass evacuations.

Hurricane Katrina resulted in the activation of Emergency Support Function ESF-6 (Mass Care) with FEMA as coordinator. Because roles and responsibilities were not clearly defined or established, FEMA found it difficult to identify the number and location of evacuees, as well as the need for shelters. The American Red Cross (ARC) stated it was responsible only for coordination and reporting on ARC mass care operations, while FEMA said it relied heavily on ARC to coordinate mass care operations and reporting. The mass care failings after Hurricane Katrina resulted in the development of the National Sheltering System, which is nearly complete. The system, although untested, should allow FEMA to more easily track victims once they arrive at a shelter.

Evacuation plans are complex and must consider a number of scenarios. Recent reports indicate that despite warnings and mandatory evacuation orders, a significant number of individuals will not leave their homes. Others may not be able to evacuate because of health considerations or lack of transportation. State and local officials are in the best position to develop evacuation plans based on these considerations and on local demographics. However, these officials must work closely with FEMA and its federal partners to minimize the loss of life that can result from catastrophic events such as Hurricane Katrina.

ACQUISITION MANAGEMENT

Balancing Urgency and Good Business Practices

With DHS annually spending about 39 percent of its budget through contracts, effective acquisition management is fundamental to DHS' ability to accomplish its missions. Due to our current homeland security vulnerabilities, DHS tends to focus its acquisition strategies on the urgency of meeting mission needs, rather than balancing urgency with good business practices.

Excessive attention to urgency without good business practices leaves DHS and the taxpayers vulnerable to spending millions of dollars on unproductive homeland security investments. Acquisitions must provide good value, because funds spent ineffectively are not available for other, more beneficial uses.

We have conducted audits and reviews of individual DHS contracts, such as the U.S. Coast Guard's (Coast Guard) Deepwater program and Customs and Border Protection's (CBP) Secure Border Initiative Network. Common themes and risks emerged from these audits, primarily the dominant influence of expediency, poorly defined requirements, and inadequate oversight that contributed to ineffective or inefficient results and increased costs. Numerous opportunities exist for DHS to make better use of good business practices, such as well-defined operational requirements and effective monitoring tools, that would have preserved the government's ability to hold poorly performing contractors accountable.

Suspension and debarment are the most serious methods available to hold government contractors accountable for failed performance and to protect the government's interests in future procurements. To ensure the government has the option of using these methods, along with other tools to hold contractors accountable, the government must lay the groundwork from the very beginning of the acquisition process. That is, contracts must specify precisely expected outcomes and performance measures and the government must properly oversee contractor performance. Without these basic provisions, the government will have no basis to assert that a contractor failed to perform, and thus, no basis to pursue suspension and debarment to protect the taxpayers in future procurements.

The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major acquisition programs. As DHS builds its acquisition management capabilities in the components and department-wide, the business of DHS goes on and major procurements continue to move. Acquisition is not just awarding a contract, but an entire process that begins with identifying a mission need and developing a strategy to fulfill that need through a thoughtful, balanced approach that considers cost, schedule, and performance. Urgent acquisitions need more discipline, not less, because the consequences of failure are higher. DHS needs to distinguish between truly urgent needs and less urgent needs.

Programs developed at top speed sometimes overlook key issues during program planning and development of mission requirements. Also, an over-emphasis on expedient contract awards may hinder competition, which frequently results in increased costs. Finally, expediting program schedules and contract awards limits time available for adequate procurement planning and development of technical requirements, acceptance criteria, and performance measures. This can lead to higher costs, schedule delays, and systems that do not meet mission objectives.

One procurement method DHS uses is performance-based contracting. While this method has certain advantages over traditional, specifications-based contracting, it also introduces risks that, unless properly managed, threaten achievement of cost, schedule, performance, and, ultimately, mission objectives.

A performance-based acquisition strategy to address the challenges of DHS' programs is, in our opinion, a good one. Partnering with the private sector adds fresh perspective, insight, creative energy, and innovation. It shifts the focus from traditional acquisition models, i.e., strict contract compliance, to one of collaborative, performance-oriented teamwork with a focus on performance, improvement, and innovation. Nevertheless, using this type of approach does not come without risks. To ensure that this partnership is successful, DHS must lay the foundation to oversee and assess contractor performance, and control costs and schedules. This requires more effort and smarter processes to administer and oversee the contractors' work. Therein lies the critical importance of describing mission needs, and the yardsticks by which to measure achievement, completely and precisely. Without clear agreement between the government and the contractor about what the procurement is to achieve, the government is vulnerable to cost overruns, delays, and, in the end, not receiving a good or service that meets its needs.

Performance-based contracting may have additional risks, but with forethought and vigorous oversight, the risks can be managed. "[R]isk management is the art and science of planning, assessing, and handling future events to ensure favorable outcomes. The alternative to risk management is crisis management, a resource-intensive process" with generally more limited options.[3] While no one has yet formulated the perfect risk management solution, risks can be controlled, avoided, assumed, or transferred. For example, programs can develop alternative designs that use lower risk approaches, competing systems that meet the same performance requirements, or extensive testing and prototyping that demonstrates performance. Risk mitigation measures usually are specific to each procurement. The nature of the goods and services procured, the delivery schedule, and dollars involved determine what mitigation is appropriate.

A balanced approach is more likely to result in obtaining the right products and services at the right times for the right prices. Little disagreement exists about the need for our nation to protect itself immediately against the range of threats, both natural and manmade, that we face. At the same time, the urgency and complexity of the department's mission create an environment in which many programs have acquisitions with a high risk of cost overruns, mismanagement, or failure. Adopting lower risk acquisition approaches that better protect the government's interests enhance the department's ability to take action against bad actors.

An Efficient, Effective, and Accountable Acquisition Function

We recently published the first of what will be a series of scorecards identifying the progress made in selected acquisition functions and activities within DHS.[4] The data included in the scorecards reflect our audits and inspections reports issued through March 2007, as well as additional fieldwork conducted in February 2007 and March 2007. We used GAO's *Framework for Assessing the Acquisition Function at Federal Agencies* (September 2005) and DHS' *Acquisition Oversight Program Guidebook* (July 2005) as a baseline. These references identify the following five interrelated elements essential to an efficient, effective, and accountable acquisition process: organizational alignment and leadership; policies and processes; financial accountability; acquisition workforce; and knowledge management and information systems.

---

[3] Department of Defense, Defense Acquisition University, *Risk Management Guide for DoD Acquisition*, Fifth Edition (Version 2.0), June 2003.
[4] DHS Office of Inspector General, *Semiannual Report to the Congress*, October 1, 2006 – March 31, 2007, pages 59 – 78.

The Office of the Chief Procurement Officer is the DHS organization with responsibility for all department acquisition activities and services. This includes management, administration and oversight, financial assistance, and strategic and competitive sourcing. Responsibilities also include the development and publication of department-wide acquisition and financial assistance regulations, directives, policies, and procedures. Each component head shares responsibility for the acquisition function with the DHS Chief Procurement Officer. Therefore, the Chief Procurement Officer has used collaboration and cooperation with the components as the primary means of managing DHS-wide acquisition oversight. Specifically, some collaborative methods include integrating departmental components through common policies and procedures, meeting monthly with component procurement managers, and providing input on component new hires and procurement employees' performances.

Recent congressional testimony, audits, and reviews indicate deficiencies and the need for DHS to improve all five elements, such as (1) lack of strong acquisition authority in the Office of the Chief Procurement Officer and less than full partnership with other departmental functions; (2) lack of comprehensive program management policies and processes; (3) ineffective internal control over financial reporting; (4) insufficient program management staffing; and (5) unreliable information systems that are not integrated and do not provide useful reports and analysis. DHS acquisition leaders identified some progress, but previously reported deficiencies are largely uncorrected. Many remaining acquisition challenges fall outside the Office of the Chief Procurement Officer's control. A brief summary of each element follows.

Organizational Alignment and Leadership. DHS executive leadership has made modest progress in ensuring that the acquisition function achieves the organizational alignment needed to perform. Strong executive leadership is needed to ensure that the importance of the acquisition function is acknowledged and integrated with all other functions involved in, or affected by, procurement activities. One area of improvement is the increased communication by acquisition leadership to inform staff about the role and importance of their mission to DHS. The atmosphere for collaboration between DHS and its components on acquisition matters has improved. However, many still view the acquisition function as a support activity, i.e., a contract processing office, rather than as a partner. Acquisition has begun to receive more resources for staffing and training.

Policies and Processes. DHS has made modest progress in developing policies and processes to ensure that components comply with regulations, policies, and processes to achieve department-wide goals. In 2005, DHS issued a management directive and guidebook that established policies and procedures for oversight of DHS acquisitions, with the common goal of delivering mission results while maintaining compliance with applicable laws, regulations, policies, and procedures. An acquisition manual and additional acquisition regulations for DHS have also been developed. According to GAO and our recent reports and interviews with DHS officials, the need still remains for a comprehensive DHS approach to program management standards.

Financial Accountability. DHS has made limited progress in ensuring financial oversight and accountability within the acquisition function. DHS financial information is generally unreliable, and financial systems do not have the internal controls and integration that acquisition personnel require. Also, the acquisition and finance offices have not successfully partnered on acquisition planning and strategic decision-making. DHS has numerous and persistent issues with inadequate internal controls and data verification. Improper payments have been made, and there are few checks on data once it is recorded in the system. This problem is exacerbated by the use of multiple, nonintegrated information technology systems across the department. Without a reliable data system, it has been very difficult for the financial office to make an impact in the broader acquisition process.

Acquisition Workforce. The capabilities of DHS' acquisition workforce will determine, to a great extent, whether major acquisitions fulfill DHS' urgent and complex mission needs. Contracting officers, program managers, and Contracting Officer Technical Representatives (COTR) make critical decisions on a nearly daily basis that increase or decrease an acquisition's likelihood of success. DHS has made modest progress in building a skilled acquisition workforce. However, until a fully trained acquisition workforce is developed, it will be difficult to achieve further progress needed for an efficient, effective, and accountable acquisition function.

Both our office and the GAO have reported that the Office of the Chief Procurement Officer needs more staff and authority to carry out its oversight responsibilities. GAO recommended that DHS provide the Office of the Chief Procurement Officer sufficient resources and enforcement authority to enable effective, department-wide oversight of acquisition policies and procedures. We made a similar recommendation. An increase in the personnel budget has allowed DHS to fill many needed acquisition staff positions. During fiscal year 2006, the Under Secretary for Management established policies for acquisition oversight and directed the eight contracting offices to measure and manage their acquisition organizations. Also, the number of oversight specialists in the Acquisition Oversight Division is authorized to expand to nine during fiscal year 2007. The Office of the Chief Procurement Office has undertaken an outreach program to involve DHS component staff to manage effectively and assist in acquisition oversight. In previous reports, our office and GAO identified the need for additional certified program managers. The Office of the Chief Procurement Officer subsequently created a training program that likely will increase the pool of certified program managers.

Office of Personnel Management data indicates that more than 40 percent of DHS' contracting officers will be eligible to retire within the next five years. To mitigate this circumstance, DHS plans to use additional appropriations to hire more personnel and implement an acquisition internship program that will bring in junior staff.

Knowledge Management and Information Systems. DHS has made limited progress since its creation in developing and deploying information systems to track and analyze acquisition data and improve user efficiency. Current systems are not fully integrated, contain unreliable input, and do not have internal controls to verify data. As a result, the acquisition program cannot effectively provide information to its stakeholders and does not have the tools necessary for planning or monitoring its transactions. Many DHS components still maintain their legacy contract writing systems and DHS lacks integration between contract writing and contract management systems. DHS has selected PRISM as its standard contract writing system, but the department-wide rollout is behind schedule. Integration and data accuracy problems will continue to exist until all components migrate to the same contract writing system.

U.S. Coast Guard Deepwater Acquisition

The Integrated Deepwater System Program (Deepwater) is a $24 billion, 25-year acquisition program designed to replace, modernize, and sustain the Coast Guard's aging and deteriorating fleet of ships and aircraft, providing a deepwater capable fleet for 40 years.[5] The Deepwater acquisition strategy is a non-traditional systems-of-systems approach by which private industry was asked to not only develop and propose an optimal mix of assets, infrastructure, information systems, and people-based solution designed to accomplish all of the Coast Guard's Deepwater missions, but also to provide the assets, the systems integration, integrated logistics support, and the program management. Under a more traditional acquisition strategy, the government would contract separately for each major activity or asset involved, such as cutters and aircraft, and their logistics support, communications equipment, systems integration, and program management operations.

Over the past year, the OIG, the GAO, the Defense Acquisition University, and Acquisitions Solutions, Inc. have conducted of audits and studies of the Coast Guard's Deepwater Program. These reviews have identified a number of management challenges and risks with the Deepwater Program which raise fundamental questions about the viability of the Coast Guard's "System of System" strategy for re-capitalizing and upgrading its Deepwater fleet of small boats, patrol boats, cutters, helicopters, and fixed-wing aircraft. These challenges and risks include:

- A contract structure that did not easily adapt to the environment of changing missions and requirements, and major systems integration;
- A Deepwater Executive Officer who did not exercise his oversight authority and, as a result, relied on a lead systems integrator to manage the Deepwater program;
- A contract structure that inhibited the Coast Guard's ability to exercise an appropriate level of technical oversight over the acquisition of key Deepwater assets and systems;
- A Deepwater acquisition work force that lacks the requisite training, experience, certification, and structure to acquire assets and systems of significant scope and complexity;
- The Coast Guard's unwillingness to enforce contract performance requirements; and
- The Coast Guard's acceptance of contractor self-certification of technical standards in lieu of independent third part certification.

As a result of these and other Deepwater problems, the Coast Guard:

- Discontinued design work on the Fast Response Cutter due to the failure of the contractor to meet minimum design and performance requirements;

[5] The Deepwater area of operations is typically defined as beyond the normal operating range, approximately 50 miles from shore.

- Withdrew eight 123-foot patrol boats from service due to the contractor's failure to meet minimum design, construction, and performance requirements outlined in the Deepwater contract; and

- Authorized the expenditure of $1.6 billion to construct three National Security Cutters with the knowledge that the cutter, as currently designed, had structural design flaws that prevent it from meeting the mission performance requirements outlined in the Deepwater contract.

To its credit, the Coast Guard now recognizes the need for urgent and immediate changes to the way it manages its major acquisitions in general, and the Deepwater Program in particular. For example, the Coast Guard recently issued its *Blueprint for Acquisition Reform,* July 15, 2007 (Blueprint), which catalogues many of the aforementioned challenges and risks that have historically impeded the efficient execution of the Deepwater contract acquisition projects. According to the Coast Guard, implementing this Blueprint will enhance its ability to efficiently execute asset-based "traditional" projects, effectively employ a governmental or commercial entity as a systems integrator for complex acquisitions, and efficiently execute non-major acquisitions and contracts for necessary goods and services.

The Blueprint specifically outlines the Coast Guard's plans for reorganizing its acquisition workforce, an effort that is expected to take several years and an unknown amount of money to implement. The Blueprint, however, does not contain critical measures of performance that would allow the Department and the Congress to assess the progress being made. For example, the Blueprint does not describe the number and type of acquisition professionals needed or when they are scheduled to arrive on board.[6] In addition, while the Blueprint contains a number of key initiatives, it does not clearly state the outcomes that will be achieved, and at what cost to the Coast Guard. Finally, neither the Blueprint nor the Coast Guard has identified the changes to the Deepwater contract that will be made to ensure full implementation of the Blueprint. Consequently, it is difficult to determine whether these initiatives will satisfactorily address the cost, schedule, and performance issues associated with the Deepwater Program.

Outlook and OIG Oversight

DHS can protect the public interest in major acquisitions. The long-run solutions include strong program and procurement offices; clearly articulated program goals; defined program technical requirements, performance measures, and acceptance terms; well-structured contracts; and thorough cost and performance oversight. In the near term, DHS can mitigate risks and limit government's exposure through such actions as writing shorter-term contracts with smaller, incremental tasks; using contract vehicles that better share risk between government and vendor; and ensuring that the government retains negotiating power with decision points and options.

We will continue a vigorous audit and investigation program to uncover DHS acquisition vulnerabilities and recommend swift, cost-effective improvements. Acquisition management is

[6] Major systems acquisition competency areas that are in the greatest need of infusion of experience are program management, contracting, and financial management (including earned value management and cost estimating). Defense Acquisition University, *Quick Look Study, United States Deepwater Program,* February 2007.

and will continue to be a priority for my office and an area where we focus considerable resources. Our plan is to continue examining such crosscutting acquisition issues as workforce qualifications, competition, small and disadvantaged business utilization, and corporate compliance, in addition to individual programs, such as Deepwater and the Secure Border Initiative.

GRANTS MANAGEMENT

In conjunction with the realignment efforts being undertaken pursuant to the Post-Katrina Emergency Management Reform Act of 2006, the grant programs administered by the Office of Grants and Training transferred to the FEMA, effective April 1, 2007. Grants and Training grant management activities were absorbed within two new FEMA Directorates. Grants and Training's grant business and administrative management functions will be centralized in the Grants Program Directorate, while program management functions will become a part of the National Preparedness Directorate. Grants and Training's financial management activities, which were previously provided by Grants and Training's legacy organization at the Department of Justice, will be absorbed by FEMA's Office of the Chief Financial Officer (OCFO). The OCFO will be responsible for all financial grants management functions within the new FEMA. Financial grants management encompasses all financial activities necessary to manage the grant funds, from appropriation through closeout of the grant award. As a result, FEMA directly oversees more than 80 percent of all grant resources awarded by DHS. This includes not only mitigation programs, but also preparedness grants valued at nearly $4 billion in FY 2007.

Recognizing that this was a mid-year transition, the processes in place to announce Grants and Training grant guidance, receive and review applications, and announce awards remained unchanged in FY 2007. The relationship between Grants and Training grantees and Preparedness Officers in providing grant guidance and other services also remained unchanged. The Grants Management System supports the grant management process involving the receipt of grant applications and grant processing activities. The FEMA Integrated Financial Management Information System (IFMIS) will be the key financial reporting system, which has feeder subsystems for budget, procurement, accounting and other administrative processes and reporting. For the short-term, FEMA will run two financial systems: (1) FEMA IFMIS, and (2) Grants and Training IFMIS. This will allow FEMA to incorporate all Grants and Training financial data, including grants data, within the new FEMA. Grants and Training IFMIS includes grantee payment functionality and financial status reporting capabilities. In FY 2008, Grants and Training IFMIS data will migrate to FEMA IFMIS to form a unified system.

Managing the multitude of grant programs within DHS poses a significant challenge. The grant programs of other federal agencies that assist states and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural disasters compound this challenge. The Congress continues to authorize and appropriate funding for individual grant programs within and outside of DHS for similar, if not identical, purposes. In total, DHS manages more than 80 disaster and nondisaster grant programs. For disaster response and recovery efforts, we have identified 36 federal assistance programs that have the potential for duplicating DHS grant programs. In addition, the internal DHS reorganization has compounded these issues, as overlapping jurisdictions and systems must be reconciled. DHS must do more to coordinate and manage grants that are stove-piped for specific, but often related purposes, to ensure that they are contributing to our highest national preparedness and disaster recovery goals, rather than duplicating one another and being wasted on low-priority capabilities.

The administration has authorized more than $110 billion to support recovery efforts in the nation's Gulf Coast as a consequence of Hurricanes Katrina, Wilma, and Rita. In the Gulf Coast states affected by these hurricanes, numerous federal grants from different agencies and components of DHS are going to state and local governments, private organizations, and individuals for response and recovery from these hurricanes, as well as for the next disaster or terrorist attack. We are currently reviewing disaster grant activities throughout the Gulf Coast and will continue to give special emphasis to Gulf Coast disaster response and recovery grant spending.

In FY 2008, DHS is expecting to award approximately $3.2 billion for state and local preparedness expenditures, as well as assistance to firefighters. Of this amount, $2.2 billion is requested for DHS to fund grant, training, and exercise programs under FEMA. In addition, in coordination with the state preparedness grant program, FEMA will be administering the $1 billion Public Safety Interoperable Communications grant program in partnership with the Department of Commerce. We are reviewing individual state's management of first responder grants and the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability, and needs assessments. Our audits have reported on the states' inability to effectively manage and monitor these funds and demonstrate and measure improvements in domestic security. Our reports also pointed out the need for DHS to monitor the preparedness of state and local governments, grant expenditures, and grantee adherence to the financial terms and conditions of the awards.[7]

Given the billions of dollars appropriated annually for disaster and nondisaster grant programs, DHS needs to ensure that internal controls are in place and adhered to, and grants are sufficiently monitored to achieve successful outcomes. DHS must ensure that, to the maximum extent possible, disaster and homeland security assistance go to those states, local governments, private organizations, or individuals eligible to receive such assistance and that grantees adhere to the terms and conditions of the grant awards. DHS needs to continue refining its risk-based approach to awarding first responder grants to ensure that areas and assets that represent the greatest vulnerability to the public are as secure as possible. It must incorporate sound risk management principles and methodologies to successfully prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.

[7] DHS OIG: *The State of New Jersey's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 through 2004*, OIG-07-58, July 2007; *Audit of State Homeland Security Grants Awarded to the American Samoa Government*, OIG-07-42, May 2007; *The State of North Carolina's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003*, OIG-07-02, October 2006; *Audit of Emergency Management Performance Grant Funds Awarded to the Virgin Islands Territorial Emergency Management Agency*, DA-07-01, October 2006; *The Commonwealth of Virginia's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003*, OIG-06-45, July 2006; *Audit of Grant 2004-TK-TX-003 and 2005-GH-T5-0001 Awarded to the National Domestic Preparedness Coalition of Orlando, Florida*, OIG-06-34, May 2006; and *The State of Indiana's Management of State Homeland Security Grants Awarded During Fiscal Years 2002 and 2003*, OIG-06-19, December 2005.

DHS management recognizes these challenges. DHS is planning a study to provide a single grants management system for all nondisaster-related grants. In addition, a risk-based grant allocation process was completed in FY 2006. DHS risk analysis was a critical component of the process by which allocations were determined for such programs as the Homeland Security Grant Program, Transit Security Grant Program, Port Security Grant Program, and the Buffer Zone Protection Program.

FINANCIAL MANAGEMENT

Financial management has been a significant challenge for DHS since its creation in 2003. This year, the independent auditors, KPMG LLP (KPMG), under contract with the OIG will be unable again to complete an audit of the DHS consolidated balance sheet and Statement of Custodial Activity as of and for the year ended September 30, 2007. In addition, KPMG noted that numerous material weaknesses in internal control continued to exist. However, the majority of the department's material weaknesses in internal control are attributable to conditions existing at the Coast Guard.

The material weaknesses in internal control are impediments to obtaining an unqualified opinion and have precluded management from giving positive assurance over internal control at the department level.[8] DHS' ability to obtain an unqualified audit report and provide assurances that its system of internal control is designed and operating effectively, is highly dependent upon process and procedural improvements at the Coast Guard, Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), FEMA and OCFO.

To move forward, DHS must develop a comprehensive financial management strategy that addresses organizational resources and capabilities, inconsistent and flawed business processes, and unreliable financial systems. In FY 2006, DHS took the initial step in this process by preparing comprehensive corrective action plans to address known internal control weaknesses. The corrective actions plans from each component were incorporated into a single management strategy document identified as the Internal Control Over Financial Reporting playbook. The DHS CFO, with the support of executive leadership and the involvement of component financial management, has aggressively pursued corrective actions throughout FY 2007.

Consequently, during FY 2007, we anticipate that DHS will make progress in addressing some internal control deficiencies. We will perform a series of performance audits later this year, which are intended to assess the extent of progress and the status of planned corrective actions. These audits will be completed and available early in the second quarter of FY 2008. Further, conditions reported as material weaknesses in internal control in previous independent auditor reports will be updated and reported in the DHS Performance and Accountability Report, submitted to the Office of Management and Budget on or before November 15, 2007. The independent auditor report will include specific conditions and recommendations for DHS consideration in updating its corrective actions in FY 2008.

---

[8] DHS-OIG, *Independent Auditors' Report on DHS' FY 2006 Financial Statements*, OIG-07-10, November 2006.

INFORMATION TECHNOLOGY MANAGEMENT

Integrating the information technology (IT) systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for secure, effective communications and information exchange remains one of DHS' biggest challenges. There are multiple aspects to achieving such an IT infrastructure. For example, creating an adequate capability for relocating mission critical information systems to an alternate disaster recovery site in the event of extended service disruptions or emergency is one concern. Implementing a department-wide program that ensures effective information security controls and addresses IT risks and vulnerabilities is just as key. Further, improved IT planning, requirements identification, and analysis will be essential not only to acquire and implement the systems and other technologies needed to streamline operations within individual DHS component organizations, but also to support effective homeland security information sharing with state and local governments, the private sector, and the public. Without sound department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues will remain untapped also. Finally, DHS faces a major challenge in addressing privacy concerns while integrating its myriad systems and infrastructures.

Department-wide IT Infrastructure

Creating an adequate disaster recovery capability for DHS' information systems is a major concern. DHS' IT infrastructure remains a collection of legacy networks, systems, and data centers. Several elements of this IT infrastructure do not have the ability to relocate to an alternate site that can be used if their primary facility suffers an extended outage or becomes inaccessible. This inability to restore the functionality of DHS' critical IT systems following a service disruption or disaster could negatively affect accomplishment of a number of essential DHS missions, including passenger screening, grants processing, and controlling the flow of goods across U.S. borders.

DHS has focused on this issue by establishing the National Center for Critical Information Processing and Storage (NCCIPS). The NCCIPS is to provide hosting of departmental applications, network connectivity, and critical data storage under the direction of DHS' Chief Information Officer (CIO). In FY 2007, DHS awarded a contract for a second data center to supplement NCCIPS. DHS listed the second data center as a large, redundant, secure, scalable capability that will provide DHS with sufficient backup, disaster recovery, and continuity of operations in an emergency. The NCCIPS and the second data center are to have 'active-active' processing capability to ensure each mission critical system has a complete disaster recovery capability. DHS plans to close 16 existing data centers by moving their processing to the new active-active processing data centers.

Due to a lack of identified funding for migration of systems, DHS has been hindered in its efforts to establish the NCCIPS as an alternate processing facility. Specifically, DHS has stated that migration of systems to NCCIPS will be based on availability of funding, not on criticality of the system. Ensuring that the initial funds provided are spent effectively and will enable DHS to achieve the desired disaster recovery capability in a timely fashion will involve significant resources, oversight, and senior management attention.

Similarly, upgrading the DHS data communications infrastructure and consolidating the various organizations that provide data communications support are major undertakings for DHS. Coordinating these related communications upgrade efforts will require significant resources and oversight. Further, DHS will need to demonstrate how it will achieve the envisioned cost savings. Ensuring that DHS data communications activities remain effective and secure during the upgrade and transition also is a major concern.

Security of IT Infrastructure

The security of IT infrastructure is a major management challenge. As required by the *Federal Information Security Management Act* (FISMA), the CIO must develop and implement a department-wide information security program that ensures the effectiveness of security controls over information resources, including its intelligence systems, and addresses the risks and vulnerabilities facing DHS' IT systems.

As we reported in September 2007, based on its annual FISMA evaluation, excluding its intelligence systems, DHS continues to improve and strengthen its security program.[9] DHS implemented a performance plan to measure the component's progress toward full compliance with its information security program. The performance plan tracks key elements indicative of a strong, functioning security program. Despite this oversight, components again are not executing fully the department's policies, procedures, and practices. Issues remain with component system certification and accreditation, Plans of Action and Milestones, and system baseline configurations. Other information security program areas where weaknesses exist include security configuration management, incident detection and analysis, and security training. Management oversight of the component's implementation of the department's policies and procedures needs to be improved to ensure the quality of the certification and accreditation process and that all information security weaknesses are tracked and remediated.

In addition to our FISMA evaluations, during the past year we conducted information security audits of DHS laptop computers, performed technical security evaluations at Ronald Reagan Washington National Airport and Dulles International Airport, assessed protective measures for personally identifiable information, and evaluated physical and system security at Plum Island. We also reviewed major programs and applications, such as DHS' implementation of Homeland Security Presidential Directive (HSPD-12) and the Automated Targeting System. Based on the results of these audits, as well as our FISMA evaluation, and despite continued improvements in DHS' information security program, we determined that DHS organizational components are not executing all of the department's policies, procedures, and practices.

For example:

- All operational systems have not been adequately certified and accredited;

[9] DHS-OIG, *Evaluation of DHS' Information Security Program for Fiscal Year 2007*, OIG-07-77, September 2007.

- All components' information security weaknesses are not included in a Plan of Action and Milestones; and

- Standard configurations have not been fully implemented.

Further, while DHS has issued substantial guidance designed to create and maintain secure systems, there exist areas where agency-wide information security procedures require strengthening: (1) certification and accreditation; (2) vulnerability testing and remediation; (3) contingency plan testing; (4) incident detection, analysis, and reporting; (5) security configurations; and (6) specialized security training. To address these issues, the CIO must identify ways to improve the review process and increase the accountability of DHS component organizations.

Additionally, DHS is required to protect its intelligence systems. We reported that DHS should grant the Office of Intelligence and Analysis (OI&A) the comprehensive authority to support the management, operation, and security of the department's Sensitive Compartmented Information systems. This authority will strengthen OI&A's oversight of component compliance with FISMA requirements for the data and the information systems that support its intelligence operations and assets.

DHS Component IT Management

Although improvements have been made, IT management at the subcomponent-level remains a major challenge, as demonstrated by our audits and subsequent reports on the IT programs and initiatives of selected DHS directorates and organizations. We continued to identify problems with outdated or stove-piped systems, at times supporting inefficient business processes. Planning to modernize IT was unfocused, often with inadequate requirements identification, analysis, and testing to support acquisition and deployment of the systems and other technologies needed to improve operations. We also found consideration of privacy matters to be lacking for some IT programs.

For example, in November 2006, we reported as part of a follow-up review that U.S. Citizenship and Immigration Services (USCIS) had made some progress by placing priority on business transformation, taking steps to centralize authority for IT personnel, initiating business process reengineering activities, and upgrading desktops and servers at key field locations.[10] However, we found that USCIS would benefit from improvements in centralizing IT operations and refining IT management practices. To be successful, USCIS also must continue to ensure that its transformation strategy as defined is clearly executed. We concluded that until USCIS addresses these issues, the bureau will not be in a position to either effectively manage existing workloads or handle the potentially dramatic increase in immigration benefits processing workloads that could result from proposed immigration reform legislation.

Similarly, our December 2006 follow-up assessment of FEMA's efforts to upgrade its principal disaster management system showed that although the agency has made short-term progress in

[10] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology*, OIG-07-11, November 2006.

addressing problems in each of these areas, more remains to be done to address long-term planning and systems integration needs. These improvements primarily included increasing the National Emergency Management Information System's (NEMIS) capacity and online access and registration. In addition, FEMA and its program offices specifically addressed our previous report's recommendations by documenting training resources, developing a plan to implement its enterprise architecture (EA), gathering requirements for new business tools, and improving configuration management.

Despite these positive steps, FEMA had not documented or communicated a strategic direction to guide long-term IT investment and system development efforts. FEMA also had not performed crosscutting requirements gathering to determine business needs, which would allow its Information Technology Services Division (ITSD) personnel to analyze alternatives to continued development of the complex, custom NEMIS system. FEMA has challenges to accomplishing these tasks, including personnel needs, time limitations, and funding constraints. Therefore, constrained by limited resources, FEMA focused its efforts on preparing for the 2006 hurricane season and made little progress in addressing long-term needs, such as updating strategic plans, defining cross-cutting requirements, and evaluating systems alternatives.

Our reviews of major IT programs and initiatives of various components' management indicate similar problems. For example, in June 2007 we reported that a key Science and Technology (S&T) data mining program, Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) was at risk, due to a number of factors.[11] Specifically, S&T program managers did not develop a formal business case for the research and development project, in part because they were unaware of requirements to do so. In addition, program managers did not address privacy impacts before implementing three pilot initiatives to support ADVISE. Further, due to inadequate data access and system usability, OI&A analysts did not use the ADVISE pilot. Finally, because S&T did not effectively communicate and coordinate with DHS leadership about the benefits of ADVISE, departmental components have been unwilling to adopt ADVISE to support their intelligence analysis operations. DHS discontinued the three ADVISE pilots due to privacy concerns and ultimately announced the termination of the ADVISE program in September 2007.

In July 2007 we reported that the National Bio-Surveillance Integration System (NBIS) program was falling short of its objectives.[12] Specifically, DHS did not provide consistent leadership and staff support to ensure successful execution of the NBIS program. For various reasons, NBIS ownership shifted among department organizations numerous times, with corresponding fluctuations in the program approach, priority, and accomplishments. NBIS also struggled since its inception to secure the staff needed to manage program activities effectively. As a result of the repeated transitions and staffing shortfalls, planning documents needed to guide IT development were not finalized. Program management did not effectively communicate and coordinate with stakeholders to secure the data, personnel, and information sharing agreements needed to support system development. Additionally, program management did not provide the contractor with adequate guidance, requirements input, or data sources to deliver a fully

[11] DHS-OIG, *ADVISE Could Support Intelligence Analysis More Effectively*, OIG-07-56, June 2007.
[12] DHS-OIG, *Better Management Needed for the National Bio-Surveillance Integration System Program*, OIG-07-61, July 2007.

functional system. As such, the contractor may not fulfill NBIS capability and schedule requirements, which potentially could result in cost increases to the program.

Privacy

DHS collects large amounts of information to support its various missions, and much of this information is personal, and must be protected in accordance with federal statutes governing privacy. As such, DHS faces challenges in ensuring that privacy concerns are addressed throughout the lifecycle of each information system or program. Our reviews of DHS programs have identified instances where DHS' efforts to meet these challenges are falling short.

Specifically, following several recent incidents involving the compromise or loss of sensitive personal information, Office of Management and Budget (OMB) issued Memorandum 06-16 Protection of Sensitive Agency Information on June 23, 2006. The memorandum recommends measures to compensate for the lack of physical security controls when information is removed from or accessed from outside the agency location. These measures include (1) verifying the adequacy of agency policies and procedures; (2) identifying systems processing Personally Identifiable Information (PII); (3) encrypting data on laptops and mobile computing devices; and (4) implementing remote access security and offsite transportation and storage controls.

In November 2006, we reported on DHS' implementation of the recommendations set forth in OMB Memorandum 06-16. We noted that DHS and its components are in the process of implementing OMB's recommended security controls for sensitive data and PII. DHS has issued updated policies and procedures to address OMB's recommendations. Further, DHS is in the process of identifying PII systems, encrypting laptop computers, and implementing remote access security and offsite transportation and storage controls. Until all systems collecting, processing, or storing PII are identified, and adequate controls for protecting remote access and storage of PII are implemented, DHS lacks assurance that sensitive data are properly protected.

In addition, our June 2007 report on ADVISE stated that S&T program management did not begin the privacy impact process until after several pilots for the ADVISE program were already operational.[13] Federal agencies are required to conduct a Privacy Impact Assessment for each new or substantially changed IT system that collects, maintains, or disseminates personally identifiable information. For its part, the DHS Privacy Office did not know that S&T had proceeded with implementation of the ADVISE pilot programs with live data, but without addressing privacy matters. In a July 6, 2006, report to the Congress, the Privacy Office stated that the ADVISE tool alone does not perform data mining. However, the report went on to explain that implementation of this system with live data could be considered a data mining tool. Unbeknownst to the Privacy Office, the ADVISE pilots had been implemented at least 18 months prior to its July 2006 report. Failure to properly address privacy issues prior to deploying the three pilots had the ultimate effect of bringing the ADVISE program to a halt.

Finally, our July 2007 report on the National Bio-Surveillance Integration System program (NBIS) revealed that DHS officials did not effectively coordinate with federal stakeholders to

[13] DHS-OIG, *ADVISE Could Support Intelligence Analysis More Effectively*, OIG-07-56, June 2007.

address concerns about the privacy and security of data shared.14 Without NBIS program officials first defining what information NBIS needs, stakeholders had little basis to determine what information might be released by their agencies.

Information Sharing

The *Homeland Security Act of 2002*[15] makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key DHS responsibility. Due to time pressures, DHS did not complete a number of the steps essential to effective planning and implementation of the Homeland Security Information Network (HSIN)—the sensitive but unclassified system it instituted to help carry out this mission.

As we reported in June 2006, DHS did not clearly define HSIN's relationship to existing collaboration systems and also did not obtain and address requirements from all HSIN user communities in developing the system.[16] Further, DHS did not provide adequate user guidance, including clear information sharing processes, training, and reference materials. Without establishing a baseline and developing specific performance measures, DHS had no effective way to track or assess information sharing using HSIN. As of June 2007, DHS' Office of Operations Coordination had taken steps to address our report's recommendations. Specifically, to remedy communication, coordination and system guidance shortfalls, program management has created a HSIN Joint Program Office to develop training initiatives. Also, a Stakeholder Relationship Management team was tasked to focus on engagement of stakeholders and communicating the mission and vision of HSIN. In addition, the Homeland Security Information Network Work Group was engaged in aligning business processes, coordinating requirements, and creating cross-functional governances for HSIN. Lastly, the HSIN Program Manager was working to ensure that performance metrics are established, instituted, and used to determine system and information sharing effectiveness.

On a broader scale, DHS is challenged with incorporating data mining into its overall strategy for sharing information to help detect and prevent terrorism. Data mining aids agents, investigators, and analysts in the discovery of patterns and relationships from vast quantities of data. *The Homeland Security Act* authorizes DHS to use data mining and other tools to access, receive, and analyze information. Our August 2006 report on DHS data mining activities identified various stove-piped activities that use limited data mining features.[17] For example, CBP performs matching to target high-risk cargo. The U.S. Secret Service automates the evaluation of counterfeit documents. TSA collects tactical information on suspicious activities. ICE detects and links anomalies indicative of criminal activity to discover relationships. However, without department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues remains untapped.

---

[15] P.L. 107-296.
[16] DHS-OIG, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.
[17] DHS-OIG, *Survey of DHS Data Mining Activities,* OIG-06-56, August 2006.

INFRASTRUCTURE PROTECTION

DHS is responsible for coordinating the national effort to enhance protection of critical infrastructure and key resources (CI/KR) of the United States. Specifically, DHS has direct responsibility for leading, integrating, and coordinating efforts to protect the chemical industry; commercial facilities; dams; emergency services; commercial nuclear reactors, materials, and waste; information technology; telecommunications; postal and shipping; transportation systems; and government facilities. In addition, DHS has an oversight role in coordinating the protection of CI/KR for which other federal agencies have the primary protection responsibility. Those CI/KR include agriculture and food; the defense industrial base; energy; public health and healthcare; national monuments and icons; banking and finance; and water and water treatment systems. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the effective implementation of protection efforts is a great challenge.

DHS has numerous CI/KR responsibilities to discharge. After issuing the National Infrastructure Protection Plan in June 2006, DHS worked toward completion of specific plans for each critical infrastructure sector. On May 21, 2007, the DHS Secretary approved all 17 sector-specific plans. More work needs to be done in the different sectors. For example, in the chemical sector, DHS issued an Interim Final Rule for Chemical Facility Anti-Terrorism Standards in April 2007. The department is now completing the rule, ensuring that vulnerability assessments are conducted, and fostering the development of site security plans. In the transportation sector, DHS is working to establish a Sector Coordinating Council and implement new statutory requirements. In the agriculture and food sector, we reported that DHS has satisfied most of its basic requirements but still needed to submit an integrated federal food defense budget plan and clearly establish assessment standards for use in the food sector.[18]

The nation's CI/KR distribution is enormous and complex. The requirement to rely on the private sector and federal partners to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI/KR. We reported several opportunities for DHS to improve its engagement of public and private partners.[19] DHS also could do more to prioritize resources and activities based on risk. To assist in overcoming this great challenge, the National Infrastructure Protection Plan envisions a comprehensive, national inventory of assets, known as the National Asset Database (NADB), to help carry out these responsibilities. A maturing NADB is essential to the development of a comprehensive picture of the nation's CI/KR, as well as to management and resource allocation decision-making. As we reported in FY 2006, DHS is improving the development and quality of the NADB.[20] DHS also is strengthening its relationships with other responsible federal departments. Standardizing vulnerability assessment methodologies, such as the Risk Analysis and Management for Critical Asset Protection tool, will also help the department better understand CI/KR. DHS also needs to

---

[18] DHS OIG, *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, February 2007.
[19] DHS OIG: *Review of the Buffer Zone Protection Program*, OIG-07-59, July 2007; *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, February 2007.
[20] DHS OIG, *Progress in Developing the National Asset Database*, OIG-06-40, June 2006.

incorporate threat information into its risk assessments and coordinate the funding of protective measures for CI/KR.[21]

We will continue to monitor and review how DHS coordinates infrastructure protection with other sectors, how it uses the NADB to support its risk management framework, and how its pursuit of basic vulnerability assessment standards can help develop overarching departmental priorities.

Protecting the nation's cyber infrastructure also is a challenge for DHS. Since our last review in 2004, the National Cyber Security Division has taken actions to further implement *The National Strategy to Secure Cyberspace* that was published by the White House in February 2003. For example, the division has established a fully operational incident handling center (United States Computer Emergency Readiness Team). The National Cyber Security Division has put into action programs that promote cyber security awareness among the public and private sectors; improve vendor software development and reduce vulnerabilities; develop and promote sound practices and standards that enhance cyber security; promote a global culture of security through international outreach awareness; promote and facilitate the development of adequately trained IT professionals; and plan, coordinate, and conduct cyber exercises with the public and private sectors to improve cyber security readiness, protection, and incident response capabilities. The National Cyber Security Division has established working groups and participated with public and private sector organizations to share information and protect cyberspace and cyber assets.

While the National Cyber Security Division has made progress in meeting its mission, it can improve its efforts to secure the nation's cyber infrastructure. Specifically, the division has not (1) established priorities to ensure that its mission-critical tasks supporting its programs are completed timely; (2) developed enhanced performance measures that can be used to evaluate effectiveness in meeting its mission; (3) fully developed its information sharing and communications programs with the private sector; (4) developed and implemented enhanced procedures to ensure that all known cyber incidents from across the federal government are reported.

BORDER SECURITY

One of DHS' primary missions is to reduce America's vulnerability to terrorism by controlling the borders of the United States. This mission is shared by a number of agencies within DHS and is dependent on the coordinated accomplishment of each agency's roles as well as, joint efforts with other agencies. To this end, DHS created and is implementing a comprehensive multi-year plan to secure the borders and reduce illegal immigration. This plan, called the Secure Border Initiative (SBI) orchestrates roles for CBP, ICE, CIS, Coast Guard, and other components.

This plan should address some of the previously reported challenges. For example, last year we reported that CBP and ICE continue to experience difficulties in coordinating and integrating

---

[21] DHS OIG, *A Review of Homeland Security Activities Along a Segment of the Michigan-Canadian Northern Border,* OIG-07-68, August 2007.

their respective operations.[22] More than two years after their creation, CBP and ICE have not come together to form a seamless border enforcement program. Their operations have significant interdependencies that have created conflict between CBP and ICE. Jurisdictional, operational, and communication gaps exist between the two organizations that must be addressed by DHS leadership.

Our follow-up review determined that DHS has made significant progress toward improving coordination and interoperability between CBP and ICE. Additional work is needed to: improve communication between headquarters and field elements; share information and intelligence; strengthen performance measures; and address relational issues among some component elements.[23]

Another example is the integration of border surveillance technologies. Previously, we reported that border surveillance cameras were not integrated with ground sensors, and sensors are plagued by false alarms. We recommended that CBP improve the effectiveness of remote surveillance technology.[24]

As previously reported, maintaining a systems approach to addressing the challenge of securing our borders is a major challenge as the SBI focus shifts to the DHS components' implementation of the various plans comprising SBI. The major planned efforts under SBI are led by the three lead components for immigration and border security.

- ICE leads plans to improve the apprehension, detention, and removal of illegal aliens, and to expand worksite enforcement. Improvements in alien detention and removal efforts require coordinated efforts across DHS and collaboration with the Department of Justice and other agencies sharing responsibility for this function.

- CIS leads plans for a temporary guest worker program; streamlining immigration benefits processes; and expanding the employment verification program. CIS plans to focus on automating and improving processes to (1) increase efficiency, (2) alleviate chronic backlogs in benefit application processing and adjudications, and (3) handle anticipated increases in applicants under proposed expanded guest worker initiatives.

- CBP leads a major investment program to gain control of the borders called SBInet. The SBInet objective is to develop solutions to manage, control, and secure the borders using a mix of technology, infrastructure, personnel, and processes. While SBInet is a new program, it replaces two previous efforts to gain control of the borders: the Integrated Surveillance Intelligence System and the America's Shield Initiative. CBP awarded a multiple year systems integration contract in September 2006 to begin the SBInet multi-billion dollar initiative.

---

[22] DHS-OIG, *An Assessment of the Proposal to Merge Customs and Border Protection with Immigration and Customs Enforcement*, OIG-06-04, November 2005.
[23] DHS-OIG, DHS' *Progress in Addressing Coordination Challenges Between Customs and Border Protection and Immigration and Custom Enforcement*, OIG-07-38, April 2007.
[24] DHS-OIG, *A Review of Remote Surveillance Technology Along U.S. Land Borders*, OIG-06-15, December 2005.

We have monitored the initiation of the SBInet program and provided a risk advisory with recommendations to address observed weaknesses in the program.[25] The SBI procurement presents a considerable acquisition risk because of its size and scope.

Our main concern about SBInet is that DHS is embarking on this multi-billion dollar acquisition project without having laid the foundation to effectively oversee and assess contractor performance and effectively control cost and schedule. DHS did not properly define, validate, and stabilize operational requirements and needs to do so quickly to avoid rework of the contractor's systems engineering and the attendant waste of resources and delay in implementation. Moreover, until the operational and contract requirements are firm, effective performance management and cost and schedule control is precluded. DHS also needs to move quickly to establish the organizational capacity to properly oversee, manage, and execute the program. In our March 2006 semiannual report, we reported progress in building that capacity and we continue to monitor this program and the new acquisition organizations closely.

Additionally, CBP faces challenges attendant to the rapid build-up of its force structure, especially the significant increases in the number of US Border Patrol Agents. In an effort to secure our nation's border, President Bush announced in May 2006 that the Border Patrol would add an additional 6,000 agents by the end of 2008. With this rapid expansion came several challenges for the Border Patrol, including recruiting, hiring, and training a sufficient number of Border Patrol agents; providing sufficient vehicles for agents; and ensuring that there are adequate facilities to house the number of agents entering on duty. While the Border Patrol has made progress in its expansion efforts, challenges continue to arise in order for the Border Patrol to realize its goal over the next 15 months. To improve recruiting, CBP has developed and implemented a strategic plan to meet its recruiting goals. Ensuring hiring process are supported by effective and timely background checks remains a concern as delays increase and instances of hires subsequently found to be unsuitable occur. In addition, once Border Patrol agents are hired and enter on duty, they are required to attend and complete training at the Border Patrol Academy and, once on station, to receive on-the-job training from experienced agents. The Border Patrol is challenged to maintain the quality of training as it changes the curriculum to accommodate the flow of students and as the ratio of experienced agents to new recruits decreases. Also, there are experienced agents who have the perception that the Academy has relaxed its standards and is graduating agents that are not well trained to meet the challenge of being an agent.

Also, the Border Patrol must ensure that agents have the vehicles necessary to conduct their mission. Vehicles used by Border Patrol agents in 2006 exceeded the recommended life for about half the fleet; however, CBP reported that funds were not available to replace vehicles in FY 2006. In FY 2007 the budget provided for marginal Border Patrol fleet growth, although during the same period the Border Patrol agent count increased by 25 percent.

Finally, CBP needs to ensure that that there are adequate facilities to accommodate the increase of Border Patrol agents. This includes predicting the location and number of new agents being deployed, building concurrent construction projects, and funding for construction projects. The location and number of new agents to be deployed are key factors in the planning process.

---

[25] DHS-OIG, *Risk Management Advisory for the SBInet Program Initiation*, OIG-07-07, November 2006.

Agents are deployed based on operational needs, which can change as the amount and type of activity changes on the border. As agents are redeployed or newly deployed, CBP has to change its real estate to accommodate them. One way CBP responds to this challenge is with Rapid Response Projects. CBP currently is building 73 Rapid Response Projects at the same time. However, building concurrent projects takes a large amount of coordination and communication between CBP and its various service providers. With so many projects underway at one time, CBP may not be able to apply adequate oversight and controls to ensure that schedule, quality, and cost requirements are met. We are reviewing the construction of Border Patrol facilities. Other DHS components share border security responsibilities and are necessarily part of a comprehensive solution to border and immigration control. For example, the US-VISIT Program is responsible for developing and fielding DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System and the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System. While US-VISIT has some early accomplishments, the tracking of foreign visitors and immigrants still has weaknesses, especially on exit, that should be addressed under a systems approach.

DHS also needs to address other weaknesses as part of the comprehensive solution to immigration and border control. For example, CBP needs to fuse the intelligence gathered with intelligence requirements to accomplish its priority mission. The CBP mission of preventing terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel is critical. Differentiating between the two requires timely intelligence. The ability of CBP to gather intelligence information and distribute it to field personnel has a direct effect on security at our borders. Border security also depends on information about terrorists kept on various watch lists. The watch lists are managed by several federal agencies. Those agencies and DHS need to coordinate access to the lists to ensure valuable information flows through CBP to field personnel on the line.

We will continue to maintain an aggressive oversight program for DHS' border security initiatives to ensure that DHS applies a systems approach and carries out the resultant plans and programs in an economical, efficient, and effective manner.

TRANSPORTATION SECURITY

Aviation

TSA was created in the wake of the terrorist attacks of September 11, 2001, to strengthen the security of the nation's transportation systems. The *Aviation and Transportation Security Act* (ATSA),[26] established TSA to protect the nation's transportation system, encompassing aircraft, ships, rail and motor vehicles, airports, seaports, trans-shipment facilities, roads, railways, bridges, and pipelines from terrorist attacks and criminal activity. TSA employs approximately 50,000 people responsible for:

[26] P.L. 107-71, November 19, 2001.

- Ensuring thorough and efficient screening of all aviation passengers and baggage through an appropriate mix of federalized and privatized screeners and technology;

- Promoting confidence through the deployment of Federal Air Marshals to detect, deter, and defeat hostile acts targeting air carriers, airports, passengers, and crews; managing the security risk to the surface transportation systems in partnership with federal, local, and private stakeholders;

- Developing and implementing more efficient, reliable, integrated, and cost effective terrorist related screening programs; and

- Improving organizational effectiveness by expanding capabilities of the workforce to leverage limited resources.

The size and complexity of the transportation system, which moves millions of passengers and tons of freight every day, makes it a difficult system to secure and an attractive target for terrorists. The nation's economy depends upon implementation of effective, yet efficient transportation security measures. However, since its inception, TSA has focused almost all of its attention on aviation security.

As part of its mandate, TSA has had to recruit, assess, hire, train, and deploy Transportation Security Officers (or TSOs, formerly known as "screeners") for approximately 450 commercial airports, and provide 100 percent screening of all checked luggage for explosives. TSA, originally a part of the Department of Transportation, became part of DHS in March 2003. Transportation security management challenges are as follows:

Checkpoint and Checked Baggage Performance

The ATSA requires TSA to screen or inspect all passengers, goods, and property before entry into the sterile areas of the airport. The OIG has periodically conducted undercover penetration testing to determine to what extent TSA's policies, procedures, equipment, and supervision ensure that TSO performance prevents threat items from entry into the sterile area and the checked baggage systems of the nations airports. Through our periodic testing, the OIG has assessed whether TSA's screening policies and procedures are adequate, whether TSOs follow the screening policies and procedures, and whether aviation security screening equipment and technologies are functioning properly and as intended. Our undercover audits of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports and do not enter the checked baggage system. In past testing, we noted four areas that caused most of the test failures and were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA agreed with our conclusion that significant improvements in screener performance will only be possible with the introduction of new technology. During FY 2008, we will release a classified report on our latest penetration testing results, including the effectiveness of TSA's performance in implementing newer technologies.

Passenger Air Cargo Security

The vast and multifaceted air cargo system transports approximately 7,500 tons of cargo on passenger planes each day, making air cargo vulnerable to terrorist threats. The Assistant Secretary of TSA has primary responsibility for enforcing and implementing all regulations related to aviation security. TSA enforces statutory and regulatory requirements, disseminates threat-related information, and provides guidance and some funding. TSA relies on the oversight and inspections carried out by Aviation Security Inspectors (ASI), who are located at airports throughout the United States. ASIs are responsible for inspecting approximately 285 passenger and all-cargo air carriers with about 2,800 cargo facilities nationwide. TSA has approximately 300 Cargo ASIs, supplemented by 600 Generalist ASIs, responsible for conducting inspections of screening activities at approximately 100 airports.

Recent OIG work showed that TSA's inspection process might not accurately represent the extent to which air carriers comply with cargo screening requirements. Additionally, TSA does not provide sufficient resources for air carrier inspection coverage. Therefore, ASIs do not have the capability to monitor cargo screening activities and are unable to report accurately on air carrier compliance. TSA's compliance database, the Performance and Results Information System, is ineffective as a tool to monitor and report air carrier compliance with screening regulations. In addition, the current level of oversight does not provide assurance that air carriers are meeting congressionally mandated goals of tripling the amount of cargo screened for passenger aircraft and that air carriers are properly applying exemption rules for cargo screening. Consequently, the process increases the opportunities for the carriage of explosives, incendiaries, and other dangerous devices on passenger aircraft.

Workers' Compensation

The physical activity required to screen passengers and baggage at the nation's airports has resulted in an inordinate number of injuries for TSA screeners. In FY 2007, the OIG completed an audit to determine whether TSA is effectively and aggressively managing its Federal Employees' Compensation Act (FECA) program to reduce workplace injuries, and minimize lost workdays and FECA-related compensation costs by returning work-capable employees to work as soon as possible. We concluded that TSA made substantial progress in improving the timeliness of new injury claims, reducing both the number of workers' compensation claims and lost time associated with workplace injuries. However, TSA must take steps to better manage its workers' compensation caseload. We identified claimants who were receiving long-term compensation for up to three years despite the fact that medical evidence indicated work capability. We also identified claimants who were not offered limited duty when capable and, when permanent restrictions existed, not recommended for vocational rehabilitation in a timely manner. As a result, the agency may be paying benefits to individuals who are not entitled to them, and may be at risk of workers' compensation fraud and abuse. In addition, the agency did not have a process to validate its workers' compensation chargeback reports. Without reviewing its chargeback reports the agency is unable to determine whether the Department of Labor is accurately billing the agency and is likely incurring inappropriate or excessive costs at other airports nationwide.

We made 12 recommendations to the Assistant Secretary of the TSA to strengthen the controls over its Federal Employees' Compensation Act program. Recommendations included a re-evaluation of long-term cases, more guidance and training for staff, a centralized tracking system for FECA cases, better monitoring of FECA costs, and sharing of safety best practices and incentive programs. TSA generally concurred with the recommendations in the report and has already taken steps to address several of them.

Employee Workplace Issues

A stable, mature, and experienced TSA workforce is the one of the most effective tools the agency has to meet its mission. Since 2004, TSA has been sharply criticized by its employees, primarily TSOs, for alleged discrimination, selective hiring practices, nepotism, management violations, and lax oversight. TSA employees have been voicing their concerns about how the agency operates by filing discrimination complaints that were significantly higher than its closest competitors among federal agencies. TSA has faced high attrition rates and low employee morale, which some say is the result of a lack of employee rights and protections. High levels of workplace dissatisfaction among the TSA screener workforce could compromise organizational stability and, therefore, the effectiveness of airport security operations. In FY 2008, we will issue a report on how effective TSA has been in proactively identifying and addressing employee workplace problems, issues and concerns.

Rail And Mass Transit

Surface transportation systems are extremely vulnerable to terrorist attack, as evidenced by the attacks on passenger rail facilities in Madrid, London, and India. Passenger rail, bus, highway, and ferry systems are inherently difficult to secure in the United States because of their open accessibility (typically, many entry and exit points), high ridership (nearly 9 billion transit trips per year on buses and subways), and extensive infrastructure (roughly 11,000 track miles of transit rail and 3000 stations, 3.8 million miles of roads nationwide, and more than 600,000 bridges and tunnels). While the majority of mass transit systems in the nation are owned and operated by state and local governments and private industry, securing these systems is a shared responsibility among federal, state, and local partners. More robust information exchange, threat detection, and preparedness measures must be undertaken to ensure the security and resilience of the surface transportation system.

The Transportation Sector Specific Plan that DHS published in May 2007 brings together federal, state, and local government partners and regional mass transit stakeholders to create a "a secure, resilient transit system that leverages public awareness, technology, and layered security programs while maintaining the efficient flow of passengers."[27] Nevertheless, the task of prioritizing and securing surface transportation is daunting. DHS has made millions of dollars available through the Transportation Security Grant Program, Homeland Security Grant Program, Trucking Industry Security Grant Program, Urban Area Security Initiative, and other funding methods. For rail and public transit safety grant programs in particular, the Congress provided $275 million in FY 2007, and FY 2008 funds may exceed $400 million. Other DHS programs include the Surface Transportation Security Inspection Program, in which TSA

[27] DHS, *Transportation Sector-Specific Plan: Mass Transit Modal Annex*, May 21, 2007 (page 3).

employs inspectors who assess a transit system's security posture and act as local liaisons. Additionally, TSA trains and deploys supplemental security manpower for high-risk transit systems through Visual Intermodal Protection and Response Teams and provides free explosive detection canines for transit systems through its Canine Program. DHS also develops and tests new technologies, such as more effective chemical and explosive detection equipment, mobile security checkpoints, and video surveillance systems.

We are reviewing DHS actions to improve passenger rail security on subway and commuter rail systems through various TSA programs, assessing how well these programs intersect with federally funded programs operated at the local level. We are examining the impact that the federal grants and policies have on local transit authorities. We also are reviewing the effectiveness of the trucking industry security grant program.

TRADE OPERATIONS AND SECURITY

Trade operations and security primarily are the responsibility of CBP, although USCG and ICE also play important support roles. CBP has the counterbalancing missions of facilitating legitimate trade and enforcing the laws associated with trade and border controls. CBP has the challenge of interdicting smuggling and stopping other illegal activities, that benefit terrorists and their supporters. In a typical year, CBP processes millions of sea containers, semi-tractor trailers, rail cars, and tons of bulk cargo and liquids, such as chemicals, crude oil, and petroleum products. CBP also processes or reviews all of the personnel associated with moving this cargo across U.S. borders or to U.S. seaports.

CBP has implemented a number of initiatives to accomplish this objective such as the Container Security Initiative, and Customs-Trade Partnership Against Terrorism (C-TPAT). CSI works with foreign allies and partners to screen and examine containerized cargo at overseas ports before it is loaded on ships bound for the U.S. The initiative calls for the increased use of non-intrusive technology to inspect this cargo both overseas and at U.S. ports. Within C-TPAT, CBP works with trade representatives to develop and implement processes and systems to help secure the supply chain. CBP uses targeting systems to assist in identifying the highest risk cargo on which to focus its limited resources. Other initiatives include the Secure Freight Initiative, a comprehensive model for improving global supply chain security while keeping legitimate trade flowing. Officially launched on December 7, 2006, it is designed to leverage information, foreign government and commercial partnerships, plus the latest technology to reduce the risk of terrorism.

In support of its trade mission, CBP is undertaking an extensive and long-term effort to develop a new system, Automated Commercial Environment (ACE), to replace older, less effective, and less capable trade processing systems. The ACE Release 4 provides an electronic truck manifest, screens for CBP officers' use, and expedited importation processing. In our 2007 audit, we reported that generally, problems referred to the ACE help desk were resolved effectively. However, CBP did not detect and resolve some operational problems that occurred at the ports and did not provide adequate communication and guidance to the ports. We recommended that CBP develop procedures to monitor post-deployment operations and communicate ACE problems, operational fixes, and system changes to CBP Officers at the ports in a timely manner.[28]

The Automated Targeting System (ATS) helps CBP identify high-risk cargo for inspection. In 2005, we reported concerns about the data to which ATS targeting rules are applied, the use of examination results to refine ATS targeting rules, and physical controls over cargo containers targeted for examination.[29] In our second ATS report, issued in November 2006, we reported that CBP did not fully utilize other sources of intelligence information available and that national ATS performance measures were still being developed for determining the effectiveness of the ATS. Furthermore, we found that additional guidance for inspection of shipments with elevated ATS scores was needed.[30]

In 2007, we reported that CBP was not consistently using entry data for all shipments, resulting in some high-risk containers being allowed to leave ports without mandatory examinations. In addition, CBP has not mandated or actively monitored the implementation by ports of corrective actions in response to our previous reports on ATS. Further, flaws in the Cargo Enforcement Reporting and Tracking System may result in improper container releases, and CBP had not automated its integration of examination findings into ATS. Finally, some ports needed to improve controls over high-security bolt seals. CBP concurred with all of the recommendations and subsequent to the end of our fieldwork, took actions to improve procedures for preventing containers from leaving the ports without the required examinations.31

In the export arena, our audit concluded that outbound shipments are not consistently targeted and inspected by CBP officers at the ports for compliance with federal export laws and regulations. As a result, shipments could be exported that violate laws and regulations. We recommended that systems and regulations be modified to require advance electronic cargo information to enable CBP to screen all shipments; collect and regularly report information necessary for its headquarters and field offices to exercise sufficient oversight of the outbound program; and modify performance measures of compliance with export laws and regulations.

The Coast Guard is the lead DHS agency for maritime homeland security and is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. The marine areas under U.S. jurisdiction cover 3.5 million square miles of ocean, 95,000 miles of coastline, and 26,000 miles of commercial waters serving 361 domestic ports. These activities account for two billion tons and $800 billion of domestic and international freight annually. Approximately 8,000 foreign vessels, manned by 200,000 foreign sailors, make more than 50,000 ship visits to U.S. ports each year. This, too, is a daunting management challenge.

To implement the Maritime Transportation Security Act of 2002 in a timely and effective manner, Coast Guard must balance the resources devoted to the performance of homeland and

---

[28] DHS-OIG, *ACE Release 4 Post-Deployment Problems*, OIG-07-54, June 2007.
[29] DHS-OIG, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary)*, OIG-05-26, July 2005.
[30] DHS-OIG, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary)*, OIG-07-09, November 2006.
[31] DHS-OIG, *Targeting Oceangoing Cargo Containers 2007(Unclassified Summary)*, OIG-07-72, August 2007.

non-homeland security missions; improve the performance of its homeland security missions; maintain and re-capitalize Coast Guard's Deepwater fleet of aircraft, cutters, and small boats; restore the readiness of small boat stations to perform their search and rescue missions; and increase the number and quality of resource hours devoted to non-homeland security missions. For example, while overall resource hours devoted to Coast Guard's homeland security missions grew steadily from FY 2001 through FY 2004 and decreased marginally in FY 2005 and FY 2006. The Coast Guard continues to experience difficulty meeting its performance goals for homeland security missions.[32]

[32] DHS-OIG, *Annual Review of Mission Performance, United States Coast Guard (FY 2006).*

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Executive Secretariat
Chief of Staff
Deputy Chief of Staff
General Counsel
Under Secretary Management
Assistant Secretary for Public Affairs
Assistant Secretary for Policy
Assistant Secretary for Legislative Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS' OIG Program Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

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

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - 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 to Major Management Challenges Facing the Department of Homeland Security

The Reports Consolidation Act of 2000 requires that the Department include a statement by the Inspector General that summarizes the most serious management and performance challenges facing the Department and briefly assesses the progress in addressing those challenges. The Office of Inspector General (OIG) considers the most serious management and performance challenges to the Department to be in the following areas:

- Catastrophic Disaster Response and Recovery;
- Acquisition Management;
- Grants Management;
- Financial Management;
- Information Technology Management;
- Infrastructure Protection;
- Border Security;
- Transportation Security; and
- Trade Operations and Security.

In addition to the OIG report on management challenges, in their biennial High-Risk Series, the Government Accountability Office (GAO) identifies federal programs and operations that are high-risk due to their greater vulnerabilities to fraud, waste, abuse and mismanagement. In recent years, GAO has also identified high-risk areas to focus on the need for broad-based transformations to address major economy, efficiency, or effectiveness challenges. Four of these areas fall within the Department's purview. The areas and the year the issue was identified are listed below. The GAO maintains these issues in their High-Risk Series until satisfied that acceptable progress has been made to correct the issues.

- Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures (1997);
- Implementing and Transforming the Department of Homeland Security (2003);
- Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security (2005); and
- National Flood Insurance Program (2006).

The Department of Homeland Security has steadfastly worked to resolve the challenges identified in the Inspector General's FY 2007 report and the GAO High-Risk Series. The Department will continue to address the unresolved challenges, many of which may require several years to completely address due to the complexity of the challenge. The following highlights the accomplishments of the Department during FY 2007, and details some of the remaining plans to be completed to overcome these challenges.

FY 2007 Challenge 1: Catastrophic Disaster Response and Recovery

Summary of 2007 Challenge: OIG noted that the Department's failures after Hurricane Katrina illuminated a number of issues, including questionable leadership decisions and capabilities, organizational failures, overwhelmed response, communications systems, and inadequate statutory authorities. Coordination of disaster response efforts, catastrophic planning, logistics, acquisitions, housing, and evacuation were among the problem areas cited by the OIG.

2007 Accomplishments

- Operational planning is a core competency of the new FEMA. To strengthen our response capabilities, operational planners have been hired at FEMA headquarters to provide the ability to perform sophisticated operational analyses, analyze trends, and improve planning for the response to ongoing and future events. Planners are also being hired for the Regions to provide this same capability. With the new staff, there is now greater depth and capability to prepare operational plans and conduct crisis action planning to ensure that the agency can lead and support a national all-hazard emergency management response.
- Under a Gap Analysis Initiative rolled out by FEMA this past spring, a Gap Analysis tool was developed in coordination with the State of New York Emergency Management Office/New York City Office of Emergency Management, and implemented to provide FEMA and its partners at both the State and local levels in the hurricane prone regions of the country a snapshot of asset gaps. Seven critical areas were incorporated in the initial application of the Gap Analysis tool for review: debris removal, commodity distribution, evacuation, sheltering, interim housing, medical needs, and fuel capacity along evacuation routes. Gap Analysis discussions provided an opportunity for local jurisdictions to ask specific questions of Federal and State officials and identify issues of critical concern to help long-term preparedness activities. Although the initial use of this very successful concept was utilized for the 2007 hurricane season, this process will be expanded to cover all hazards and applied nationwide in FY 2008.
- FEMA has instituted a major Catastrophic Disaster Planning Initiative that will improve response capabilities and complement the National Response Plan/Framework (NRP/NRF), National Incident Management System (NIMS), and Federal, State, and local planning activities. This initiative addresses both notice and no-notice events, and reflects the considerable measures that DHS and FEMA and its Federal, State, and local partners have taken to ensure appropriate, quick, effective, and efficient response and recovery to protect the health, safety, and well-being of the population and, to the extent possible, restore the infrastructure following a catastrophic event. FEMA's Catastrophic Disaster Response Planning Initiatives are currently focused on four specific geographic areas: southeast Louisiana, the eight states in the New Madrid Seismic Zone (NMSZ), the State of Florida, and the State of California.
- A Mass Evacuation Incident Annex has been developed to describe in more detail evacuation functions and agency roles and responsibilities in mass evacuations. It provides guidelines for evacuating large numbers of people in incidents requiring a coordinated Federal response through the NRP/NRF Emergency Support Functions, and describes how Federal resources are integrated into State, local, and tribal support. In addition to the Mass Evacuation Incident Annex, FEMA is also working on developing an Incident Supplement to the Annex that will provide specifics regarding how and by whom many of the

responsibilities outlined in the Annex will be accomplished. Issues such as evacuee registration and companion animal sheltering will also be addressed.

- FEMA has also developed a new and robust Office of Acquisition Management. Staffing has dramatically increased, from 98 in 2006 to 221 at the present, an increase of 123 acquisition personnel positions. Approximately 90 percent of acquisition positions are filled. The Office has been reorganized into three core branches for greater efficiency of operations.
- Other acquisition accomplishments:
  - Developed a Disaster Response Training Course which is required for all acquisition personnel at HQ and in the Regions who will be deployed at a disaster.
  - Issued an Emergency Acquisition Field Guide to assist non-contracting personnel in effectively and appropriately contracting for goods and services in an emergency situation.
  - Established a Contracting Officer Technical Representative (COTR) Training Program.
  - Pre-positioned agreements have been established by determining what types of goods and services are traditionally utilized in a disaster. This ensures industry contracts are competitive and have a reasonable price and allows for a more responsive industry focus ensuring quick mobilization. Prior to Hurricane Katrina, there were nine contracts in place. There are currently 40 contracts pre-positioned for use in a disaster.

<u>Remaining Plans</u>

- FEMA plans to continue its aggressive staffing policies by filling vacant positions and maintaining high staffing levels and succession planning. Training will also be a key element. The Disaster Training Course and Emergency Acquisition Field Guide will be updated as necessary. All acquisition personnel will be given training and course changes and updates will be made via the Virtual Acquisition Office. COTR training will also be emphasized. FEMA will ensure that the COTR Training program remains current by hosting refresher courses as necessary and implementing a tiered COTR certification program in order to better match COTR competencies to contract complexity.
- FEMA plans to implement the DHS-standard (PRISM) contracting writing system which will provide FEMA's Office of Acquisition Management with
  - better workload tracking,
  - more consistent and accurate reporting,
  - improved contract writing and overall management, and
  - enhanced and more efficient use of other Federal acquisition personnel as approximately 64 percent of Federal agencies use this application.
- FEMA also plans to develop contract administration procedures for cost and schedule oversight for other national procurements.
- FEMA will develop and roll out the capability for long-term recovery planning at the operational Joint Field Office level.

FY 2007 Challenge 2: Acquisition Management

Summary of 2007 Challenge: OIG commented that DHS tends to focus its strategies on the urgency of meeting mission needs, rather than balancing urgency with good business practices, leaving the Department vulnerable to spending millions of dollars on unproductive investments. Common themes and risks include the dominant influence of expediency, poorly defined requirements, and inadequate oversight, which can contribute to ineffective or inefficient results and increased costs. Of specific concern is the USCG's Deepwater program and CBP's Secure Border Initiative Network (SBInet).

Office of the Chief Procurement Officer (OCPO)

2007 Accomplishments

Acquisition Policy & Legislation (APL)

- OCPO Acquisition Policy Board - OCPO stood up the OCPO Acquisition Policy Board. The Board's membership consists of each Component's Head of the Contracting Agency (HCA) Policy chiefs as well as a member of OCPO's Oversight staff. The purpose of the Board is both to disseminate Department-wide acquisition policy information, as well as foster dialog between Component staff members.
- Performance-Based Acquisition (PBA) - DHS OCPO has for much of the year been actively engaged in the Office of Federal Procurement Policy's (OFPP's) PBA Interagency Working Group. The Group has worked to enhance OFPP's PBA Seven Steps Guidance and make available appropriate samples tailored to Component needs. Additionally, OCPO Oversight has begun during its Component reviews to check acquisitions coded in the Federal Procurement Data System (FPDS) as performance-based to verify if the contracts are in-fact performance-based. PBA was also one of the very first Excellence in Contracting training topics.
- Federal Acquisition Regulation (FAR) Cases – Through its representation on the Civilian Agency Acquisition Council, OCPO is very engaged in all regulatory changes to the FAR. OCPO's active involvement ensures that the balance between good business decisions and urgency is a consideration when government-wide acquisition regulations are promulgated.
- Policy Guidance on Service Contracts – Because DHS utilizes a substantial amount of services contracting, the Chief Procurement Officer issued a memo to Components which reminded acquisition professionals of the range of types of services contracting and certain restrictions that apply to each.
- Source Selection Guide – During FY 2007, OCPO issued a Source Selection Guide that provides extensive guidance on conducting formal source selections under FAR Part 15 designed to improve effectiveness in the acquisition process without sacrificing efficiency.
- Improving Competition – OCPO held a Competition Advocates meeting to review DHS achievements and stress the importance of improving upon those achievements; established a Competition Award to recognize significant achievement in strengthening competition; issued an Acquisition Alert spearheading an initiative for Components to correct existing records; and began a systematic review of FedBizOpps sole source announcements to ensure that authorities are being appropriately used.
- Interagency Acquisition (IAA) – OCPO sees IAAs as an area of risk and therefore has been an active member of OFPP's Interagency Working Group crafting the first government-wide comprehensive guidance on IAA in accordance with the Services Acquisition Reform Act

Panel's recommendations. OCPO is working to ensure that the final product meets our needs.

- Emergency Acquisition Flexibilities Guide – OCPO coordinated comments from Components on the draft OMB guide that was published in May 2007. Use of the Guide during emergency situations will enhance the Department's ability to complete acquisitions in a timely manner.
- Suspension & Debarment – OCPO participates on the Interagency Suspension and Debarment Committee (ISDC) established by Executive Order 12549. ISDC issues regulations with government-wide criteria for procurement and non-procurement programs, facilitates lead agency coordination, and serves as a forum to discuss current suspension. As a result of a July 18, 2007 Congressional hearing on responsibility issues, OCPO's Acquisition Policy and Legislation branch (APL) compiled an extensive list of Federal Government Business Systems, other public sector, nongovernmental or State/city systems or entities regarding business information that may be used as a source of information. APL is also participating in the discussion and analysis of an ongoing ISDC Information Sharing project in response to GAO's study (July 2005) on six Federal agencies which included management of "administrative agreements" and "compelling reasons determinations" to continue performance.

Acquisition Oversight

- DHS issued Management Directive 0784 formally initiating a DHS wide acquisition oversight program. Under this program DHS in partnership with Component leaders manage the DHS acquisition function. To date, the acquisition organizations have performed a self assessment and have begun to report key metrics on a quarterly basis. These metrics facilitate internal management and provide a verification mechanism to ensure that data available to external organizations is accurate and complete. Currently each of the acquisition organizations is undergoing a baseline review of the human resources capacity, adherence to policies and procedures, and status of IT systems to facilitate acquisitions and integration with financial systems. To date, OCPO has completed the baseline reviews of four Components and scheduled the remainder of reviews for FY 2008.
- Acquisition Oversight conducts special reviews of specific high-risk acquisitions assessing all aspects of the acquisition in support of DHS's mission and provides a risk analysis and recommends improvements for the instant acquisition. Where applicable the review also recommends systemic changes, revised policies, or improved training to reduce risk for future acquisitions.
- With respect to improving the management of service contracts, DHS conducted training and additional oversight of service contracts to ensure compliance with Federal regulations and procured services were provided. OCPO has internal capability to monitor and investigate high-risk contracts to provide DHS with additional ability to manage and control.

Acquisition Systems

- Enterprise PRISM Instance (EPI) – DHS assumed control of the firewall, thereby strengthening the system security. Several on-going efforts to improve internal business processes and controls and increase the use of PRISM functionality are underway. Several examples follow. Because EPI is not presently interfaced to the accounting system, in partnership with the Finance and Program Offices, processes have been instituted to prevent inconsistent recording of contract obligations in the finance system. Workshops are being conducted to improve user efficiency and to identify areas for improvement. Reports are being utilized to ensure that PRISM transactions are accurate and complete. Training documentation has been customized to implement best practices and to marry policy with system functionality.

- Enterprise Acquisition System Initiative (EASI) - The consolidation effort of Component contract writing and management systems continues to make progress. In FY 2007 work began on the interface between EPI and FEMA's financial system.
- Federal Procurement Data System-Next Generation (FPDS-NG) - Verification and Validation Plan was developed along with additional HSAM policy to improve timeliness and accuracy of reported data. DHS representatives are participating in the FPDS-NG Change Control Board and User Group to continuously improve procurement reporting.
- Acquisition Systems Governance Board (ASGB) – This is a DHS-wide community of practice which meets on a regular basis to share leading practices and lessons learned on DHS Shared eAcquisition Systems. ASGB provides input to the Department in developing strategies for new automation products and services which support the acquisition function.

Strategic Sourcing Program

- In FY 2007, the DHS Strategic Sourcing Program (SSP) continued to leverage leading practices to optimize its program and ensure continued support for DHS's commodity councils and for Component specific business efforts. Positive results in price reductions, cost avoidances, and socioeconomic participation continued to be impressive, with the following delivered:
  - Cost Avoidance - Achieved $99,252,306 in Price Reductions and $690,714 in Cost Avoidances. These results were achieved by multiple initiatives across eight of DHS's 14 commodity councils;
  - Deliveries - Delivered eight distinct strategically sourced vehicles that will potentially place billions of dollars with small business while meeting the stringent operational requirements of DHS's end-users; and
  - Performance Measures - Implemented various performance measures, in addition to price reductions and cost avoidances, to gauge the success of its programs. Representative performance measures that were utilized during FY 2007 included reduced downtime, total costs for maintenance moves and installation reductions, and awards, recognition, and customer satisfaction surveys.

Program Management

- OCPO has reorganized to include a Program Management SES-level directorate to develop and disseminate policy on program management to DHS Components.
- Additional certified program managers (PM) are now on board as a result of various DHS PM training programs, totaling 237 certified program managers since December 2006. This is a 53 percent increase in the past nine months.
- Additionally, in September 2007, a Memorandum of Agreement (MOA) was signed between the DoD and DHS. This strategic relationship enables DHS to take direct advantage of the Defense Acquisition University's acquisition, technology and logistics expertise in training, consulting, knowledge sharing, continuous learning, career workforce planning, and management services.
- One of the Chief Procurement Officer's top priorities is to build a strong acquisition system, with the right people, in DHS. OCPO is doing that through initiatives such as building standards for all acquisition professionals in DHS, installing a metrics system to measure cost, schedule and performance of major programs, and redesigning the investment review

process, as examples. OCPO is also hiring experts in various acquisition career fields to build those competencies and systems throughout DHS. OCPO already has several program managers, cost estimators, Testing & Evaluation personnel, and a logistician at present.

- OCPO initiated program reviews on designated Level 1 investments, to strengthen the investment review process and provide greater independent analysis in an effort to mitigate risk. These reviews are scheduled for completion in first quarter FY 2008, with more extensive reviews as needed. This initiative is a three-prong approach in helping to identify and mitigate high-risk areas, provide a mechanism for sharing best practices, and promulgate policies and processes, as well as identify competencies gaps/training needs.
- Additionally, OCPO uses the Program Management Council, co-chaired by an operational program manager and the CPO, as a Department-wide forum for involvement as DHS builds acquisition expertise.

Acquisition Workforce

- Established framework for a developmental program to bring in up to 60 entry level positions in the 1102 career field, train the interns and provide broad experience across DHS to assist in closing the gap in contracting career field vacancies.
- Improved certification process for the three current acquisition career fields within DHS Program Managers, Contracting Officer Technical Representatives, and Contract Specialists.
- Participated in Government-wide emergency contracting working group to identify a cadre of specially trained contracting officers to provide support in catastrophic emergencies.
- Established and managed training for the 1102 career field within DHS. Conducted one hour DHS wide training sessions to address specific acquisition issues and immediately address gaps in training or acquisition processes.

Office of Small and Disadvantaged Business Utilization

- Met OCPO's goal of making good business deals and supporting public policy objectives such as the Federal small business program. The U.S. Small Business Administration recently recognized DHS in their first annual small business scorecard with a score of green, one of only seven out of 24 Federal departments to receive a green score.

<u>Remaining Plans</u>

Acquisition Policy & Legislation

- Emergency Procurement Tool Box/Framework – OCPO is currently working an initiative with FEMA to develop a framework in order to be able to expedite the acquisition function in the event of a significant national emergency, per the National Response Plan.
- Kaizen Event on Interagency Contracting - In conjunction with active participation in OFPP's Working Group developing a Government-wide Guide on Interagency Acquisition, OCPO is sponsoring and leading a Lean Six Sigma Kaizen event for the purpose of developing a Management Directive on Interagency Acquisition for the Department.
- Price Fighters Memorandum of Understanding (MOU) – OCPO is negotiating an MOU with Navy Inventory Control Point (NAVICP) to provide cost and pricing support for major Department acquisitions.
- Updating HSAM and/or Management Directive Guidance – seven documents are being developed.

- Electronic HSAR/HSAM - OCPO Acquisition Policy is engaged in integrating the HSAR and HSAM into a single electronic document to assist Component operational personnel with research Department acquisition policy. Future plans include providing links within the body of the revised HSAR/HSAM document to other applicable documents (e.g., memos, directives, training slides, etc.) to enable "one-stop shopping."
- Homeland Security Acquisition Regulation (HSAR) Cases – OCPO is engaged in developing seven DHS-only acquisition regulations.
- E-Verify – Crafted a Federal Acquisition Regulation rule to require Federal contractors to verify the employment eligibility of their employees. OMB approved going forward. The FAR change is currently in process. This is a major step in increased enforcement of ensuring only eligible persons work in the United States.
- Time and Material (T&M) Contracts – OCPO is developing guidance on the use of T&M in response to recent changes in Government-wide T&M policy.
- Competition – Various activities for improving the level of competition are currently in process.
- Contract Funding Guidance – Guidance on contract funding is currently in review. It discusses FAR contract funding policies and clauses to assist Contracting Officers in developing effective strategies that afford the maximum benefit to DHS contracts and programs.
- Blended Workforce Initiative- Discussions are underway regarding the development of a reporting system to obtain information from contractors on the types and amounts of contracted labor being performed under DHS's services contracts for the purpose of enabling DHS to better manage use of contractors performing functions on behalf of DHS.
- Acquisition Guidelines – APL plans to develop new form of communicating with Components to provide timely "how to" and interpretive guidance. This will be a series of "Acquisition Guidelines" that will be published on the web and will be linked to and from various HSAR/HSAM policies.

Acquisition Oversight

- Of the eight full acquisition organizations, four baseline onsite acquisition reviews are physically complete. The remaining four have been scheduled and will be completed by October 2008.
- Review of the full role of acquisition oversight.

Acquisition Systems

- EPI Rehost - EPI will be moved to the DHS Hosting Facility in FY 2008. This is to increase system security.
- Enterprise Reporting – will improve reporting and management controls by increasing data sharing which will enable better business decisions.
- EASI - FEMA and FLETC are scheduled to go live on EPI.
- eInvocing – will reduce Prompt Payment Act interest penalties and streamline the invoice approval process.

Program Management

- DHS currently has three acquisition career fields for which DHS has certification standards (Contracting Officer, Contracting Officer's Technical Representative, and Program Manager). DHS will be adding certification standards for other acquisition career fields,

including logistics, systems engineering, cost estimating, and test and evaluation as soon as practicable. OCPO plans to meet both the civilian agency standards, where they exist (currently for contracting and program management), as well as meeting the DAWIA standards, so as to ensure the Department has the best acquisition workforce.
- DHS is retooling the process for reviewing and approving major Department programs and has begun its review of existing programs to determine how to proceed.
- OCPO is conducting Quick Look reviews of all Level 1 acquisition programs. The Quick Look Reviews are designed to provide a rapid assessment of the risk in the Level 1 Acquisition Program Portfolio. The results will be used to identify any high-risk programs for which a more in-depth review may be tasked. These reviews will also provide insight into Component governance and oversight processes that DHS can leverage to refine Departmental acquisition policies and processes.

Acquisition Workforce
- FY 2008 will be the first fiscal year implementing the new intern training and development program. As implementation proceeds, additional interns will be added and improvements to the program will be instituted.
- Additional acquisition career fields required for successful execution of acquisition programs will be identified. Specific training and certification requirements will be assessed for each of these new career fields.
- A mechanism to identify acquisition corps members will be developed.
- Training funds will be centralized to efficiently ensure that all acquisition corps members receive prompt training so they can better perform the mission and improve within the career field.
- Recruitment efforts will be centralized to improve efficiency.

U.S. Coast Guard Deepwater Acquisition

Five years into this 25-year acquisition, USCG has overcome many significant challenges, though more remains to be done. As a result of those lessons learned, USCG is taking aggressive action to strengthen program management and execution. By redefining roles and responsibilities, fundamentally changing relationships with industry, and by strengthening the assessment of government and industry performance, the Deepwater program is showing notable improvements in multiple areas.

2007 Accomplishments

Stand-up of the Acquisition Directorate
- As outlined in the Blueprint for Acquisition Reform, one important objective was to establish a consolidated acquisition directorate which initially came together on July 13, 2007. As part of this consolidation, the Acquisition Directorate, the Deepwater Program Office, the Office of Procurement Management, the Office of Research, Development, and Technical Management, the Research and Development Center, and the Head of the Contracting Authority have been brought together under one roof, led by an Assistant Commandant for Acquisition. This means that USCG is better able to allocate its contracting and acquisition professionals and resources to focus on excellence in program management and contract execution. This is expected to create more efficient and consistent processes, leading ultimately to a more effective acquisition organization.

Changes in the Contract Structure

- As the OIG has suggested, USCG agrees that working closely with industry is still the best approach to recapitalizing and modernizing USCG's platforms and mission systems. However this relationship must be based on sound business practices to ensure suppliers can meet the Government's requirements while adhering to cost, schedule and performance parameters. Therefore, in all dealings with the private sector, USCG is ensuring new acquisition contracts are clearly written and provide for careful Government oversight and management of manufacturer's cost, schedule, and performance.
- In an effort to better define program requirements, USCG has improved the detailed Delivery Task Orders by increasing the use of Statements of Work specifications as compared to Statements of Objective. This reflects a strategic change for USCG by transitioning from a pure performance based approach for assets towards more explicit contract language which includes relevant specifications, standards, and increased written detail as recommended by OIG.

Implementing the Blueprint for Acquisition Reform

- To guide its acquisition reform and business transformation initiatives, USCG developed and published its own strategic and overarching vision called the Blueprint for Acquisition Reform modeled after that developed by GAO for the assessment of Federal Government acquisition processes.
- The success or failure of USCG's acquisition reform initiatives will be tracked by two tiers of metrics. The first is to measure activity called for in the Blueprint on how USCG is doing in executing the plan of action and milestones that are outlined in the Blueprint.
- A more important metric, which will be longer in coming, is the measurement of return on investment measured against project cost, schedule, and performance. It will take time to generate that strategic assessment, "How does the Blueprint reflect back on Coast Guard project and program execution?"

Establishing a Capable Acquisition Workforce

- USCG has built a much more capable acquisition organization than it has ever had. Among many attributes this right-sized dedicated USCG acquisition workforce incorporates two underlying principles: (1) reinvigorated and documented use of a technical authority, outside the acquisition directorate, for all major projects and (2) partnering with other government agencies whenever additional competencies are needed.
- Some of the significant accomplishments during 2007 were:
    - Creating a standard Project Management Core Team model, which is consistent across all USCG acquisition projects and includes all critical functions in support of project execution;
    - Conducting an assessment of current certification levels to ensure personnel are aligned with their respective roles and expected outputs; and
    - Evaluating, and revising as necessary, position descriptions for proposed new hires.

Improvement of Technical/Program Oversight

- The Assistant Commandant for Engineering and Logistics has been designated as the technical authority for all designs and design changes, the Assistant Commandant for Operations for definition of asset performance requirements, and the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT) as the technical authority for all Command, Control, Communications, Computers, Intelligence, and Reconnaissance (C4ISR) systems and equipment. Additionally, the Assistant Commandant for Human Resources is the technical authority for all USCG human resource issues. This means that project and program managers, as well as associated contracting and acquisition professionals, have a direct link back to technical and operational experts to ensure that designs are technically robust, meet standards and are supportable.

- In order to strengthen Government management and oversight of the Deepwater program, as well as to better position USCG to fully oversee the contractor and effectively adjudicate technical concerns, all Integrated Product Teams (IPT) must be chaired by a USCG officer or employee. That change was executed in March 2007. Additionally, all IPT charters have been re-examined to determine where other changes are needed. USCG leadership of IPTs means USCG is better able to resolve non-major technical concerns or, where concerns persist, raise them to the appropriate management and contracting levels for adjudication.
- To ensure that designs and assets will meet USCG needs, there has been in increase in the use of independent, third-party review and analysis (in concert with the USCG technical authorities) for all new starts or substantial design changes. Inherent in this initiative is a renewed commitment to utilize full business case analyses for all new acquisition decisions to instill confidence that USCG is building and buying the right tools for our Coast Guard men and women and at the best value for taxpayers.
- The Directorate has placed renewed emphasis on the USCG's Major Systems Acquisition Manual (MSAM) and DHS-sanctioned processes for program management and acquisition.

Remaining Plans

Alternatives Analysis

- USCG's Acquisition Directorate has asserted its role as the lead systems integrator across its entire $27 billion investment portfolio. The investment portfolio includes the 25-year, $24 billion Integrated Deepwater System (IDS), the largest of eight major acquisition programs. The IDS program modernizes and recapitalizes legacy surface, air, and shore assets to enable USCG to deploy more capable and interoperable offshore maritime patrol and interdiction forces. As lead systems integrator, USCG has restructured Deepwater and the rest of the Coast Guard's acquisition investment portfolio under the aegis of proven acquisition policies and processes, including the procurement principles outlined in USCG's MSAM.
- MSAM requirements state that an Alternatives Analysis (AA) should be conducted and updated whenever significant changes occur in requirements, life cycle cost estimates, or return on investment assessments. The original Deepwater AA was conducted by industry teams as part of the Deepwater proposal process (circa 2001). Operational requirements and design changes that have evolved since September 11, 2001 make it prudent and timely to conduct an independent AA at this time, in order to ensure that USCG continues to acquire systems that fully meet its mission needs. Therefore, in accordance with requirements set forth in the MSAM, the Coast Guard is conducting a state-of-the-market AA of the Deepwater program. The AA will be a program-wide analysis and will include an assessment of the major systems and platforms within the IDS projects. The AA is a positive step in that it aligns with best practices established through DHS and OMB acquisition policy.

Workforce Management Analysis

- The USCG Human Capital Strategy will include a Long-Range Workforce Plan for the entire USCG Acquisition Directorate. The Long-range Workforce Plan will describe the specifics of the necessary workforce over several years. It will forecast and convey the specific skill sets and competencies needed, broken down by both full time equivalent and functional area. The Long-range Workforce Plan will be a dynamic plan linked to acquisition program execution schedules, maintained by Acquisition Program and Project Managers. This dynamic linkage will allow human capital managers to plan for future workforce needs well in advance, and to react swiftly to changes in acquisition strategy initiated at the program or project level.

SBI*net* Management

2007 Accomplishments

Fielding Border Surveillance Technologies/SBInet Program Management

- CBP awarded an SBI*net* task order to demonstrate the effectiveness of the overall approach to SBI*net* along 28 miles of border flanking the Sasabe Port of Entry in Arizona. CBP has made significant progress in implementing Project 28, including deploying all nine re-locatable camera and radar towers, and fitting all 50 of the Project 28 agent vehicles with Common Operating Picture hardware.
- Under the SBI*net* prime contract, CBP awarded a task order for the test and evaluation of fencing solutions. The purpose was to test effective low-cost solutions that meet operational requirements and can be reproduced for rapid deployment along the Southwest Border. This testing will help CBP add to existing tactical infrastructure to reach a total of 370 miles of fencing and 200 miles of vehicle barriers by the end of calendar year 2008.
- CBP met its commitment to construct 70 miles of primary fencing along the Southwest Border. This effort was comprised of both new and previously planned projects brought together under SBI*net*.
- CBP formed a Secure Border Initiative (SBI) Executive Steering Committee (ESC) to provide oversight of the implementation of SBI and SBI*net*. The SBI ESC serves as an advisory board, helping the SBI Executive Director to effectively implement program management decisions.
- SBI is developing, documenting, and implementing sound program and performance management processes. SBI developed a process asset library, with a baseline of 76 program management policies, plans, processes and procedures. The program has established scheduling standards for the development and maintenance of the Integrated Master Schedule and project schedules. SBI has established processes and procedures for Earned Value Management System baseline analysis and reporting. Monthly Program Management Reviews, which address cost, schedule, performance, and risk – are conducted to monitor the program progress. Oversight of Prime contractor deliverables are performed to ensure measures and metrics reported are consistent and traceable to the Quality Assurance Surveillance Plan.
- SBI and SBI*net* have significantly increased organizational capacity, adding 168 staff members to help manage the program and address crosscutting issues such as coordination with USCG on maritime border security issues.

Remaining Plans

Fielding Border Surveillance Technologies / SBInet Program Management

- CBP is committed to build a total of 370 miles of fence and 200 miles of vehicle barriers along the Southwest Border by the end of calendar year 2008.
- CBP is committed to deploying 70 communications, camera, and radar towers by the end of calendar year 2008.

FY 2007 Challenge 3: Grants Management

Summary of 2007 Challenge: The OIG letter acknowledges that managing the multitude of grant programs within DHS poses a significant challenge. Further, the grant programs of other Federal agencies that assist State and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural disasters compound this challenge. Congress continues to authorize and appropriate funding for individual grant programs with similar, if not identical, purposes. However, they comment that the Department must do more to coordinate and manage grants that are stove-piped for specific, but often related purposes, to ensure they are contributing to our highest national preparedness and disaster recovery goals, rather than duplicating one another and being wasted on low-priority capabilities.

2007 Accomplishments

- FEMA streamlined business processes from three legacy organizations into one FEMA Grants Directorate (transitioned legacy Preparedness Grants into FEMA).
- FEMA migrated the Grants and Training IFMIS Financial System and the Payment and Reporting System web system from the Office of Justice Programs to FEMA.
- FEMA stood up a Grant Programs Directorate with no additional resources and awarded over $4 billion dollars in non-disaster Federal assistance while working through transition issues of migrating the Office of Grants and Training to FEMA.
- FEMA provided advanced level grants management training to States, local governments, non-profit organizations, and other grantee recipients all across the country and in the territories.
- FEMA Headquarters (HQ) collaborated with its Regions to interview 20 Grants Management Specialists (GMS) to begin financial grants work related to transitioned preparedness grants in the Regions. This was a huge undertaking for both HQ and Regional offices as these positions came as a result of the reprogramming and were announced and interviewed in a short timeframe.

Remaining Plans

- FEMA is striving for strong collaboration with its Regional offices to work towards the new FEMA vision.
- FEMA will hire and train 20 new Grants Management Specialists in the Regions to facilitate more coordination with local partnerships.
- FEMA is working to transition the administration of preparedness grants to FEMA Regional offices.

- DHS is in the process of streamlining all the DHS grant management business processes to provide oversight monitoring capability as well as unified grant management processing.
- DHS HQ is establishing a DHS-wide audit tracking system that will record and track resolution completion for the A-133 audit process. This will ensure that audits are resolved in a timely manner and that trends in audit findings are addressed.
- DHS is working with the OIG in reviewing the 36 Federal assistance programs (identified as potential programs that may duplicate DHS programs) to determine if they duplicate or complement DHS programs.
- DHS HQ is anticipating the transfer the Office of Grant Policy and Oversight from the Office of the Chief Procurement Officer to the Office of the Chief Financial Officer in order to provide resources for a more robust oversight capability related to accountability of funds, internal controls and audit processing.

FY 2007 Challenge 4: Financial Management

Summary of 2007 Challenge: Per OIG, financial management is a significant challenge for DHS. A number of material weaknesses in internal control continue to exist. The material weaknesses in internal control are impediments to obtaining an unqualified opinion and have precluded management from giving positive assurance over internal control at the Department level. DHS's ability to obtain an unqualified audit report, and provide assurances that its system of internal control is designed and operating effectively, is highly dependent upon process and procedural improvements across DHS.

However, the Department notes that many of our material weaknesses were inherited and are longstanding challenges. These challenges will not be solved in a single step, but through near and long-term fixes. The auditor's reports highlight the challenges we face. They identified weaknesses that have occurred for a variety of reasons common to newly formed organizations, such as inconsistent processes, reliance on legacy policies, undeveloped internal controls, incomplete and inaccurate information, or systems that cannot properly process reliable data and information. But we are not stopping at simply fixing what the auditors find. One of the most important lessons learned from our initial years of implementing the DHS Financial Accountability Act involved shifting from just focusing on audit opinions or addressing auditor-identified issues to also building support for the Secretary's Assurance Statement by focusing on management-identified root causes and management-performed test work. While audit outcomes are important, we will also concentrate on management's responsibility for internal controls. Through our multi-year internal controls assessments, we are documenting the design of our controls to best discover the root causes of a problem and to guide our corrective action efforts. We will then test their operating effectiveness to build support for the Secretary's Assurance Statement.

2007 Accomplishments

- On March 1, 2007, the Secretary and Chief Financial Officer issued the inaugural version of the Internal Control Over Financial Reporting (ICOFR) Playbook. The ICOFR Playbook represents an ambitious multi-year effort to build assurances and retire material weakness conditions. Highlights of significant FY 2007 accomplishments include:

  - Strengthened the control environment within the Office of the Chief Financial Officer and bolstered financial management and oversight functions with the strong support of the Department's Secretary and Under Secretary for Management;
  - Implemented Department-wide financial reporting process improvements;
  - Developed Department-wide financial management policies and procedures;
  - Developed standard operating procedures at TSA to improve financial reporting control activities;
  - Provided oversight and held Component management accountable for financial system security corrective actions through partnership between the Under Secretary for Management, Chief Financial Officer, Chief Information Officer, and Chief Information Security Officer, resulting in compliance with the Federal Information Security Management Act;
  - Implemented policies and procedures to improve accounting for legal contingent liabilities, intragovernmental and interdepartmental reconciliations, and capitalization of internal use software; and
  - Sustained FY 2006 progress at ICE and eliminated all remaining ICE material weakness conditions.

Remaining Plans

- Significant challenges remain at USCG and FEMA. To support these Components, the Department's Chief Financial Officer conducts monthly corrective action meetings with Senior Management and weekly working group meetings with Senior Staff. Highlights of these support efforts include:
  - Setting USCG priorities for resolution of ten material weakness conditions, based on risk, resource availability, mission impact, and other factors.
  - Partnering with the Under Secretary for Management and Department's Chief Procurement Officer to strengthen management and oversight functions at FEMA and establishing internal controls for delivering benefits and assistance to disaster victims.
- A summary of planned corrective action efforts is provided within the Other Additional Information's Summary of Financial Statement Audit and Management Assurances section.

FY 2007 Challenge 5: Information Technology Management

Summary of 2007 Challenge: According to OIG, integrating information technology (IT) systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for secure, effective communications and information exchange remains one of DHS's biggest challenges. OIG believes it is essential that DHS implement a Department-wide program to ensure effective information security controls and address IT risks and vulnerabilities. They also believe it is critical that the Department acquire and implement systems and other technologies to streamline operations within DHS Component organizations, and to support effective information sharing with State and local governments, the private sector, and the public. Finally, they opine that DHS is challenged in addressing privacy concerns while integrating its myriad systems and infrastructures.

Department-wide IT Infrastructure

2007 Accomplishments

Department-wide IT

- Completed 50 percent of IT projects within 10 percent of the cost and schedule dates.
- Integrated information security architecture with DHS Enterprise Architecture (EA), System Development Life Cycle (SDLC), Capital Planning Investment Control (CPIC), and acquisition processes.
- Implemented National Institute of Standards and Technology (NIST) SP 800-53 in policy and information security compliance tools.
- Developed and deployed the DHS Information Security Scorecard for communicating departmental progress in Certification and Accreditation (C&A), FISMA Compliance and Weakness Remediation.
- Consolidated IT support for unclassified, Secret, and Top Secret local area networks (LANs) into a single vendor to improve service delivery and cost efficiency.
- Leveraged delivery of infrastructure operations and management (O&M) to capture additional cost reductions and efficiencies as the population continues to grow.
- Supported the migration of legacy data centers to two DHS Data Centers.
- Increased the use of IT research and advisory service contracts by DHS personnel by 100 percent over the prior year.
- Developed and initiated a plan to establish test facilities at the DHS enterprise data center.
- Developed a plan to integrate DHS IT test facilities and consolidate these with data centers in coordination with Science and Technology Directorate.

Information Technology Services

- Continued the enterprise implementation of the Department-wide Smart Buy enterprise license agreement for access to Geographic Information System (GIS) software/training, saving DHS approximately $4 million over General Services Administration (GSA) list pricing.
- Coordinated a Department-wide investment in geospatial data through partnership with the National Geospatial-Intelligence Agency and the U.S. Geological Survey, achieving $12 million in cost avoidance.
- Implemented the Enterprise Information Repository to support IT security, portfolio management, program oversight, and Enterprise Architecture governance.
- Completed the target architecture for the Technology Reference Model (TRM), including completion of Enterprise Architecture (EA) TRM insertion packages for 18 critical technology areas.
- Formalized a strategy for the enhancement of information sharing by developing and enhancing workflow, document management, and Business Process Management (BPM) capabilities to increase user satisfaction by 40 percent and decrease cost by 15 percent while also reducing production time by 25 percent.
- Established a repeatable process for the DHS CIO to approve procurements that contain IT elements of $2.5 million and above to ensure that all contracts fully comply with FISMA;
    - Partnered with the Office of Procurement Operations (OPO) and Chief of Administrative Services (CAO) to share data to provide offices with advanced notice of procurements and purchases of property.

- Established preliminary performance measures that will be refined after at least 12 months of data are reported.

- Developed and executed the IT Budget Review Process, ensuring that IT requirements are integrated with the FY 2009-2013 Resource Allocation Plan data call. Reviewed and made recommendations regarding Component portfolio and investment IT budgets. Reduced duplication and showed cost savings of 5 percent of the budget of one portfolio through the analysis and implementation of recommendations.
- Complied with the President's Management Agenda (PMA) and the OMB mandate to implement and monitor Earned Value Management (EVM) and Operational Analysis (OA).
- Identified Portfolio Managers for all of the DHS Portfolios and half of the Portfolio managers directly contributed Portfolio analysis to the budget, acquisition, and investment review process.
- Implemented Application Authentication for: the Secretary's Priority Tracker, the Homeland Secure Information Network (HSIN), DHS's primary authentication service enabling E-authentication, and for the FedBridge capability for the Department. Identified and consolidated the Disaster Management (DM) technology platform onto the target HSIN platform, resulting in more than $2 million savings in FY 2007.
- Integrated Disasterhelp.gov with E-authentication, meeting the OMB milestones.
- Implemented new enterprise Learning Management Systems for DHS headquarters and several Components.
- Issued first DHS Smartcard in advance of the October 27, 2006 deadline.

Wireless Activities/Security Activities

- Processed 3,795 frequency assignment records in support of DHS operations including coordination of 410 assignment proposals and spectrum support for CBP Project-25 upgrade and modernization efforts in Arizona.
- Jointly led with the Department of Justice (DOJ) government-industry interchange, design competition, and final selection for $10 billion, 15-year Integrated Wireless Network contract vehicle.
- Established a primary Network Operation Center (NOC) and Security Operation Center (SOC) to full operating capability.
- Completed 90 percent of Component migrations to MS Exchange.

Homeland Secure Data Network

- Established a second backup data center at the Stennis, Mississippi data center to provide increased system availability and disaster recovery with 24/7 operations during times of national incidents or disasters.
- Established a secondary access point to DOD Secret Internet Protocol Router Network (SIPRNet) to increase availability to HSDN critical customers.
- Migrated the HSDN Backbone to OneNet, providing OneNet connectivity to the HSDN Data Center to support field site deployments on OneNet.

Information Security

- Comprehensive Certification and Accreditation process in place.
  - At the end of July 2007, 88 percent of FISMA systems had valid Authority to Operate letters.
- Improved Plan of Action and Milestones (POA&M) tracking process for remediating security weaknesses
  - Closed 363 of 438 IT security audit findings.
- Annual user IT Security Awareness Training is at or near 100 percent for all employees and contractors with system access.
- Configuration guides have been published for all operating systems in the department.
  - The Department has validated configuration compliance programs for all Components.
  - Components have reported that over 90 percent of systems in the Department have implemented configuration guides.
  - Percentage of systems that have completed annual National Institute of Standards and Technology Special Publication 800-53 assessments is over 90 percent..
- Enhanced security operations capability.
  - All Components now regularly report IT security incidents to the DHS Security Operations Center, who in turn report to US-CERT, as appropriate.
  - Improved DHS Security Operations Concept of Operations published in 2007, detailing specific enterprise-wide security operations procedures.

<u>Remaining Plans:</u>

Department-wide IT

- Maintain full FISMA compliance for each of 700+ systems in the Department's inventory.
- Complete the implementation of the plan to retire all financial systems security weaknesses.
- Update Security Policy and Architecture Guidance to address new operational requirements, advancing technology, and new threats as well as adapting new best practices.
- Complete a rigorous review and analysis of the standards, products, and services contained in the Technical Reference Model to ensure they comply with the Security Architecture.
- Begin to replace all IT hardware assets per National Capital Area (NCA) - developed replacement periods (e.g., wireless devices – 18 to 24 months, personal equipment – 36 months, and server/network equipment – 48 to 60 months).
- Conduct requirements gathering and planning for the development of the new consolidated DHS location at the St. Elisabeth's campus.
- Ensure capability readiness and migrate legacy data center systems to the two DHS Data Centers.
- Implement testing of information technologies at the DHS enterprise data center.

Information Technology Services

- Migrate 100 percent of DHS enterprise to Environmental Systems Research Institute (ESRI) SmartBuy investment.

- Stand up initial geospatial data warehouse capability at the DHS Enterprise Architecture and DHS's National Center for Critical Information Processing and Storage (NCCIPS) Data Center at Stennis, Mississippi.
- Deploy standardized and interoperable common operating picture (COP) technology, support the NOC, the National Infrastructure Coordination Center (NICC), and the National Response Coordination Center (NRCC), and formalize this architecture as part of the DHS Enterprise Architecture through the technology insertion process.
- Oversee the Single Sign-On integration with the DHS Portal Environment.
- 100 percent of IT Portfolios Managers will directly contribute Portfolio analysis to the budget, acquisition, and investment review process.
- 100 percent of DHS Portfolios will identify IT EA targets
- Initiate Portfolio Management framework across 25 percent of DHS Components.
- Complete the migration of consolidated Disaster Management technology platform onto the target HSIN platform.
- Continue implementation of the new enterprise Core Personnel system (EmpowHR) for ICE, USCIS and other Components.
- Implement new enterprise Learning Management Systems additional Components.
- Continue to implement new enterprise Recruitment suite of systems (ICE, USCIS, CBP, and other Components).
- Provide Program Management Support for Information Quality and ensure that the Department remains compliant.
- Provide Program Management Support for Government Paperwork Elimination Act and ensure that the Department remains compliant.
- Define standard capability for Smartcard issuance and scale for use by all Components.

Security Activities
- Move all remaining Components to OneNet with centrally managed Network Services with enterprise-wide NOC/SOC services.
- Establish a secondary NOC/SOC.
- Complete Component migrations to MS Exchange.
- Establish disaster recovery capability between the two DHS Data Centers.

Homeland Secure Data Network
- Establish and maintain periodic HSDN program self-assessment and evaluation through the DHS established Operational Analysis periodic review and reporting process in order to identify areas for improvements in costs and operational efficiencies and effectiveness.
- Establish support for the mission requirements of DHS Component organizations and homeland security partners staying abreast of and identifying applicable advancing information and applied technologies capable of improving data gathering, fusion, analysis, intelligence gathering and dissemination at a SECRET-classified level.

Information Security
- Comprehensive Certification and Accreditation process in place.
  - Goal is 100 percent of FISMA systems have valid Authority to Operate letters.
- Close all IT audit findings.
- Annual user IT Security Awareness Training is at 100 percent for all employees and contractors with system access.

- Configuration guides have been published for all operating systems in the department
    - The Department validates configuration compliance programs for all Components.
    - Percentage of systems that have completed annual National Institute of Standards and Technology Special Publication 800-53 assessments is 100 percent.
- Enhance security operations capability by continuing to report all IT security incidents to the DHS Security Operations Center, who in turn reports to US-CERT, as appropriate.

Component IT Management

2007 FEMA Accomplishments

- Started modernization and upgrade efforts to improve information sharing and functionality among six critical systems.
    - National Emergency Management Information System (NEMIS);
    - Logistics Information Management System (LIMS-III);
    - Automated Deployment Database (ADD);
    - Total Asset Visibility (TAV);
    - Integrated Financial Management Information System (IFMIS); and
    - Acquisition Management System (PRISM).
- Migrated the Grants and Training IFMIS Financial System and the Payment and Reporting System web system from the Office of Justice Programs to FEMA.
- Participated in two field operation demonstrations and exercises to test our interoperability with Federal, State and local response efforts, and our communications plans in order to identify failures or shortcomings, corrected by June 1, 2007.
- Expanded State and local communications planning efforts to include assistance in the development of interoperable communications plans for all States in Regions 4 and 6, Puerto Rico and the Virgin Islands, as well as all Emergency Support Functions that are on the Federal response team to assist in disasters.
- Acquired 34,000 licenses of the Asset Tracking Software (CompuTrace Complete) and deployed 3,399 licenses on laptops supporting disasters.
- Acquired 36,450 licenses for Full Disk Encryption software to support laptops used in support of disaster operations.
- Acquired 4,000 licenses of 2-Factor authentication solution as a FEMA pilot to comply with OMB M06-16.
- Replaced Egress and DMZ Firewalls that were becoming obsolete.
- Completed pilot on deploying an Enterprise Patch Management solution and developed schedule for Agency-wide deployment.
- Acquired software for Enterprise Patch Management solution and currently deploying agents.
- Installed NetIQ Security Manager on critical servers to monitor critical network devices, specifically egress firewalls, virtual private network concentrators and some ingress firewalls.
- Provided training for 28 Information Systems Security Officers.
- Completed plan to support and guide critical IT improvements with the following five Strategic Imperatives: 1) Stabilize and Integrate IT Assets Across the Agency; 2) Secure the IT environment; 3) Network the Agency; 4) Evolve to a "Service-Forward" Organization; and 5) Establish the Supporting IT Policy and Governance Structure.

- Continued refining and documenting IT management practices, policies, and procedures.
- Implementing Enterprise Architecture based standards of interoperability, security, and cost efficiency.
- Completed initial architecture-based analysis of systems.
- Identified mission critical systems.
- Determined mission needs through customer analysis and began work to identify functions that the Office of the CIO is currently capable of providing to meet needs.
- Began process of aligning system functions to meet FEMA's mission needs.
- Created system guidance to direct technical improvements and system upgrades.
- Upgraded several systems to improve their capabilities and ability to share information.
- Continued the monthly project management and professional development training sessions.
- Continued analysis of the optimal project and portfolio management tools and implementation options.

FEMA Remaining Plans

- Continue upgrade of six critical systems, NEMIS, LIM-III, ADD, TAV, IFMIS, and PRISM.
- Complete Mitigation Advisors Statistical Tracker.
- Improve operations and testing by creating Integrated Test Facility for software, updating the Test Development Laboratory servers, and evolving two testing environments to the required five environments which will allow NEMIS modules to be reengineered and replaced completely with a minimum number of disruptions (phased completion).
- Replace legacy servers to improve processing speeds, increase capacity, and reduce the number of replication cycles in the current systems.
- Deploy Emergency Management Mission Integrated Environment and migrate data to that system from Regional server.
- Deploy Document Management and Records Tracking System for multiple FEMA applications.
- Complete development of numerous Individual Assistance support systems including the National Shelter System, Fulsome letters, Web indexing code, Web Registration Intake, and the IA Center.
- Work with Emergency Management Institute to develop concurrent training plans and materials
- Acquire and deploy 10,000 additional licenses for Asset Tracking Software (CompuTrace Complete) on all FEMA laptops.
- Deploy Full Disk Encryption software to support 36,450 remote access users as a FEMA pilot Install 4,000 licenses of 2-Factor authentication solution (RSA) as a FEMA pilot to comply with OMB M06-16 Fully deploy Enterprise Patch Management Solution Agency-wide.
- Expand implementation of NetIQ Security Manager for any security-related events including failed logon attempts and configuration changes.
- Conduct security assessment to determine effectiveness of security measures to ensure secure sharing of information.
- Deploy Community Information System (CIS) v4.5 Code into production.
- Complete development of Electronic Fingerprint System (EFS).
- Complete Enterprise Oracle database improvements.

- Develop Emergency Management Information Management System (EMIMS).
- Complete Executive Management System v1.0 (EMS).
- Complete EMS v2.0.
- Deploy Fire Grants Review/Award V4.30 to production.
- Implement process improvement for software development projects and execute project reviews Implement MS Project Server 2007.
- Complete project to limit to three failed login attempts to database.
- Develop Personally Identifiable Information Application & database.
- Develop Real Property Management Application.
- Develop Real Property Management E-Dashboard.
- Implement Tower TRIM (Mitigation Electronic File Storage).
- Implement Travel Manager v9.0.
- Complete consolidation of training database.

2007 USCIS Accomplishments

- Integrated seven legacy enterprise applications through a Service Oriented Architecture Enterprise Service Bus improving information access and sharing with another Federal Department.
- Implemented and instituted the USCIS information technology lifecycle management process.
- Implemented and instituted an Office of Information Technology organizational structure based on the industry best practice model of information technology infrastructure library and information technology service management.
- Received Departmental approval for USCIS's Transformation Program Concept of Operations and Strategic Plan and the Transformation Program for Milestone Decision Point (MDP) two – Concept and Technology Development Phase.
- DHS's Enterprise Architecture Community of Excellence approved USCIS Transformation Program for Milestone Decision Point two – Concept and Technology Development Phase.
- USCIS Transformation Program Office (TPO) completed foundational documents to support the Program Management Office including: Program Management Plan, Governance Plan, Risk Management Plan, Quality Management, Change Management Plan, and Communication Plan.
- Initiated Federal Stakeholders Advisory Board that includes members from: CBP, USCIS, I&A, Department of Justice, Department of State, ICE, Treasury, and US-VISIT.
- Completed the Transformation Increment 1 Target Business Process definition which defines the business model and high-level requirements for the program.
- USCIS TPO completed initial round of field briefings and focus group meetings with field leadership.
- For the pilot projects, the TPO engaged users through focus groups and surveys to gather and validate requirements, validate new business processes, and collect feedback for future requirements.
- Deployed three pilot projects – Secure Information Management Service, Enterprise Document Management System, and Enumeration.

USCIS Remaining Plans

- Complete procurement of Solutions Architect services.
- Begin development of integrated operating environment.
- Complete hiring process to staff Enterprise Architecture Branch with the USCIS Office of Information and Technology.
- Execute USCIS EA development plan to achieve level three maturity.
- Facilitate USCIS-wide performance architecture task force to gather and analyze performance measures and metrics

FY 2007 Challenge 6: Infrastructure Protection

Summary of 2007 Challenge: OIG acknowledged that the Nation's distribution of critical infrastructure and key resources (CI-KR) is enormous and complex. The requirement to rely on Federal partners and the private sector to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI-KR. However, according to OIG, the Department continues to face a challenge in prioritizing its protection efforts based on risk and mission requirements and needs to incorporate threat information into its risk assessments and coordinate the funding of protective measures for CI-KR.

2007 Accomplishments

The Department of Homeland Security's Office of Infrastructure Protection (OIP) is responsible for coordinating and advancing protection efforts throughout all 17 critical infrastructure and key resource sectors:

- The completion of the National Infrastructure Protection Plan's Sector Specific Plans (SSPs) is just one of many OIP activities that illustrate the evolution of the Department's CI-KR protection capabilities. This undertaking represents the first time that government and the private sector have worked together on such a large scale to develop a joint plan for protecting the Nation's key assets and resources. In completing the SSPs, DHS:
    - Worked with the private sector to implement tailored protective measures, including conducting site-assistance visits and transforming feedback into educational reports that owners and operators can use to identify vulnerabilities;
    - Worked with the private sector to develop more than 800 Buffer Zone Protection Plans (BZPP) to enhance security around critical infrastructure;
    - Provided security guard training and courses on increasing terrorism awareness; and
    - Boosted information sharing across the sector through the Homeland Security Information Network (HSIN), which has a specifically dedicated portal for critical infrastructure.
- More work continues in these different sectors. For example, in the chemical sector, DHS issued an Interim Final Rule for Chemical Facility Anti-Terrorism Standards in April 2007. The Department is now finalizing the final rule, ensuring vulnerability assessments are conducted, and fostering the development of site security plans. OIP also began sector-wide registration processes in the Nuclear, Oil and Gas, and Chemical Sectors to clearly identify all owners and operators.

- Sharing information on threats in the form of tailored strategic sector-specific risk assessments, vulnerabilities, consequences, and protective planning was an essential underlying foundation for executing these activities and completing these deliverables.
- Because strategic information motivates protective investments and preparedness, the National Infrastructure Protection Plan (NIPP) Sector Partnership Model, which is fully operational, has been and will continue to be an essential mechanism for the exchange of strategic information at an unprecedented level between government and the owners and operators of CI-KR.
- The National Infrastructure Coordinating Center (NICC) has taken important strides in the realm of information sharing. Consistent with the NIPP "network approach" to information sharing, the NICC routinely shares a wide range of information products containing warning, threat, and CI-KR protection information via HSIN-Critical Sectors (HSIN-CS). During the last year, the NICC has posted more than 900 information products to HSIN-CS for use by CI-KR owners and operators.
    - Nine of the CI-KR sectors or major sub-sectors have signed MOUs with DHS to deploy HSIN-CS to their sectors, which reflects a long process to overcoming challenges unique to information sharing with the private sector.
    - This comprehensive environment and its mechanisms have been formally adopted by the Program Manager, Information Sharing Environment (PM-ISE), as the private sector component of the information sharing environment.
- The Buffer Zone Protection Program reduces the threats and vulnerabilities for critical infrastructure through identification and analysis of critical infrastructure sites and by providing grant funding to law enforcement entities to mitigate identified gaps. DHS is documenting, through the Vulnerability Reduction Purchasing Plan (VRPP), how BZPP grantees are utilizing the grant money to reduce threat and vulnerabilities.
    - OIP provided $25 million of BZPP grant funds for increased local law enforcement (LLE) capability to protect the buffer zones around high-risk chemical facilities.
    - OIP completed 200 Buffer Zone Plans and provided $50 million in BZPP grant funds for increased LLE capabilities.

In addition, OIP:

- Completed 110 Site Assist Visits (SAVs) in conjunction with Federal, State, local, and private-sector stakeholders.
- Completed the remaining 28 (of 65 total Nuclear Power Plants) Nuclear Comprehensive Reviews (CRs).
- Completed the remaining 5 of (6 total high-risk chemical regions) Regional Chemical CRs.
- Completed 130 Soft Target Awareness Courses to LLE and private sector security managers.
- Completed 50 Surveillance Detection Courses to LLE protecting the CI-KR.
- Completed FY 2008 Tier 2 Data Call for infrastructure information with States and SSAs.
- Achieved initial operating capability of iCAV system to provide situational awareness within the National Operations Center.
- Completed the 2007 National and Sector CI-KR Protection Annual Reports in accordance with the NIPP.
- Initiated and completed the 2007 NIPP CI-KR Protection Core Metrics Initiative to include NIPP and OIP implementation actions.

Remaining Plans

DHS will continue to prioritize resources and activities based on risk. In addition, OIP will:

- Develop a scalable assessment methodology to execute SAVs, Buffer Zone Protection Plans, Comprehensive Reviews, and High-Risk Infrastructure Cluster Assessments. This represents an important step in working with other Sector Specific Agencies to standardize assessment methodologies while fulfilling bombing prevention requirements, providing accessibility to State and local partners, and allowing Protective Security Advisor-led assessment teams to coordinate and report on vulnerability assessments in the field.
- Integrate 10 National Guard teams into the Vulnerability Assessment project and conduct approximately 300 vulnerability assessments on Tier 1/2 CI-KR. The National Guard will test, evaluate, and calibrate the new methodology.
- Conduct the high-risk cluster assessment pilot on 72 assets in the Lower Manhattan Security Initiative and 24 assets in the District of Columbia Metroplex Initiative. These assessments will allow OIP to evaluate and enhance the methodology to conduct full scale High-Risk Infrastructure Cluster assessments in following years.
- Expand the CR effort to conduct assessments for high-consequence sectors such as liquefied natural gas.
- Establish a Protective Measures Section to track Federal, State, and local government and private sector assessments and protective actions. This section will collect and analyze information to evaluate the effectiveness of assessments, protective measures implemented, and grant funding provided to high-priority CI-KR.
- Evolve the National Asset Database into an integrated Infrastructure Data Warehouse (IDW) with raw CI-KR-related asset information and completed CI-KR information products. All NIPP Stakeholders will have access to the IDW via a common graphics user interface.
- Review, as requested, sector-specific risk assessment methodologies to ensure NIPP compliance, and then assist with the technical implementation of the tool for use in the collection and assessment of sector-level CI-KR.

FY 2007 Challenge 7: Border Security

Summary of 2007 Challenge: The OIG letter asserts that one of DHS's primary missions is to reduce America's vulnerability to terrorism by controlling the borders of the United States. This is dependent on the coordinated accomplishments of DHS, as well as joint efforts with other agencies. To this end, DHS is implementing a comprehensive multi-year plan to secure the borders and reduce illegal immigration, called the Secure Border Initiative (SBI). OIG believes that DHS must quickly establish the organizational capacity to oversee, manage, and execute a program of this size and scope. Until the operational and contract requirements are firm, effective performance management and cost and schedule control are precluded. Concurrently, CBP must increase the number of agents by 6,000 in less than three years. The rapid timeline presents risks in recruiting and training fully qualified agents and procuring the necessary infrastructure to support them.

2007 Accomplishments

Fielding Border Surveillance Technologies / SBI*net* Program Management

- CBP awarded an SBI*net* task order to demonstrate the effectiveness of the overall approach to SBI*net* along 28 miles of border flanking the Sasabe Port of Entry (POE) in Arizona. CBP has made significant progress in implementing Project 28, including deploying all nine re-locatable camera and radar towers, and fitting all 50 of the Project 28 agent vehicles with Common Operating Picture hardware.
- Under the SBI*net* prime contract, CBP awarded a task order for the test and evaluation of fencing solutions. The purpose was to test effective low-cost solutions that meet operational requirements and can be reproduced for rapid deployment along the Southwest Border. This testing will help CBP add to existing tactical infrastructure to reach a total of 370 miles of fencing and 200 miles of vehicle barriers by the end of calendar year 2008.
- CBP met its commitment to construct 70 miles of primary fencing along the Southwest Border. This effort was comprised of both new and previously planned projects brought together under SBI*net*.
- CBP formed a Secure Border Initiative (SBI) Executive Steering Committee (ESC) to provide oversight of the implementation of SBI and SBI*net*. The SBI ESC serves as an advisory board, helping the SBI Executive Director to effectively implement program management decisions.
- SBI is developing, documenting, and implementing sound program and performance management processes. SBI developed a process asset library, with a baseline of 76 program management policies, plans, processes, and procedures. The program has established scheduling standards for the development and maintenance of the Integrated Master Schedule and project schedules. SBI has established processes and procedures for Earned Value Management System baseline analysis and reporting. Monthly Program Management Reviews, which address cost, schedule, performance, and risk – are conducted to monitor the program progress. Oversight of Prime contractor deliverables are performed to ensure measures and metrics reported are consistent and traceable to the Quality Assurance Surveillance Plan (QASP). .
- SBI and SBI*net* have significantly increased organizational capacity, adding 168 staff members to help manage the program and address crosscutting issues such as coordination with the Coast Guard on maritime border security issues.

Office of Border Patrol

- OASISS (Operation Against Smugglers Initiative for Safety and Security) has been embraced and expanded by both the U.S. and Mexico as a successful cross-border prosecution and deterrent to smugglers who jeopardize the lives of aliens.
- 311 cases were generated, a 9 percent increase over FY 2006, with an 86 percent acceptance rate.
- Interior Repatriation (13,292 aliens were removed via this program) along with OASISS has complimented the Border Security Initiative campaign to inform and deter potential crossers.
- Operation Streamline has decreased Del Rio Sector apprehensions by 47 percent (and Other Than Mexican (OTM) apprehensions by a similar 46 percent).
- Nationwide apprehensions were down 19.5 percent for FY 2007 to 876,704.

- Nationwide apprehensions of OTM nationalities were down 37 percent to 68,016.
- 59,146 OTM aliens have been removed through the Expedited Removal (ER) program helping to end Catch and Release.
- In FY 2007, CBP significantly increased the number of Border Patrol Agents from 12,319 to 14,923 agents as part of the President's initiative to increase the ranks of the Border Patrol by 6,000 by December 31, 2008.
- The Border Patrol Academy participated in a curriculum review with the Federal Law Enforcement Training Center before initiating a new 81-day program.
- As of September 30, 2007, 1,712 agents have graduated from the Academy with 1,442 FY 2007 recruits still in class. This is a single year record for graduates at the Academy. To accomplish this goal the Academy doubled the size of permanent staff and has increased the number of temporary duty instructors. The infrastructure at the Artesia Academy was improved to meet the need; a new dorm, physical techniques training center, modular classrooms, and other additions have been made.
- The Academy has, with input from best in practice practitioners and from field Border Patrol Agents, designed a new Spanish language program and physical techniques training program. The redesign will ensure that new Agents who are already proficient in Spanish can complete the basic training at the Academy in 55 days. Those needing Spanish, will enter a 40 day task-based Spanish program.
- Planned for 6,000 new agents by December 31, 2008. Conducted site surveys of existing stations. Identified facility conditions and needs of each station receiving additional agents.
- Environmental kick off meeting conducted with environmental contracting firm on September 25, 2007 for all Integrated Project Team (IPT) projects. Environmental Assessments (EAs) to start immediately on identified sites.
- Initiated land acquisition activities for Rapid Response sites.
- Execution underway for several Rapid Response projects.
- Completed Rapid Response Planning IPT activities in April 2007. Outputs included initial cost estimates and program of requirements for all Rapid Response sites, prioritized list of projects, programmatic cost benefit analysis, risk management plan, and mission needs statement.
- Implemented cost and schedule management system for Rapid Response projects.
- Completed BP facilities for 12 sites.
- 36 renovations, additions, upgrades, and/or new facilities were completed in various locations.
- 184 acres acquired for five facilities.

Advance Passenger Information System (APIS)

- On August 23, 2007, the APIS Pre-Departure Final Rule, requiring air and vessel carriers to transmit complete APIS manifest data prior to sealing the aircraft doors or the departure of a vessel, was published in the *Federal Register*. This rule enables CBP to conduct no fly and selectee watch list screening prior to passengers gaining access to the aircraft or departing onboard a vessel, adding an essential layer to our anti-terrorism security measures. Carriers have been given 180 days from the publication of the rule to transition their systems into compliance.
- On September 18, 2007, the CBP Private Aircraft Notice of Proposed Rule Making, requiring pilots of private aircraft to transmit complete APIS manifest data 60 minutes prior to departure was published in the *Federal Register*. This rule enables CBP to conduct no fly

and selectee watch list screening and provide Landing Rights for Private Aircraft through an automated system, adding an essential layer to our anti-terrorism security measures.

Intelligence

- Developed a complete Field Intelligence Construct, and successfully validated it through a six month, Tucson, Arizona-based Pilot focused on the Southwest Border. This initiative integrates with and compliments the Border Security and Intelligence aspects of the SBI*net* Program.
- Developed a Strategic Threat Assessment Program and completed first assessment on the threat posed by Terrorism at the CBP Ports of Entry.
- Refined the Passenger Targeting Rules Set, resulting in increased focus on problematic passengers, and a reduction in delays and secondary screening of unlikely terrorists and other criminals.

<u>Remaining Plans</u>

Fielding Border Surveillance Technologies / SBI*net* Program Management

- CBP is committed to build a total of 370 miles of fence and 200 miles of vehicle barriers along the Southwest Border by the end of calendar year 2008.
- CBP is committed to deploying 70 communications, camera, and radar towers by the end of calendar year 2008.

Office of Border Patrol

- Extend Operation Streamline-like initiatives to other Border Patrol Sectors.
- Continue to refine the use Interior Repatriation and the OASISS program to deter at risk crossers.
- Continue to expand the use of ER to more eligible classes of aliens and in more geographic locations.
- The Border Patrol will further improve the Academy training program.
- The Academy plans to conduct 96 classes for a total of 4,800 trainees.
- Continue 55 Rapid Response program projects currently underway.
- In FY 2008, complete Border Patrol facilities for eight locations.
- Complete Northern Border standard, 50 agent standard station design.
- New construction activity underway in six sectors.
- Continue activity with offers pending with an estimated value of $3.8 million, for six site locations, totaling 123 acres.

Advance Passenger Information Systems (APIS)

- Monitor carrier compliance/implementation progress of requirements defined in the APIS Pre-Departure Final Rule.
- Finalize and publish the CBP Private Aircraft Final Rule upon analysis and reconciliation of comments received from the Notice of Proposed Rule Making.

Intelligence

- Deploy 2-3 Intelligence and Operations Coordination Centers and 6-10 Intelligence Coordination Teams to Border locations over a 24-month time frame commencing October 1, 2007. These are the key structural elements of the Field Intelligence Construct.

- Complete build out of the Strategic Threat Assessment Program to encompass All Crimes/All Threats; integrate programmatically into the new CBP Integrated Strategic Planning and Resource Allocation Process; and develop Indicators and Warning capability based on this program to provide, in concert with our mission partners, a first-ever Predictive Capability for All Crimes/All Threats.
- Enhance CBP Leadership and Mission Partner Situational Awareness by combining the Intelligence Watch and the Operations Situations Room conceptually and under one leader.

FY 2007 Challenge 8: Transportation Security

Summary of 2007 Challenge: The OIG's letter acknowledged that the size and complexity of the transportation system, which moves millions of passengers and tons of freight every day, make it a difficult system to secure and an attractive target for terrorists. The Nation's economy depends upon implementation of effective, yet efficient transportation security measures. The OIG claimed however, that since its inception, TSA has focused almost all of its attention on aviation security, perhaps to the detriment of other forms of transportation.

Checkpoint and Checked Baggage Performance

2007 Accomplishments

Screening SOP Refinements

- TSA has undertaken a number of initiatives in 2007 to improve checkpoint and checked baggage performance. Screening SOPs continue to be refined to shift attention from lower security risks, such as lighters, to address markedly higher security risks that could do catastrophic damage to an aircraft—IEDs, IED parts, and electric ignition devices. This focus is fundamental to a risk-based approach to aviation security. TSA continues to direct resources toward higher risk areas and make its security protocols less transparent to potential terrorists. We believe we gain a higher return in threat detection when our TSOs concentrate on finding explosive devices or components of explosive devices.

Screener Performance

Aviation Screening Assessment Program (ASAP)

- In order to improve screener performance, TSA instituted ASAP in 2007. The mission of ASAP is to measure screening performance using realistic and standardized assessment scenarios to improve aviation security. This is being accomplished by:
  - Establishing a three-tiered assessment system with standardized criteria and menu-driven scenarios;
  - Conducting on-going evaluation and modification to the program and scenarios;
  - Utilizing the local screening workforce including TSA Approved Instructors (TAI) and Bomb Appraisal Officers (BAO) as subject matter experts;
  - Integrating the program plan into the Transportation Security Inspector (TSI) Annual Inspection Plan; and
  - Providing clear and consistent communication to the field.
- The program's main goal is to achieve a national assessment measurement. This measurement provides information that helps TSA improve aviation security and identify vulnerabilities across screening operations.

Performance Accountability and Standards System (PASS)

- The objective of PASS is to promote and sustain a culture of high performance and accountability in TSA and to help achieve the organizational goals that support TSA's mission. PASS is designed to ensure that employees know what they need to do to accomplish their work successfully and to help TSA accomplish its mission through the use of a pay-for-performance system. PASS begins with a sit-down face-to-face planning meeting between employees and their supervisors or managers at the beginning of the performance period. At the end of the first and third performance quarters, quarterly discussions are held. A Mid-Year Review occurs halfway through the performance period, and the performance period wraps up with an End-of-Year Review.

Emerging Technologies

- TSA continues its efforts to identify and deploy emerging technologies that will constitute the next advancement in explosives detection screening at passenger security checkpoints. Those emerging technologies that are either in, or will soon be ready for, operational evaluation in screening for explosives includes: (1) Cast & Prosthesis scanners, (2) Whole Body Imagers, (3) bottled liquids scanners and (4) advanced carry-on baggage scanning technologies.

Additional Layers of Security

Aviation Direct Access Screening Program (ADASP)

- TSA is implementing ADASP as one more layer of protection against terrorism. Recent incidents in the United States and overseas have highlighted vulnerabilities that exist with regard to individuals with unescorted and unscreened access to secured areas and sterile areas of airports. Increased random inspections of individuals, accessible property, and vehicles entering secured areas and/or sterile areas are required to reduce the risk from these vulnerabilities.

Visible Intermodal Protection and Response (VIPR)

- To help combat threats such as the one experienced in Glasgow, TSA instituted VIPR, a visible deterrent to terrorist activity. VIPR consists of Behavior Detection Officers, Federal Air Marshals, Explosives Detection Canine Teams, Transportation Security Inspectors, and State and local law enforcement officers, who operate throughout the airport environment as an additional layer of security.

Remaining Plans

- To meet the challenges of a constantly evolving threat, our passenger screening systems must constantly evolve and adapt. To this end, TSA created a passenger screening task force charged with creating a new vision for aviation passenger screening. A vision that will enable TSA to focus more on high-risk individuals, that expands the range of threats that can be detected, that enables the information sharing across the enterprise, and that improves our system's ability to respond to ever-changing threat conditions. The task force has established guidelines for the development of the passenger screening system vision of the future. Next steps include integration of these guidelines and working with stakeholders, such as airports, to bring the concepts to fruition.

Passenger Air Cargo Security

2007 Accomplishments

- TSA has removed exemptions to screening to include the elimination of shrink wrap exemptions. In addition, TSA holds four weeks of core inspector training. Cargo Inspectors complete a two-week on-the-job training program. TSA's more than 460 canine teams each spend at least 25 percent of their work day in the cargo environment.

Remaining Plans

- TSA will plan direct nighttime and weekend inspection activities (when most of the cargo is moving) to better determine compliance with requirements, and conduct monthly "cargo strike" surges at high volume cargo airports. By the end of FY 2008, TSA will add another 170 canine teams to the force who's primary focus will be cargo, which will significantly increase the amount canine teams screening cargo.

Worker's Compensation

2007 Accomplishments

- Developed agency policies and procedures on the FECA program to include roles and responsibilities for the Office of Human Capital (OHC) and airport personnel.
- Developed and implemented a centralized, automated case management system to track the status of the Agency's workers' compensation cases.
- Provided 40 positions in which to concentrate exclusively on the Workers Compensation program in field locations.
- Developed and implemented FECA related performance goals and measures, and established performance standards for workers' compensation specialists and Federal Security Directors (FSDs) that will hold TSA officials accountable for program performance.
- Developed agency policies and procedures on TSA's chargeback process to include roles and responsibilities for OHC and airport personnel. Additionally, the verification process of reviewing and verification of the Chargeback Cost has been added to the *Workers' Compensation Desk Guide.*

Remaining Plans

- Finalize the Management Directive outlining roles and responsibilities for the FECA program, and continue to communicate the fact that locations should use the case management system and provide associated training.

Employee Workplace Issues

2007 Accomplishments

- TSA's Equal Employment Opportunity complaints are comparable to other deferral agencies. TSA's attrition is decreasing and is comparable to other transportation sector jobs. Additionally, TSO job satisfaction has increased significantly over the past two years. TSA has multiple processes for complaint resolution including the Ombudsman's Office, the Office of Civil Rights, Disciplinary Review Board, and Peer Review Programs. TSA has established a Model Workplace Program where employees and managers form councils to address workplace complaints and grievances.

Remaining Plans

- OIG is currently conducting an audit of employee workplace issues. At the conclusion of the OIG audit, TSA will review and address the identified findings and recommendations.

Rail and Mass Transit

2007 Accomplishments

- DHS has developed and administered grant programs for various surface transportation modes.
- Developed and adopted a strategic approach for implementing surface transportation security functions.
- Conducted threat, criticality, and vulnerability assessments of surface transportation assets.
- TSA has taken actions to develop and issue surface transportation security standards for passenger and freight rail modes.
- TSA has taken steps to conduct compliance inspections for surface transportation systems and has made progress in hiring and deploying inspectors.

Remaining Plans

- OIG and GAO are both conducting audits in this area. At the conclusion of the audits, TSA will review and address the identified findings and recommendations.

FY 2007 Challenge 9: Trade Operations and Security

Summary of 2007 Challenge: OIG states that trade operations and security are primarily the responsibility of CBP, although USCG and ICE also play important support roles. CBP has the mission of ensuring that all persons and cargo enter and exit the U.S. legally, while facilitating the lawful movement of goods and persons across U.S. borders. OIG believes CBP's three major challenges to meeting its trade mission are the modernization of trade systems, risk management programs to use scarce resources efficiently, and partnerships with the trade and foreign Customs offices.

2007 CBP Accomplishments

Container Security Initiative (CSI)
- Reached a milestone of 58 Operational CSI ports, covering 86 percent of U.S. bound maritime containers.
- Transitioned 12 CSI ports in eight countries to permanent staffing, bringing the total number of posts with permanent personnel to 40.
- Increased the level of examinations conducted at CSI locations by 92 percent.
- Evaluated 40 CSI ports using automated tools and protocols.
- Launched Secure Freight Initiative (SFI).

Cargo Enforcement Reporting and Tracking System (CERTS)
- The CERTS examinations and findings module, a component of Automated Targeting System, Version 4 (ATS-4), was actively deployed during FY 2007. This new module enables CBP Officers and Agriculture Specialists to report and track all CBP examinations and findings data using a single-point of entry application.
- ATS-4/CERTS is currently deployed to 36 CBP seaports, five CBP Airports, and two SFI seaports (Port Qasim, Pakistan and Port Cortes, Honduras).
- Thirty international airports have just finished sending representatives to the CERTS Train-The-Trainer Course.

Customs-Trade Partnership Against Terrorism (C-TPAT)
- Initiated 2,503 validations of which 1,812 have been completed, resulting in 5,314 total validations completed.
- Increased to a total of 156 Supply Chain Security Specialists (SCSS) positions.
- Implemented a third party validation pilot program and achieved several milestones to include: (1) soliciting applications from companies wanting to conduct validations on behalf of CBP in China on the Federal Business Opportunities Website and selecting 11 companies to participate; (2) identifying and inviting 304 validated importers to participate in the pilot; and (3) developing standard operating procedures to ensure consistent application of validation principles.
- Strengthened supply chain security through the development and issuance to the trade community of minimum-security criteria for U.S and Foreign-Based Marine Port Authority and Terminal Operator, Licensed U.S. Customs Brokers, Mexican Long Haul Carriers, and Air Carriers.

Automated Commercial Environment (ACE)
- Deployment of truck e-Manifest was completed at all land border cargo crossings (105 port codes, 144 sites).
- ACE e-Manifest, as required by the Trade Act of 2002, advance electronic cargo information mandate, was deployed at all ports by November 2007. The use of ACE e-Manifest became mandatory in Maine and Minnesota on October 12, 2007 and will become mandatory in Alaska on February 11, 2008.
- Ports with ACE truck e-manifest capabilities are operating at a compliance rate of nearly 100 percent.
- CBP collected nearly $1 billion dollars in duties and fees via the ACE periodic monthly statement payment process, which represents 36 percent of all duties and fees collected.

- Currently, there are 12,265 ACE accounts (10,189 truck carriers, 1,306 importers, 770 brokers, filers and sureties).
- ACE truck manifest capabilities are operating at 98 or 99 land border ports; the mandatory e-Manifest policy is in effect at 79 land border ports.
- Deployed initial ACE entry summary, accounts, and revenue capabilities on September 9, 2007.
- More than 245 users from 35 participating Government agencies are using ACE to access trade data, including more than 100 reports that draw from entry and entry summary data.
- Periodic monthly statement receipts grew to $1 billion, representing 42 percent of total adjusted collections. Overall, there are nearly 12,000 ACE Secure Data Portal accounts, and more than 8,000 corporate entities approved to pay duties and fees monthly.
- CBP achieved the planned target for the ACE Critical Few performance measures, based on the CBP Performance Reference Model (PRM), that track the number of ACE accounts, the percentage of duties and fees paid via the ACE periodic monthly statement process, the national percentage of e-Manifests filed, and the percent of reduction in truck processing time due to e-Manifest filing.
- CBP continues to fine tune ACE truck processing capabilities and is working to address and resolve system defects. The completion of computer hardware upgrades that were being performed during the survey period have resulted in officers at several ports reporting a remarkable improvement in ACE processing speed. A recent consolidation of system databases addressed previous system problems that often necessitated multiple system queries to obtain truck-related information, and since the consolidation, ACE has consistently provided officers with immediate access to this data. CBP also developed a portal-generated “cover sheet” that can be used by carriers as proof of filing an e-Manifest during system down times.
- CBP continues efforts to improve the availability and responsiveness of ACE user support, as well as communications to users and stakeholders regarding system status. Efforts taken to date include increasing help desk staff, referring more complicated inquiries to a higher tier of support, using automated phone messages to alert callers to system problems, and developing a communications plan for the immediate notification of ACE status to users and stakeholders. CBP held a National Truck Manifest Conference to brief CBP field staff on deployment, share lessons learned, and discuss both standard operating procedures and the aforementioned user satisfaction survey.

ATS Targeting Rule Revisions/Automated Targeting System: CBP Targeting Efforts/Initiatives

- Developed and implemented a new weight set for security targeting of ocean cargo. In addition the weight set performance is monitored and adjusted by incorporating identified seizures into the proxy positive set utilized in the Receiver Operating Characteristics rule performance model.
- CBP has designed, developed, and deployed the Mock Shipment Module. This module provides a platform for the development of scenario based shipment and evaluation of rule performance.
- Implemented with the U.S. Postal Service to utilize an automated targeting solution for outbound mail.
- Implemented a process to extract examination data, analysis shipment findings data, compare targeted shipments findings data utilizing Receiver Operating Characteristics

(ROCs), conduct impact assessments, and modify rules and weight sets as need to increase targeting effectiveness.

Office of International Trade

- Organized the trade functions resident in three different CBP offices into one Office of International Trade.
- Signed a Memorandum of Cooperation with China on intellectual property intended to reduce China's export of counterfeit goods.
- Increased intellectual property seizures by 22 percent to 7,245 (323 of which have a nexus to health and safety) with a value of $110 million, a year-on-year increase of 141 percent.
- Published an updated System of Records Notice, under the Privacy Act, and a Notice of Proposed Rulemaking for Privacy Act Exemptions in the Federal Register, and posted a revised Privacy Impact Assessment on the DHS web site for the Automated Targeting System (ATS). ATS is the premier tool employed by DHS and CBP to screen and vet, in advance, both persons, coming to and departing from the United States, and all cargo entering or exiting U.S. Commerce. The publication of this separate System of Records Notice and Privacy Impact Assessment for ATS permits CBP to ensure protections for individual privacy while contributing to the achievement of DHS's principal mission of preventing and deterring terrorist attacks. The ATS System of Records Notice and Privacy Impact Assessment establish strict time limits for the Government regarding the retention of personal or identity information belonging to international travelers and afford those same travelers the means to obtain access and correct the information that the CBP has collected about them and their travel itinerary.
- Enhanced the development of the ACE project by drafting and publishing Federal Register Notices that expanded the implementation of ACE e-manifest for trucks to all the land border locations and mandated the use of ACE e-manifest for trucks at all land border locations except for ports in Alaska.
- Supported the development of ACE by publishing Federal Register Notices that established formal terms and conditions for participation of trade members in the ACE test, increased the number and type of merchandise that can be released from CBP off the ACE e-manifest for trucks, and allowed third-party service providers to submit e-manifest information in the truck environment.
- A final rule requiring United States citizens and nonimmigrant aliens from Canada, Bermuda, and Mexico departing from or entering the United States from within the Western Hemisphere at air ports-of-entry to present a valid passport was published on November 24, 2006 in the *Federal Register*.
- A final rule requiring that electronic manifest information for passengers on board commercial aircraft arriving in and departing from the United States and passengers and crew onboard arriving and departing commercial vessels (with certain exceptions) be vetted by DHS against a government-established and maintained terrorist watch list prior to departure of the aircraft or vessel was published on August 23, 2007 in the *Federal Register*.
- Issued regulations implementing several Free Trade Agreements, including U.S. agreements with Chile, Singapore, Jordan, and Morocco.

Remaining CBP Plans

Container Security Initiative (CSI)
- Maintain 58 CSI ports, continuing coverage of 86 percent of containerized cargo destined to the United States.
- Train personnel to work with and support the Secure Freight Initiative (SFI).
- Evaluate remote targeting pilot project with real-time remote imaging and live video of the inspectional process.

Cargo Enforcement Reporting and Tracking System
- Deployment to all U.S. seaports and airport, the 58 CSI ports and the one remaining SFI port (Southampton, UK).

Customs-Trade Partnership Against Terrorism
- Conduct approximately 3,500 validations in FY 2008
- Finalize personnel actions to staff new offices in Buffalo, New York and Houston, Texas.
- Seek to finalize two additional Mutual Recognition Arrangements.

Automated Commercial Environment (ACE)
- Develop new ACE capabilities to strengthen screening and targeting.
- Complete deployment of ACE truck processing capabilities and expand the mandatory e-Manifest policy.
- Continue development of new ACE capabilities that will further strengthen border security and streamline operations for CBP officers and the trade community.

2007 USCG Accomplishments

The USCG continued to mature its Ports, Waterways, and Coastal Security (PWCS) program increasingly focusing on risk based measures and maximizing effects. Some key port security accomplishments include:

- The Coast Guard updated its operations order for Operation NEPTUNE SHIELD, which directs and guides field implementation of the PWCS mission. A few examples of recent improvements include:
    - Risk-based patrol activity: Improved effectiveness and efficiency of surveillance patrols by focusing patrol activity near maritime CI-KR at greatest risk, leveraging the Maritime Security Risk Analysis Model (MSRAM);
    - Risk-based escorts: Focused escorts on vessels laden Especially Hazardous Cargoes rather than all Certain Dangerous Cargoes;
    - Increased availability of aerial assets to conduct patrols and escorts increased USCG presence and reduced the threat of adversary planning; and
    - Prioritizing Security Activities: Emphasized execution of activities that produced greatest reductions in maritime risk and aligned resource usage on this risk based approach.
- Refined High Interest Vessel targeting matrix to focus boardings on vessels with highest risk.

- USCG commissioned two Maritime Force Protection Units, funded by the Navy, to provide dedicated security to transiting SSBNs and free up other USCG assets to perform other homeland security and non-homeland security missions.
- Engaged with small vessel community thru the June 2007 DHS National Small Vessel Security Summit to identify ways to mitigate risk associated with small vessels (< 300 Gross Tons).
- USCG Atlantic Area Commander and USN Commander Second Fleet developed a Homeland Security – Homeland Defense Concept Plan.
- Verified compliance with Vessel and Facility Security Plans through announced and unannounced spot checks and inspections
- USCG completed two Waterways Suitability Reports for LNG facilities in FY 2007.
- Underwater Terrorism Preparedness Plans (UTPPs) have been developed and delivered to 17 major ports. The goal of this program is to deliver actionable plans that local (field level) USCG commanders can use to readily access information about underwater capabilities and coordination mechanisms in their Area of Responsibility (AOR) to prevent, detect, and respond to an underwater threat. UTPPs are locally developed preparedness plans that establish preventive measures to make it more difficult for terrorist to conduct underwater surveillance or launch underwater attacks in and around our Marine Transportation System (MTS). Because if the complexity, scope, and potential consequences of an underwater terrorist event, UTPPs focus on preparedness of port partners through communications, coordination, enhanced awareness of potential threats, and clear delineation of roles and responsibilities in enhancing underwater security.
- USCG reorganized its deployable response capabilities under the Deployable Operations Group streamlining response capabilities of specialized teams and equipment to meet the Department's all hazards protect and respond requirement.
- USCG made significant improvements in National Maritime Strategic Risk Assessment (NMSRA), which enhances the utility of MSRAM.

Remaining USCG Plans

- The Coast Guard is in the final stages of review and prepared to publish an updated version of *Combating Maritime Terrorism.* This campaign plan details the way ahead for the PWCS mission and further expounds upon maritime governance, the Coast Guard's three-pronged approach to protecting the Nation's ports and waterways. As the *Combating Maritime Terrorism* plan matures, activities will be refined, risk reduction numbers will be validated, and the Coast Guard will leverage its DHS lead Federal agency role to provide a more comprehensive maritime risk reduction strategy.
- The Coast Guard leads an interagency group developing the National Strategy for Small Vessel Security that specifically examines and addresses the threats small vessels pose to free and smooth maritime commerce.
- The Coast Guard is consolidating the documents, policies, and procedures that encompass port security into a concise manual that provides direction to field units in the successful protection of the Nation's ports and free and smooth maritime commerce.
- The Coast Guard is developing implementation plans for an aggressive weapons training policy that maximizes technologies, reduces costs, is more environmentally friendly, and reduces risk.

- Maritime Force Protection Units: The first dedicated vessel arrives at Kings Bay, Georgia, in December 2007 and second arrives at Bangor, Washington, in April 2008.
- The Coast Guard made significant progress in FY 2007 toward updating Area Maritime Security Plan and Area Maritime Security Committee guidance. Through an inter-agency working group this plan will include implementation of the new SAFE Port Act (Section 101) requirements for a Salvage Response Plan to support expeditious post-TSI resumption of commerce. It also will assist in the implementation of the new DHS Strategy to Enhance International Supply Chain Security. This will then complete the first formal five year review and approval cycle mandated by MTSA.
- The Coast Guard intends to develop and deliver Underwater Terrorism Preparedness Plans to 12 additional ports.
- The Coast Guard is co-leading an effort with DHS to develop Adaptable Capability Packages of DHS-agencies specialized teams to respond and mitigate non-National Response Framework incidents. Testing of the concept continues with overall positive results.

GAO High-Risk Area - Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures

Summary of High-Risk Identification – As identified by GAO, protecting Federal computer systems and the systems that support critical infrastructures - referred to as cyber critical infrastructure protection - is a continuing concern. The continued risks to information systems include escalating and emerging threats such as phishing, spyware, and spam; the ease of obtaining and using hacking tools; the steady advance in the sophistication of attack technology; and the emergence of new and more destructive attacks.

GAO notes that as the focal point for Federal efforts to protect the Nation's critical infrastructures, DHS and its National Cyber Security Division have key cybersecurity responsibilities and claims that DHS has not yet completely fulfilled any of its key responsibilities. As an example, GAO asserts that DHS has not yet developed national cyber threat and vulnerability assessments or public/private recovery plans for cybersecurity. Per GAO, progress has been impeded by several challenges, including the reluctance of many in the private sector to share information with DHS, and a lack of departmental organizational stability and leadership needed to gain the trust of other stakeholders in the cybersecurity world.

2007 Accomplishments

DHS's National Cyber Security Division (NCSD), within the Office of Cyber Security and Communications (CS&C), continues to make progress developing and enhancing cyber analysis, watch and warning, and collaboration with the private sector:

- NCSD's U.S. Computer Emergency Readiness Team (US-CERT) provides a 24 hour, 7-day a week watch center to conduct daily analysis and situational monitoring to provide information on incidents and other events, as they are detected, to raise awareness and understanding of the current operating environment. The timely detection and analysis of cyber attacks helps to assess operational risk and mitigate the impact to our Nation's critical infrastructure.

- US-CERT's Einstein program enables the rapid detection of current and pending cyber attacks affecting agencies and provides Federal agencies with early incident detection. The information gathered by Einstein is used to provide actionable and timely alerts and reporting regarding current and impending cyber attacks, as well as indications and warnings of actual and potential intrusions to Federal Government computer security teams.
- US-CERT produces products that increase awareness among public and private sector stakeholders, including critical infrastructure owners and operators. This near real-time data collection and information sharing reduces cyber infrastructure vulnerabilities. US-CERT notifies public and private partners through a variety of products that encompass the National Cyber Alert System (NCAS). US-CERT established a vulnerability remediation process and the NCAS to collect, mitigate, and disseminate vulnerability information. NCAS is America's first cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. NCAS delivers targeted, timely, and actionable information for technical and non-technical audiences to enhance security. NCAS reports are made available through the NCAS, Information Sharing and Analysis Centers (ISACs), and on the US-CERT public website.
- Specifically for critical infrastructures, US-CERT produces Critical Infrastructure Information Notices (CIIN). Similar to the Federal Information Notice (FIN) provided to Federal agencies, the products are intended to provide information about a cyber security incident and make recommendations for avoiding or mitigating risks. The CIIN is specifically written to notify private sector organizations and Federal agencies involved with the protection of critical infrastructure.
- US-CERT relies on its collaboration with a variety of stakeholders and is working to formalize processes and procedures for collaboration with the private sector. US-CERT developed a draft concept of operations (CONOPs) for Private Industry Cyber Security Incident Handling that addresses information sharing, communication, and coordination with the private sector, including the ISACs. The CONOPs, which will be finalized in the near future, addresses sharing activities and coordination efforts with the private sector for cyber incidents, including Internet disruption.

In addition, CS&C:

- Drafted US-CERT Private Sector Concept of Operations (CONOPS).
  - Implemented US-CERT CONOPS across the Federal Government; the Office of Management and Budget (OMB) determined the US-CERT CONOPS to be a government regulation for Federal Government agencies within OMB.
  - Updated and implemented US-CERT CONOPS with the White House Policy Coordination Committee to define Personal Identifiable Information (PII) reporting requirements.
  - Refined Standard Operating Procedures (SOPs) to be consistent with US-CERT CONOPS.
- Standardized incident reporting across the government utilizing US-CERT's new incident tracking mechanism.
- Established an integrated joint operations center comprised of public and private sector members consisting of IT and communications organizations.

- Co-located US-CERT and National Coordinating Center for Telecommunications watch operations to facilitate the sharing of critical cyber and communications information.
- Engaged with the Partnership for Critical Infrastructure Security (PCIS) and Information and Analysis Center (ISAC) Council to develop a CONOPS and associated plans for coordinated watch and warning and incident response.
- Consistent with the NIPP Risk Management Framework, identified, assessed, and prioritized risks to the IT and Communications infrastructure, by analyzing threat, vulnerability, and consequence information.
- Continued to expand the National Vulnerability Database (NVD) to help establish a national baseline of specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).
- Provided outreach to the seventeen CI-KR sector operators; this provided situational awareness for analysis across the Federal Government, critical infrastructure, and the private sector, and enabled the US-CERT Analysis Program to correlate significant cyber incidents.

Remaining Plans

The Department has also held, and will continue to hold, exercises as mechanisms to identify ways to improve and promote public and private sector interaction toward enhancing situational awareness that supports decision making, communicating appropriate information to key stakeholder and the public, and planning and implementing response and recovery activities:

- NCSD is actively planning its second large-scale national cyber exercise, Cyber Storm II, which will be held in 2008. The exercise will build on Cyber Storm I, which enhanced DHS's relationship with private sector participants and helped to establish trust between the public and private sectors for future information sharing efforts. Cyber Storm II is being planned in close coordination with its stakeholders and participants. The exercise will feature a cyber-focused scenario that will escalate to the level of a cyber incident requiring a coordinated Federal response. Cyber Storm II is part of DHS's ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector.
- Cyber Storm II will also provide an opportunity to exercise new government and private sector concepts and processes developed since Cyber Storm I, such as Concepts of Operations and Standard Operating Procedures. The scenario will utilize coordinated cyber and physical attacks on critical infrastructures within selected sectors to meet a specific political and economic agenda (these cyber attacks will be simulated and will not impact any live networks). Participation will include Federal, State, local, and international governments, as well as private sector players from multiple critical infrastructure sectors. These types of exercises enable DHS to maintain and strengthen cross-sector, inter-governmental and international relationships, enhance processes and communications linkages, and ensure continued improvement to cyber security procedures and processes. Exercises also promote information sharing among participants and build relationships for future collaboration.

In addition, CS&C will:

- Increase manpower for 24/7 US-CERT Operations Center to provide the capability for in-depth incident tracking, detection, and mitigation.
- Continue to respond with a coordinated national system to major cyber and communications disruptions to restore essential communications.
- Continue to establish an integrated joint operations center comprised of public and private sector members consisting of IT and communications organizations.
- Continue to work with international partnerships to enable security partners to work together to promote secure, resilient IT and communications infrastructure.
- Continue to identify, assess, and prioritize risks to the IT and Communications infrastructure by analyzing threat, vulnerability, and consequence information.
- Continue to expand the National Vulnerability Database (NVD) to help establish a national baseline of specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).

GAO High-Risk Area - Implementing and Transforming the Department of Homeland Security

Summary of High-Risk Identification: GAO designated implementing and transforming DHS as high-risk in 2003 because DHS had to transform and integrate 22 agencies – several with existing program and management challenges – into one department, and failure to effectively address its challenges could have serious consequences for homeland security.

Managing the transformation of an organization of the size and complexity of DHS requires comprehensive planning and integration of key management functions that will likely span a number of years. DHS has made progress in these areas but additional work is required to ensure sustainable success (GAO-07-833T).

2007 Accomplishments

- Outlined and monitored financial material weakness corrective actions and built internal control management assertions in the Internal Control Over Financial Reporting (ICOFR) Playbook.
- Increased IT system availability and disaster recovery capability with 24/7 operational support and infrastructure security in preparation for national incidents or disasters by initiating the migration of legacy data centers to two DHS Data Centers.
- Implemented a strategy to enhance information sharing by improving workflow, document management, and business processes to increase user satisfaction by 40 percent, decrease cost by 15 percent, and reduce production time by 25 percent.
- Improved interoperable facility and system access for employees by issuing a single, secure, tamper-proof smartcard; the first card was issued prior to the October 27, 2006 deadline.
- Increased procurement operational and strategic sourcing effectiveness by implementing a central DHS-wide Program Management Support Office.

- Implemented a strategy to improve the hiring and retention of talent needed to achieve DHS's mission by focusing on five key priorities in the FY 2007-2008 Human Capital Operational Plan.
- Improved leadership preparation by developing and implementing a Department-wide senior executive service development program.
- Streamlined training delivery and opportunities for employees through a new enterprise Learning Management System (currently available to DHS Headquarters, Transportation Security Agency (TSA), and other Component employees).
- Designed a consolidated DHS Headquarters facility that will co-locate disparate national capital regional offices. The design completes phase one of the consolidation plan.

Remaining Plans

- Review alignment of department programs and projects to updated mission goals and work to improve consistent and transparent method to measure the *status* and *progress* of defined performance expectations for projects and programs.
- Develop action plans to correct and monitor internal control weaknesses and compliance using GAO guidance such as "*Standards for Internal Control in the Federal Government*."
- Improve performance measures with the assistance of department-wide program analyst and evaluation teams.
- Issue Integrated Planning Guidance informed by threat and vulnerability assessments for budget planning cycles.
- Create technology initiatives that provide real-time connectivity between forward incident commanders and Joint Field Office communication platforms.
- Ensure more effective procurement practices across Department contracting offices through strategic sourcing and supplier management.

GAO High-Risk Area – Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security

Summary of High-Risk Identification: As stated in the 2007 GAO high-risk report update, the Federal Government still faces formidable challenges in analyzing and disseminating key information among Federal, State, local, and private partners in a timely, accurate, and useful manner. Since September 11, 2001, multiple Federal agencies have been assigned key roles for improving the sharing of information critical to homeland protection to address a major vulnerability exposed by the attacks, and this important function has received increasing attention. However, the underlying conditions that led to the designation continue and more needs to be done to address these problems and the obstacles that hinder information sharing.

The Federal Government still has not implemented the government-wide policies and processes that the 9/11 Commission recommended and that Congress mandated. Completing the information sharing environment is a complex task that will take multiple years and long-term administration and congressional support and oversight, and will pose cultural, operational, and technical challenges that will require a collaborated response.

Federal agencies are also focusing on improving sharing with States, localities, and the private sector - a critical step since they are our first line of defense against terrorists - but these efforts are not without challenges. DHS has implemented a program to protect sensitive information the private sector provides on security at critical infrastructure assets, such as nuclear and chemical facilities. However, users of the information network were confused and frustrated with the system and as a result do not use it regularly; and DHS has still not won all of the private sector's trust that the agency can adequately protect and effectively use the information that sector provides. These challenges will require longer-term actions to resolve.

However, the Department notes that implementation and initial manning of DHS's State and Local Fusion Centers (SLFC) over the last year has gone a long way toward improving the information sharing nexus between DHS and its partners. DHS's primary partners are State and local governments (including tribal and territorial) and the private sector. These entities collect information outside the boundaries of the Intelligence Community (IC). Simultaneously, they have information needs not always recognized by the traditional IC agencies. DHS was created, in part, to bridge this gap and develop fusion at the *national*, vice *federal*, level.

To meet their own all-threats, all-hazards information needs many states and larger cities have created fusion centers. Fusion centers represent the logical touch-points for DHS to harvest local information and to provide them with timely relevant information and intelligence derived from all sources and analysis.

The DHS support effort provides ***people and tools*** to the SLFCs to create a web of interconnected information nodes across the country that will ensure information is gathered from all relevant operations and is fused with information from the Homeland Security Stakeholder Community to enable SLFCs and DHS to produce accurate, timely, and actionable intelligence products and services in support of homeland security.

On June 7, 2006, the Office of Intelligence & Analysis (I&A) was designated as the Executive Agent to manage the DHS State and Local Fusion Center program. It has been codified by PL 110-53, the law implementing the recommendations of the 9/11 Commission. This law requires that DHS take a stronger, more constructive role to assist SLFCs.

The SLFC Program is a major initiative to engage all players, at all levels of government, in confronting threats to the Homeland. It is a key element of DHS' strategy to exchange information with State and local authorities. Our goal is to create analytic centers of excellence nationwide to develop and exchange information with the Federal Government.

2007 Accomplishments

- The Secretary of Homeland Security issued a DHS-wide policy on information sharing, *DHS Policy for Internal Information Exchange and Sharing,* which provides guidance for all departmental information sharing activities. To supplement this memorandum, additional policy guidance and an Information Sharing and Access Agreement (ISAA) Guidebook are being developed to assist Components in creating information sharing agreements.
- DHS has established and is operating a three-tiered governance structure for information sharing. At the executive level, the Information Sharing Governance Board (ISGB) meets quarterly to decide department-wide information sharing issues. At the management level,

the Information Sharing Coordinating Council, comprised of representatives from all DHS Components and offices, meets semi-monthly to bring information sharing issues to the table and to formulate recommendations for the ISGB. At the execution level, the Shared Mission Communities and Integrated Project Teams meet regularly to develop solutions for information sharing issues.

- Through the governance structure, a Law Enforcement SMC was established, which represents the first time that DHS law enforcement components have come together to discuss their mutual needs for information sharing. The LE-SMC is in the process of finalizing a DHS Law Enforcement Information Sharing Strategy.
- In response to direction from the ISGB, DHS is finalizing a department-wide Concept of Operations (CONOPS) for how components of the Department will interact with State and local fusion centers to ensure consistency and continuity.
- DHS created a department-wide metric for information sharing as part of the Department's Performance Plan that will examine compliance against the DHS policy on information sharing.
- The Secretary added a goal on information sharing to the Secretarial Priorities. The Department will measure its progress against this goal on a monthly basis.
- Last year Intelligence & Analysis (I&A) started the State and Local Fusion Program to deploy intelligence officers to fusion centers. I&A is deploying people and tools to build a national fusion center network.
- Recognition of I&A's efforts by Congress in the 9/11 Implementation law will help I&A build and sustain the Program.
  - Currently I&A has 19 intelligence officers deployed nationwide.
  - The Secretary has committed to 35 deployed officers by the end of FY 2008.
- Homeland Secure Data Network (HSDN), DHS's SECRET-level data network, is in 18 centers and will be doubled by the end of FY 2008.
  - I&A is building an analytic training program – equivalent to what it has for its own officers – for the state and local analysts in fusion centers.
  - Privacy and civil rights training is being developed and will be delivered as well.
- I&A's officers in the fusion centers help to develop the human network that creates true information sharing across the country. They are the link to I&A, DHS, and the Intelligence Community from our State and local partners.
- I&A is focused on supporting the SLFCs as the centers of gravity in each state. I&A:
  - provides the national threat perspective, warning information, and responses to requests to information,
  - writes products for, and with, state and local customers,
  - collaborates in researching topics with subject matter experts in SLFCs,
  - hosts analytic exchange conferences,
  - provides daily intelligence support,
  - posts and disseminates raw and finished intelligence products on HSIN State and Local unclassified portal and HSDN (classified network), and
  - supports development of Homeland Intelligence Reports (HIRs) from state- and local-origin information to provide to the Intelligence Community.
- Current Department of Defense (DoD) policy prevents us from giving access to the intelligence on SIPRNET via HSDN to our State and local partners. We have been working with DoD for the past year to change that policy and ensure that our investment in providing

HSDN access to State and locals will be as fruitful as possible, so that we can live up to our "responsibility to provide" federal information to these partners.

Remaining Plans

- In the area of SLFCs, the key to harvesting the value from them is in tailoring DHS's support offering to meet their specific needs. This process begins with an assessment of the SLFC by a team of staff officers. The result is a set of recommendations on staffing and services that will deliver value to both DHS and the Fusion Center. Assessments have been conducted at 27 Fusion Centers across the country. Assessments will be done at more centers in FY 2008.
- Based on the results of the SLFC assessments and other factors, DHS has deployed intelligence officers to State Fusion Centers in Maryland, Georgia, Louisiana, Arizona, New York, Virginia, Illinois, Florida, California, Ohio, New Jersey, Massachusetts, Connecticut, and Washington State as well as to major city or regional centers in New York City, Los Angeles, and Dallas. The intent is to deploy officers to several more locations this year. As resources permit, DHS plans to have officers in as many as 35 sites by the end of fiscal year 2008.
- All SLFCs will soon have access to the HSDN, a SECRET collateral capability. Every SLFC will have an HSDN webpage to post State- and local-origin products making them available to other SLFCs and the Intelligence Community. These systems will create the information sharing environment necessary to enable information flow among the DHS intelligence and operational communities and the States.

GAO High-Risk Area – National Flood Insurance

Summary of High-Risk Identification – GAO placed the National Flood Insurance Program (NFIP) on its high-risk list in March 2006 because the NFIP will unlikely generate sufficient revenues to repay the billions borrowed from the Department of the Treasury to cover flood claims from the 2005 hurricanes. And it is unlikely that NFIP—a key component of the Federal Government's efforts to minimize the damage and financial impact of floods—could cover catastrophic losses in future years. Estimated claims for Hurricanes Katrina, Rita, and Wilma far surpass the total claims paid in the 38-year history of the NFIP. The insufficient revenues highlight structural weaknesses in how the program is funded.

The NFIP, by design, is not actuarially sound. Total collected premiums will unlikely be sufficient to pay all expected flood losses over time. In addition, the program is not structured to build loss reserves like a typical commercial insurance company, and it does not build and hold capital. Instead, it generally pays claims and expenses out of current premium income. When it has insufficient income to pay claims, the NFIP has authority to borrow from Treasury. It is highly unlikely that the NFIP, as currently funded, could generate revenues to repay Treasury, particularly if future hurricanes result in loss levels greater than the average historical loss levels.

2007 Accomplishments

- Improved NFIP delivery by: (a) distributing the *NFIP Summary of Coverage* and the *Flood Insurance Claims Handbook* to policyholders; (b) issuing informative supplemental policy coverage forms with new and renewed flood insurance policies; (c) providing Acknowledgement Forms to flood insurance policy purchasers; (d) implementing important agent-training initiatives, (e) adopting a flood insurance claims appeals rule, and (f) carrying out initiatives that address repetitive loss properties.

- In FYs 2006 and 2007, FEMA transferred $40 million from the National Flood Insurance Fund to mitigate severe repetitive loss properties. The FY 2008 President's Budget requested an additional $80 million for SRL.
- The Severe Repetitive Loss (SRL) Interim Rule was published on October 31, 2007 at 72 FR 61720. After the regulations go into effect on December 3, 2007, FEMA will provide guidance to potential applicants, and will begin awarding funds.
- Greatly increased the number of agents who are trained to sell flood insurance.
- The Repetitive Flood Claims Program distributed a total of $19.8 million in FY 2006 and 2007 to help communities remove more than 80 buildings from floodplains.
- The Flood Mitigation Assistance Program committed $31 million to States for various floodplain management projects and plans. These programs, combined with flood insurance and other mitigation activities are important elements of a systematic effort to eliminate the flood-rebuild-flood scenario.
- Through the delivery of the Floodplain Management programs in FY 2007 and FY 2008, FEMA continues to lead a national effort to:
    - Identify and improve the understanding of communities' flood hazards and their risks by providing flood hazard maps.
    - Develop and improve techniques and planning processes which mitigate those flood risks.
    - Provide technical assistance and an environment at the State and local levels that is conducive to applying those techniques and processes.
    - Provide financial assistance to states to support State NFIP implementation and compliance activities.
    - Support development of incentives and disincentives that make application of those techniques and processes a social, political, and/or economic priority.

<u>Remaining Plans</u>

- Issue SRL program implementation plans and guidance in December 2007, and solicit and award grant applications. This initial implementation year will include FY 2006, 2007 and 2008 funding.
- FEMA will continue efforts to streamline the grant award process for all hazard mitigation assistance program grants, including Flood Mitigation Assistance (FMA), SRL and Repetitive Flood Claims (RFC). Guidance will be issued early in the fiscal year so as to open and close the application period earlier. In FY 2008, FEMA expects to expand the mitigation options available under the RFC program to include property acquisitions, elevations, dry flood-proofing and minor localized flood control projects to achieve the greatest savings to the fund in the shortest time. In FY 2008, approximately 15 awards to communities for 35 to 40 properties are expected. Efforts to engage partners and coordinate implementation of the FMA and RFC programs with the expanded SRL program will be continued.

Appendix: Glossary of Acronyms and Abbreviations

The ***Appendix*** contains a glossary of acronyms and abbreviations.

Appendix: Glossary of Acronyms and Abbreviations

AA – Alternatives Analysis
ACE – Automated Commercial Environment
ADASP – Aviation Direct Access Screening Program
ADD – Automated Deployment Database
ADVISE – Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement
AFG – Assistance to Firefighters Grants
AFR – Annual Financial Report
AMSC – Area Maritime Security Committee
AMSP – Area Maritime Security Plan
AOR – Area of Responsibility
APIS – Advance Passenger Information System
APL – Acquisition Policy & Legislation
APR – Annual Performance Report
ARC – American Red Cross
ASAP – Aviation Screening Assessment Program
ASGB – Acquisition Systems Governance Board
ASI – Aviation Security Inspectors
ATO – Authority to Operate
ATS – Automated Targeting System
ATSA – Aviation and Transportation Security Act
BAO – Bomb Appraisal Officer
BDO – Behavior Detection Officer
BPD – Bureau of Public Debt
B&SA – Bureau & Statistical Agent
BZPP – Buffer Zone Protection Plan
C4ISR – Command, Control, Communications, Computers, Intelligence, and Reconnaissance
C4IT – Command, Control, Communications, Computers, and Information Technology
C&A – Certification and Accreditation
CAO – Chief of Administrative Services
CBJ – Congressional Budget Justification
CBP – Customs and Border Protection
CDC – Certain Dangerous Cargo
CDL – Community Disaster Loan
CDSOA – Continued Dumping & Subsidy Offset Account
CERTS – Cargo Enforcement Reporting and Tracking System
CFO – Chief Financial Officer

C.F.R. – Code of Federal Regulations
CIA – Central Intelligence Agency
CIIN – Critical Infrastructure Information Notices
CI-KR – Critical Infrastructure and Key Resources
CIO – Chief Information Officer
CIS – Community Information System
CISO – Chief Information Security Officer
COBRA – Consolidated Omnibus Budget Reconciliation Act
COE – U.S. Army Corps of Engineers
CONOPS – Concept of Operations
COP – Common Operating Picture
COTR – Contracting Officer Technical Representative
COTS – Commercial Off-the-Shelf Software
CPIC – Capital Planning Investment Control
CS&C – Cyber Security and Communications
CSI – Container Security Initiative
CSRS – Civil Service Retirement System
C-TPAT – Customs-Trade Partnership Against Terrorism
CY – Current Year
DADLP – Disaster Assistance Direct Loan Program
DAU – Defense Acquisition University's
DAWIA – Defense Acquisition Workforce Improvement Act
DCIA – Debt Collection Improvement Act
DCMA – Defense Contract Management Agency
DHS – Department of Homeland Security
DM – Disaster Management
DNDO – Domestic Nuclear Detection Office
DOC – Department of Commerce
DOD – Department of Defense
DOE – Department of Energy
DOI – Department of Interior
DOJ – Department of Justice
DOL – Department of Labor
DOS – Department of State
DRF – Disaster Relief Fund
DRO – Detention and Removal Operations
EA – Enterprise Architecture
EA – Environmental Assessment
EASI – Enterprise Acquisition System Initiative
EFS – Electronic Fingerprint System

EHC – Especially Hazardous Cargo
EMIMS – Emergency Management Information Management System
EMS – Executive Management System
EPI – Enterprise PRISM Instance
ER – Expedited Removal
ESC – Executive Steering Committee
ESRI – Environmental Systems Research Institute
EVM – Earned Value Management
FAA – Financial Accountability Act
FAMS – Federal Air Marshal Service
FAR – Federal Acquisition Regulation
FASAB – Federal Accounting Standards Advisory Board
FBI – Federal Bureau of Investigation
FBwT – Fund Balance with Treasury
FCRA – Federal Credit Reform Act of 1990
FECA – Federal Employees Compensation Act
FEGLI – Federal Employees Group Life Insurance Program
FEHB – Federal Employees Health Benefits Program
FEMA – Federal Emergency Management Agency
FFMIA – Federal Financial Management Improvement Act
FERS – Federal Employees Retirement System
FIN – Federal Information Notice
FIRA – Flood Insurance Reform Act
FISCAM – Federal Information System Controls Audit Manual
FISMA – Federal Information Security Management Act
FLETC – Federal Law Enforcement Training Center
FMA – Flood Mitigation Assistance
FMFIA – Federal Managers' Financial Integrity Act
FOC – Full Operating Capability
FPDS – Federal Procurement Data System
FPDS-NG – Federal Procurement Data System-Next Generation
FPS – Federal Protective Service
FSD – Federal Security Director
FSIO – Financial Systems Integration Office
FY – Fiscal Year
FYHSP – Future Years Homeland Security Program
GAAP – Generally Accepted Accounting Principles
GAO – Government Accountability Office
GIS – Geographic Information System
GMS – Grants Management Specialist

GOTS – Government Off-the-Shelf
GPEA – Government Paper Elimination Act
GPRA – Government Performance and Results Act
GSA – General Services Administration
G&T – Grants and Training
HHS – Department of Health and Human Services
HQ – Headquarters
HSA – Homeland Security Act
HSAM – Homeland Security Acquisition Manual
HSAR – Homeland Security Acquisition Regulation
HSDN – Homeland Secure Data Network
HSGP – Homeland Security Grant Program
HSIN Homeland Security Information Network
HUD – Department of Housing and Urban Development
IAA – Interagency Acquisition
I&A – Intelligence and Analysis
iCAV – Infrastructure Critical Asset Viewer
ICCB – Internal Control Coordination Board
ICE – U.S. Immigration and Customs Enforcement
ICOFR – Internal Controls Over Financial Reporting
IDI – Injured Domestic Industries
IDS – Integrated Deepwater System
IEFA – Immigration Examination Fee Account
IFMIS – Integrated Financial Management Information System
IHP – Individuals and Households Program
IHS – Internet Health System
INA – Immigration and Nationality Act
IP – Improper Payment
IPA – Independent Public Accountant
IPIA – Improper Payments Information Act
IPP – Infrastructure Protection Program
IPT – Integrated Product Teams
ISAA – Information Sharing and Access Agreement
ISAC – Information and Analysis Center
ISCC – Information Sharing Coordinating Council
ISDC – Interagency Suspension and Debarment Committee
ISGB – Information Sharing Governance Board
ISIS – Integrated Surveillance Intelligence System
ISSO – Information System Security Officer
IT – Information Technology

ITSD – Information Technology Services Division
IWN – Integrated Wireless Network
JPO – Joint Program Office
LAN – Local Area Network
LIMS – Logistics Inventory Management System
MAST - Mitigation Advisors Statistical Tracker
MD&A – Management's Discussion and Analysis
MGMT – Management Directorate
MDP – Milestone Decision Point
MFPU – Maritime Force Protection Unit
MOA – Memorandum of Agreement
MOU – Memorandum of Understanding
MRS – Military Retirement System
MSAM – Major Systems Acquisition Manual
MSRAM – Maritime Security Risk Analysis Model
MTS – Marine Transportation System
MTS – Metric Tracking System
NADB – National Asset Database
NAVICP – Navy Inventory Control Point
NBIS – National Bio-Surveillance Integration System
NCA – National Capital Area
NCAS – National Cyber Alert System
NCCIPS – National Center for Critical Information Processing and Storage
NCSD – National Cyber Security Division
NDMS – National Disaster Medical Systems
NEMIS – National Emergency Management Information System
NFIP – National Flood Insurance Program
NGA – National Geospatial-Intelligence Agency
NICC – National Infrastructure Coordination Center
NIMS – National Incident Management System
NIPP – National Infrastructure Protection Plan
NIST – National Institute of Standards and Technology
NMSRA – National Maritime Strategic Risk Assessment
NMSZ – New Madrid Seismic Zone
NOC – National Operations Center
NPPD – National Protection and Programs Directorate
NRCC – National Response Coordination Center
NRF – National Response Framework
NRP – National Response Plan
NSA – National Security Agency

NSVSS – National Small Vessel Security Summit
NVD – National Vulnerability Database
OASISS – Operation Against Smugglers Initiative for Safety and Security
OCPO – Office of the Chief Procurement Officer
OEC – Office of Emergency Communications
OFPP – Office of Federal Procurement Policy
OHA – Office of Health Affairs
OHC – Office of Human Capital
OI&A – Office of Intelligence and Analysis
OIG – Office of Inspector General
OJS – Operation Jump Start
O&M – Operations and Management
OMB – Office of Management and Budget
OM&S – Operating Supplies and Materials
OPEB – Other Post Employment Benefits
OPM – Office of Personnel Management
OPO – Office of Procurement Operations
ORB – Other Retirement Benefits
OSEM – Office of the Secretary Executive Management
OTM – Other than Mexican
PA&E – Performance Analysis and Evaluation
PAR – Performance and Accountability Report
PART – Program Assessment Rating Tool
PASS – People Access Security Service
PBA – Performance-Based Acquisition
PCIS – Partnership for Critical Infrastructure Security
PII – Personally Identifiable Information
PKEMR – Post Katrina Emergency Management Reform Act
PL – Public Law
PM – Program Manager
PMA – President's Management Agenda
POA&M – Plans of Action and Milestones
PPBE – Planning, Programming, Budgeting, and Execution
PP&E – Property, Plant, and Equipment
PREP – Preparedness Directorate
PRM – Performance Reference Model
PWCS – Ports, Waterways, and Coastal Security
PY – Prior Year
QASP – Quality Assurance Surveillance Plan
RAP – Resource Allocation Plan

REPP – Radiological Emergency Preparedness Program
RFC – Repetitive Flood Claim
RND – Results Not Demonstrated
RSSI – Required Supplementary Stewardship Information
SAFETEA-LU – Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users
SAP – Systems Applications Products
SAT – Senior Assessment Team
SBA – Small Business Administration
SBI – Secure Border Initiative
SBInet – Secure Border Initiative Network
SCIP – Statewide Communications Interoperability Plan
SCNP – Statement of Changes in Net Position
SCSS – Supply Chain Security Specialists
SDLC – System Development Life Cycle
SES – Senior Executive Service
SFFAS – Statements of Federal Financial Accounting Standards
SFI – Secure Freight Initiative
SFRBTF – Sport Fish Restoration and Boating Trust Fund
SIPRNet – Secret Internet Protocol Router Network
SLFC – State and Local Fusion Centers
SMC – Senior Management Council
SME – Subject Matter Expert
SOC – Security Operations Center
SOP – Standard Operating Procedure
SRL – Severe Repetitive Loss
SRM – Stakeholder Relationship Management
SSP – Strategic Sourcing Program
S&T – Science and Technology
ST&E – System Tests and Evaluations
TAI – TSA Approved Instructor
TASC – Transformation and Systems Consolidation
TAV – Total Asset Visibility
TDL – Test Development Laboratory
TFS – Treasury Fund Symbol
T&M – Time and Material
TOD – Test of Design
TOE – Test of Operating Effectiveness
TPO – Transformation Program Office
TRM – Technology Reference Model

TSA – Transportation Security Administration
TSI – Transportation Security Inspector
TSO – Transportation Security Officer
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
USGS – U.S. Geological Survey
USPS – U.S. Postal Service
USSGL – United States Standard General Ledger
USSS – U.S. Secret Service
US-VISIT – U.S. Visitor and Immigrant Status Indicator Technology
UTPP – Underwater Terrorism Preparedness Plan
VA – Vulnerability Assessment
VIPR – Visible Intermodal Protection and Response
VoIP – Voice over Internet Protocol
VTC – Video Teleconference
WHTI – Western Hemisphere Travel Initiative
WYO – Write Your Own

This report satisfies the reporting requirements of the following laws:

- Federal Managers' Financial Integrity Act of 1982
- Government Performance and Results Act of 1993
- Government Management Reform Act of 1994
- Clinger-Cohen Act of 1996
- Reports Consolidation Act of 2000
- Federal Information Security Management Act of 2002
- Chief Financial Officer Act of 1990
- Department of Homeland Security Financial Accountability Act of 2004

This report was compiled and submitted in accordance with:

- Accountability of Tax Dollars Act of 2002 Office of Management and Budget (OMB) Circular A–11 Preparation, Submission, and Execution of the Budget
- OMB Circular A–136 Financial Reporting Requirements

Homeland
Security