Other Accompanying Information

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

Tax Burden/Tax Gap

Revenue Gap

The Entry Summary Compliance Measurement (ESCM) program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations, and agreements, and is used to produce a dollar amount for Estimated Net Undercollections and a percent of Revenue Gap. The Revenue Gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and trade agreements using a statistically valid sample of the revenue losses and overpayments detected during ESCM entry summary reviews conducted throughout the year. For FY 2007 and 2008, the Estimated Net Undercollections were $412 and $396 million, respectively. CBP calculated the preliminary FY 2009 Estimated Net Undercollections to be $250 million. As a percentage, the preliminary Revenue Gap for FY 2009 represents less than 1 percent of all collectable revenue for the year, the lowest it has been in over five years. The estimated over collection and under collection amounts due to noncompliance for FY 2009 were $40 million and $290 million, respectively. The overall trade compliance rate for FY 2007 and FY 2008 is 97.8 and 97.6 percent, respectively. The preliminary overall compliance rate for FY 2009 is 98.5 percent.

The final overall trade compliance rate and estimated revenue gap for FY 2009 will be issued in February 2010.

Summary of Financial Statement Audit and Management Assurances

Table 1 and Table 2 below provide a summary of the financial statement audit and management assurances for FY 2009.

Table 1. FY 2009 Summary of the Financial Statement Audit

Audit Opinion	Disclaimer				
Restatement	Yes				
Material Weakness	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
Financial Management and Reporting	1				1
IT Controls and System Functionality	1				1
Fund Balance with Treasury	1				1
Property, Plant, & Equipment and Operating Materials & Supplies	1				1
Actuarial and Other Liabilities	1				1
Budgetary Accounting	1				1
Total Material Weaknesses	**6**	**0**	**0**	**0**	**6**

In FY 2009, the Independent Auditor implemented the Department's first ever integrated financial statement and internal control audit, resulting in six material weakness conditions at the Department level. In addition, standalone financial statement audits were expanded to five DHS Components, including: CBP, USCIS, FLETC, ICE, and TSA. Portions of prior year material weakness conditions were resolved or reduced in severity; however, new conditions were identified causing material weaknesses to repeat at the consolidated level. For example, FEMA resolved control deficiencies in Property, Plant, and Equipment (PP&E) and Operating Materials and Supplies, but TSA's control deficiencies in PP&E repeated and new deficiencies were identified at CBP. FEMA implemented corrective actions to reduced portions of the prior year Budgetary Accounting deficiencies. TSA implemented corrective actions to reduce the severity of the prior year Financial System Security deficiency condition; however, new deficiencies were identified in ICE's IT Controls and System Functionality. Finally, FLETC, ICE, and S&T corrected deficiencies which contributed to the Department's Actuarial and Other Liabilities material weakness condition.

Table 2. FY 2009 Summary of Management Assurances

Effectiveness of Internal Control Over Financial Reporting (FMFIA Section 2)						
Statement of Assurance	No Assurance					
Material Weaknesses	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Financial Reporting	1					1
Fund Balances with Treasury	1					1
Financial Systems Security	1					1
Budgetary Resource Management	1					1
Property Management	1					1
Human Resource Management	1					1
Total Material Weaknesses	**6**	**0**	**0**	**0**	**0**	**6**
Effectiveness of Internal Controls over Operations (FMFIA Section 2)						
Statement of Assurance	Qualified					
Material Weaknesses	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Entity Level Controls at FEMA	1					1
Improper Payments Information Act at FEMA	1				✓	0
Assistance Awards Policy and Oversight	1					1
Funds Control at U.S. Coast Guard and ICE	1					1
Controls Over Collection, Depositing of Fees, and Quality Assurance at USCIS	1				✓	0
Federal Protective Service Operations at ICE	1				✓	0
Property Management	1					1
Acquisition Management	1					1
Human Capital Management	1				✓	0
Business Continuity and US-VISIT System Security at CBP	1					1
Total Material Weaknesses	**10**	**0**	**0**	**0**	**(4)**	**6**
Conformance with financial management systems requirements (FMFIA Section 4)						
Statement of Assurance	Systems do not conform to financial management systems requirements					
Non-Conformances	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Federal Financial Management Systems Requirements, including Financial Systems Security and Integrated Financial Management Systems	1					1
Noncompliance with the U.S. Standard General Ledger	1					1
Federal Accounting Standards	1					1
Total Non-conformances	**3**	**0**	**0**	**0**	**0**	**3**
Compliance with Federal Financial Management Improvement Act (FFMIA)			DHS		Auditor	
Overall Susbstantial 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 DHS FAA, 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, between FY 2005 and FY 2009, DHS reduced the number of conditions that comprise the Department's material weakness structure by more than half. In addition, in FY 2009, the Department completed a limited scope evaluation of processes that provide internal control over the Balance Sheet and Statement of Custodial Activity.

The Secretary reported six material weakness conditions at the Department level in FY 2009 and concurred with the material weakness conditions reported by independent audit. Differences between condition titles reported by DHS Management and the Independent Public Auditor (IPA) are 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). The FSIO process definitions used by management aid corrective actions and facilitate development of standard controls and business processes.

Significant internal control challenges remain at U.S. Coast Guard, FEMA, TSA, CBP, and ICE. To support these Components, the Department's Chief Financial Officer will conduct weekly working group meetings with Senior Management and Staff. Table 3 summarizes material weaknesses in internal controls as well as planned corrective actions with estimated target correction dates.

Table 3. FY 2009 Internal Control Over Financial Reporting Corrective Actions

Material Weaknesses in Internal Controls Over Financial Reporting	Year Identified	DHS Component	Corrective Actions	Target Correction Date
Financial Management and Reporting: U.S. Coast Guard, TSA, and FEMA have not established an effective financial reporting process due to limited staffing resources, informal policies and procedures, and lack of integrated financial processes and systems.	FY 2003	U.S. Coast Guard, TSA, and FEMA	The DHS OCFO will continue efforts to support U.S. Coast Guard, TSA, and FEMA in implementing corrective actions to develop policies/procedures and to establish effective financial reporting control activities. In addition, a comprehensive risk assessment will be conducted by the DHS OCFO to ensure new significant deficiency conditions are contained.	FY 2012
IT Controls and System Functionality: The Department's Independent Public Auditor had identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to inherited control deficiencies surrounding general computer and application controls. The *Federal Information Security Management Act* mandates that Federal Agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance.	FY 2003	U.S. Coast Guard, FEMA, and ICE	TSA reduced the severity of prior year system security findings to a reportable condition and will continue efforts to implement corrective actions related to activity financial statement risks. Additional financial audit support for U.S. Coast Guard, FEMA, and ICE will be provided from the Offices of the Chief Financial Officer and the Chief Information Security Officer in order to design and implement internal controls in accordance with *DHS 4300A Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Financial Systems.*	FY 2012
Fund Balance with Treasury: U.S. Coast Guard did not implement effective internal controls to accurately clear suspense transactions in order to perform accurate and timely reconciliations of Fund Balance with Treasury accounts.	FY 2004	U.S. Coast Guard	U.S. Coast Guard will continue efforts to develop short-term compensating controls to reconcile significant payroll classes of transactions, while longer-term corrective actions are implemented to sustain Fund Balance with Treasury reconciliations.	FY 2012
Property, Plant, and Equipment and Operating Materials and Supplies: The controls and related processes surrounding U.S. Coast Guard Property, Plant, and Equipment (PPE) and Operating Materials and Supplies (OMS) to accurately and consistently record activity are either not in place or contain errors and omissions. New conditions related to CBP SBINet Capitalization were identified in FY 2009. TSA conditions include capitalization of internal use software, idle property, and other direct costs.	FY 2003	U.S. Coast Guard, TSA, and CBP	FEMA and TSA made progress towards implementing policies and procedures to identify and account for software capitalization in accordance with Statement of Federal Financial Accounting Standard (SFFAS) No. 10, *Accounting for Internal Use Software* . U.S. Coast Guard will implement policies and procedures to support completeness, existence, and valuation assertions for PPE and OMS. In addition, acquisition, construction, improvement, and construction in progress controls will be implemented to properly capitalize PPE. The DHS OCFO will continue efforts to support U.S. Coast Guard, TSA, and CBP in implementing corrective actions to address capital asset and supplies conditions and will address staffing shortfalls and develop policies and procedures to establish effective financial reporting control activities. In addition, a comprehensive risk assessment will be conducted by the DHS OCFO to ensure new conditions are contained.	FY 2012
Actuarial and Other Liabilities: U.S. Coast Guard has not completely implemented policies and procedures to account for actuarial liabilities. In addition, internal control weaknesses exist in developing estimates for accounts payable and environmental liabilities at U.S. Coast Guard.	FY 2006	U.S. Coast Guard	Prior year significant deficiencies related to environmental liabilities at ICE, FLETC, and S&T, were corrected in FY 2009. U.S. Coast Guard made significant progress for actuarial liability processes associated with unfunded military retirement pay by improving data quality and establishing controls at servicing personnel offices. U.S. Coast Guard efforts in FY 2010 will focus on sustainment and implementing service provider controls with the Department of Defense.	FY 2011
Budgetary Accounting: Policies and procedures over obligations, disbursements, and validation and verification of undelivered orders for accurate recording of accounts payable were not effective.	FY 2004	U.S. Coast Guard	U.S. Coast Guard developed corrective actions to improve budgetary accounting. However, corrective actions may extend beyond FY 2011 due to resource constraints and magnitude of other corrective actions. FEMA reduced the severity of its portion of the prior year budgetary accounting related to undelivered orders to a significant deficiency.	FY 2012

Effectiveness of Internal Control Over Operations

The DHS Management Directorate is dedicated to ensuring that Departmental Offices and Components perform as an integrated and cohesive organization, focused on leading the national effort to secure America. Critical to this mission is a strong internal control structure. As we strengthen and unify DHS operations and management, we will continually assess and evaluate internal control to evaluate our progress in ensuring the effectiveness and efficiency of operations and compliance with laws and regulations. For the third consecutive year, we have made tremendous progress in strengthening Department-wide internal controls, as evidenced by the following FY 2009 achievements:

- Established mechanisms to provide governance and oversight of *American Recovery and Reinvestment Act* projects to ensure competitive opportunities are maximized and funds are obligated timely to contribute to the Administration's economic recovery objectives.
- Achieved consensus with the U.S. Government Accountability Office (GAO) with regard to DHS/GAO protocols; as a result, the Department is poised to establish an audit follow-up process to improve the efficiency and effectiveness of operations.
- Issued the DHS Financial Management Policy Manual, designed to ensure DHS maintains efficient and transparent operations and our resources are not vulnerable to waste, fraud, and mismanagement.
- Published a comprehensive update of the DHS information security policy with a new corresponding 5 Year enterprise cybersecurity strategy. This policy addresses changes in executive/congressional guidance, new mission requirements, and new technology challenges.
- Successfully closed 5 of 24 legacy data centers on the migration list. There are currently 13 data center projects in execution and another 18 projects in active planning stage to achieve consolidation into two enterprise data centers.
- Conducted 30 Acquisition Review Boards (ARBs) chaired by either the Deputy Secretary, Under Secretary for Management or the Chief Procurement Officer to maximize the value of and manage risks to DHS acquisitions. In addition, we implemented Portfolio Reviews to complement the ARB process, support portfolio management, and strengthen Departmental governance and oversight.
- Initiated a Quarterly Operational Assessment to evaluate and measure specified metrics and program progress.
- Issued more than 10,500 HSPD-12 Personal Identity Verification access cards; developed a separate and distinct Consolidated Headquarters Security Division within the management structure of the Office of the Chief Security Officer; and received a favorable review from the Information Security Oversight Office (ISOO) on DHS Headquarters' classification management programs.
- Deployed the Integrated Security Management System (ISMS) within CBP and FLETC. The system tracks personnel security investigations, provides electronic adjudication management and file information sharing, and supports One DHS.
- Established a Field Security Coordinator (FSC) program consisting of a cadre of security professionals to ensure that classified national security information and sensitive but unclassified information shared with state, local, tribal and private sector (SLTPS) partners are appropriately safeguarded and protected. The Personnel Security Division changed Contractor Suitability Requirements that will result in increased timeliness.

- Expedited the filling of all Office of the Chief Administrative Officer (OCAO) vacant positions, completed a comprehensive assessment of staff development needs, and implemented a telework program to address quality of life and performance efficiencies to address identified conditions in property management and replace functional integration activities within the OCAO.
- In support of the HQ consolidation project: funds were received for both GSA and OCAO along with additional *American Recovery and Reinvestment Act* (ARRA) *of 2009* funding; a project team was stood up and staffed; the demolition process was started; a design build contract was awarded; and a project kick off ceremony was conducted.
- Reviewed and updated all USM policies and procedures to ensure they are current.
- Achieved great strides in strengthening and unifying human capital programs within the Department. Improved the favorable response rate by DHS employees on the annual employee survey by four percentage points; and, improved the attrition rate for career senior executive service personnel by 2.1 percent (from 11.0 percent in FY 2008 down to 8.9 percent in FY 2009).
- Deployed the Department's eRecruitment solution to DHS HQ and FEMA.
- Implemented an on-line HR Resource Center of HR policies, programs, and practices for use by HR professionals, supervisors, and employees.
- Conducted the Department's first-ever Veterans Job Fair.

To address challenges to internal control over operations, the Department's Under Secretary for Management conducts weekly Senior Management Council Oversight. Table 4 summarizes material weaknesses in internal control over operations as well as planned corrective actions with estimated target correction dates.

Table 4. FY 2009 Internal Control Over Operations Corrective Actions

Material Weaknesses in Internal Controls Over Operations	Year Identified	DHS Component	Corrective Actions	Target Correction Date
Property Management: Oversight and monitoring controls of the Department's investment in property, equipment, and other sensitive materials need to be strengthened.	FY 2008	DHS	The Department's Office of Chief Administrative Officer (OCAO) will establish an oversight capability in this area. In addition, OCAO plans to develop a program for reviewing current capabilities in inventory management and for determining whether internal capabilities are sufficient to meet consolidated needs. Finally, OCAO is developing a three-five-year strategic plan, with recommendations for significant staffing increases to address this specific oversight management material weakness, as well as other capability issues.	FY 2011
Assistance Awards Policy and Oversight: DHS has not defined the Assistance Award Line of Business. We have not promulgated formal policy for use by DHS Components and recipients of DHS grants and cooperative agreements in order to ensure an understanding of all statutory, regulatory and policy requirements that govern the use of Federal funds. DHS has not established the related strategy and annual plan for monitoring Component compliance with all legal requirements, including ensuring Component monitoring of recipients to ensure their compliance.	FY 2008	DHS	An SES Level Director was selected in FY 2009 to bolster efforts to establish Assistance Awards Policy and Oversight. In addition, Management, in consultation with the Office of the Inspector General, will develop an approach regarding resolution of findings arising from the annual audit of recipient uses of Federal funds.	FY 2011
Acquisition Management: The continued absence of a strategic requirements process potentially results in requirements gaps (inability to meet mission requirements) and redundancies (additional costs). This issue is currently being addressed via the Quadrennial Homeland Security Review (QHSR), but a formal institutionalized process is needed to flow down to the program level.	FY 2008	DHS	While progress has been recognized, broader implementation of Acquisition Directive 102-01 is needed to ensure Department-wide compliance. In FY09, 30 Acquisition Review Boards (ARBs) were conducted by either the Deputy Secretary or Under Secretary for Management. However, the principles of 102.01 need to implemented at the component level to review lower level programs. One key aspect of 102-01 is the designation of the Component Acquisition Executive (CAE) who is responsible for reviewing and approving lower level programs to proceed at periodic Acquisition Decision Events. To date, six CAEs have been designated. In FY10, the remaining CAEs need to be designated, and the OCPO will monitor compliance for the Level 2 and 3 programs. Finally, the Department needs to address its need to establish independent cost estimating as a competency across the Department. Without better cost estimating, the acquisition programs are vulnerable to cost overruns and budget shortfalls in the out years. In FY10, the Department plans to increase its number of cost estimators both at the Department and component levels.	FY 2011
Entity Level Controls at FEMA: FEMA has not completely implemented a process to provide assurance that FEMA internal controls are achieving the objectives of the Federal Financial Managers Financial Integrity Act.	FY 2007	FEMA	FEMA is establishing an Internal Control Board (ICB) to strengthen efforts to improve internal controls across FEMA. The ICB will demonstrate FEMA's commitment to increasing awareness and leadership sponsorship of internal control across FEMA programs.	FY 2011
Funds Control: USCG identified a material weakness within Anti-Deficiency Act (ADA) controls. In addition, ICE's Detention and Removal Program identified a condition related to the monitoring and oversight of the budget formulation and execution.	FY 2007	U.S. Coast Guard and ICE	U.S. Coast Guard is developing enterprise-wide polices and procedures for assessing ADA risks, testing effectiveness of controls and monitoring to fully implement DHS policy. ICE deployed an integrated financial management team to address critical process and internal control issues to resolve conditions in FY 2010.	FY 2010
System Security and Financial System Service Continuity: CBP has inadequate resources for business continuity testing of designated financial systems. In addition, GAO performed a review of US-VISIT systems and determined that CBP needed to immediately address significant security weaknesses in systems supporting core CBP systems.	FY 2008	CBP	CBP has implemented 61 of the 82 GAO audit recommendations; however, significant upgrades to the CBP infrastructure are needed.	FY 2011

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.

Financial Management Systems – Transformation and Systems Consolidation

The Transformation and Systems Consolidation (TASC) effort increases the transparency and reliability of DHS information by consolidating financial, asset and acquisition management systems and standardizing business processes. The implementation of TASC results in an integrated solution that continues to help move the Department towards increased fiscal accountability to the American taxpayer and opportunities to improve the efficiency of the Department's mission-critical services.

Current State: DHS maintains 13 disparate financial management systems resulting in multiple business processes and accounting lines. Mission support requires a real-time enterprise view of DHS resources, yet some systems rely heavily on manual processes and lack integration that may result in inaccurate and incomplete data. Many of the components across DHS are utilizing redundant systems with similar functionality. As a result, the cost for upgrades, integration, operations, maintenance, and mandated changes are unnecessarily replicated across the Department. DHS understands that its current manual financial management processes and stove-piped financial management systems are not sustainable over the long term.

Future State: The Transformation and Systems Consolidation effort focuses on increasing the transparency and reliability of information by consolidating financial, asset, and acquisition management systems and standardizing business processes. This effort will provide increased fiscal accountability to the American taxpayer as well as opportunities to improve the efficiency of our mission-critical services.

TASC Objectives:

- Eliminate financial, asset and acquisition management system redundancies;
- Standardize business processes and establish single accounting line structure;
- Avoid costs associated with inefficiencies;
- Create timely, accurate and comprehensive reporting capability that increases financial transparency;
- Reduce manual processes;
- Strengthen internal controls and correct Department-wide material weaknesses;

- Align with goals of Financial Management Line of Business (FMLoB); and,
- Centralize hosting, database integration, upgrades, and maintenance.

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 *2009 Federal Information Security Management Act (FISMA) Report and Privacy Management Report* consolidates reports from three DHS offices:

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

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, the OIG in FY 2009 identified progress the Department has made on the following seven key areas of DHS's information system security program:

- Information Systems Inventory;
- Certification and Accreditation;
- Plan of Action and Milestones;
- Configuration Management;
- Incident Detection, Handling and Analysis;
- Security Training; and
- Privacy.

The Department continues to improve and strengthen its security program. The OIG report, "Evaluation of DHS's Information Security Program for Fiscal Year 2009," identified six recommendations for information security improvements and two recommendations for privacy compliance. DHS plans to utilize the FY 2010 Information Security Performance Plan to enhance its security program, with enhanced metrics further improving compliance.

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, Section 831 of the FY 2002 *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." The 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.

I. Risk Assessments

In FY 2009, risk assessments were conducted on 95 DHS programs, totaling $46 billion in FY 2008 disbursements. Assessments were not conducted on programs with disbursements less than $10 million. Two FEMA Disaster Relief Programs, Individuals and Households Program (IHP) and Vendor Payments, were not risk-assessed as they were already determined to require sample testing based on prior year sample test results. All payment types were assessed except for Federal intra-governmental payments which were excluded after consultation and concurrence with the Office of Management and Budget and the Office of Inspector General.

The susceptibility of programs to significant improper payments was determined by qualitative and quantitative factors. These factors included:

- Payment Processing Controls – Management's implementation of internal controls over payment processes including existence of current documentation, the assessment of design and operating effectiveness of internal controls over payments, the identification of deficiencies related to payment processes and whether or not effective compensating controls are present, and the results of prior IPIA payment sample testing.
- Quality of Internal Monitoring Controls – Periodic internal program reviews to determine if payments are made properly. Strength of documentation requirements and standards to support test of design and operating effectiveness for key payment controls. Presence or absence of compensating controls.
- Human Capital – Experience, training, and size of payment staff. Ability of staff to handle peak payment requirements. Level of management oversight and monitoring against fraudulent activity.
- Complexity of Program – Time program has been operating. Complexity and variability of interpreting and applying laws, regulations, and standards required of the program.
- Nature of Payments and Recipients – Type, volume, and size of payments. Length of payment period. Quality of recipient financial infrastructure and procedures. Recipient experience with Federal award requirements.
- Operating Environment – Existence of factors which necessitate or allow for loosening of financial controls. Any known instances of fraud. Management's experience with designing and implementing compensating controls.

- Additional Grant programs factors – Federal Audit Clearinghouse information on quality of controls within grant recipients. Identification of deficiencies or history of improper payments within recipients. Type and size of program recipients and sub-recipients. Maturity of recipients' financial infrastructure, experience with administering Federal payments, number of vendors being paid, and number of layers of sub-grantees.

A weighted average of these qualitative factors was calculated. This figure was then weighted with the size of the payment population to calculate an overall risk score.

Based on this year's assessment process, the following programs were deemed to be vulnerable to significant improper payments:

Table 5. Programs at High-Risk for Improper Payments Based on FY 2009 Risk Assessments and Prior Year Payment Sample Testing

Component	Program Name	FY 2008 Disbursements ($ Millions)
CBP[1]	Custodial – Refund & Drawback	$1,245
CBP	Custodial – Continued Dumping & Subsidy Offset Act (CDSOA) & Payments to Wool Manufacturers	$293
FEMA	Disaster Relief Program – Individuals and Households Program (IHP)	$638
FEMA	Disaster Relief Program – Vendor Payments	$836
FEMA	Insurance – National Flood Insurance Program (NFIP)	$825
FEMA	Grants – Public Assistance Programs (PA)	$3,325
FEMA	Grants – Homeland Security Grant Program (HSGP)	$1,390
FEMA	Grants – Assistance to Firefighters Grants (AFG)	$582
ICE[2]	Detention and Removal Operations (DRO)	$1,202
ICE[2]	Investigations	$170
ICE[2]	Federal Protective Service (FPS)	$712
TSA	Aviation Security – Payroll	$2,876
U.S. Coast Guard	Active Duty Military Payroll (ADMP)	$2,715
U.S. Coast Guard	Contract Payments – Operating Expenses	$953
U.S. Coast Guard	Contract Payments – Acquisition, Construction & Improvements (AC&I)	$738
Total FY 2008 Disbursements		**$18,500**

Notes:
1. The FY 2008 payment population for the Refund & Drawback Program was $5.6 billion lower than the previous year due to the absence of softwood lumber refunds which were a single year event.
2. Only the non-payroll portion of ICE programs was found to be high-risk. Disbursement figures are for non-payroll disbursements.

II. Statistical Sampling Process

A stratified sampling design was used to test payments based on FY 2008 disbursement amounts and the assessed risk of the program. FEMA also completed an additional round of sample testing of two programs during times of greatest payment stress – responding to a catastrophic disaster. 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 five to ten percent of total payment dollars was used in the sample size calculation.

Using 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:

- Identify large payment dollars as the certainty stratum;
- Assign each payment a randomly generated number using a seed;
- Sort payments within each stratum (by ordered random numbers); and
- Select payments following the sample size design. For the certainty strata, all payments are selected.

To estimate improper payment dollars for the population from the sample data, the stratum specific ratio of improper dollars (gross, underpayments, and overpayments, separately) to total payment dollars was calculated.

DHS sample test results are listed in Table 6.

Table 6. DHS Sample Test Results

Component	Program	FY 2008 Payment Population ($millions)	FY 2008 Sample Size ($millions)	Est. Error Amount ($millions)	Est. Error Percentage (%)
CBP	Refund & Drawback	$1,245	$143	$11	0.91%
	Custodial – Continued Dumping & Subsidy Offset Act & Payments to Wool Manufacturers	$293	$228	$0	0.00%
FEMA	Assistance to Firefighters Grants	$505	$41	$23	4.63%
	Disaster Relief Program - Individuals and Households Program	$638	$2	$12	1.86%
	Disaster Relief Program - Vendor Payments	$836	$337	$74	8.82%
	Homeland Security Grant Program[1]	$157	$129	$24	18.75%
	National Flood Insurance Program	$819	$44	$52	6.38%
	Public Assistance Program[2]	$1,192	$146	$10	5.48%
ICE	Detention and Removal Operations[3]	$1,202	$235	$12	0.97%
	Federal Protective Service[3]	$712	$161	$0	0.01%
	Investigations[3]	$170	$44	$3	1.49%
TSA	Aviation Security - Payroll	$2,212	$1	$2	0.07%
U.S. Coast Guard	Operating Expenses - Active Duty Military Payroll	$2,715	$4	$13	0.46%
	Operating Expenses - Contracts	$953	$139	$0	0.00%
	Acquisition, Construction, and Improvements - Contracts	$738	$384	$0	0.00%
DHS	**All Programs**	**$14,387**	**$2,038**	**$236**	**1.64%**
DHS	**High-Risk Programs (Est. Error Amount >$10 Million)**	**$9,309**	**$1,081**	**$231**	**2.48%**

Notes:

1. Sample testing of the Homeland Security Grant Program was limited to the State of California which is the program's largest state recipient representing 11 percent of all FY 2008 payments made nationally. Data listed in the table above is for the State of California only and is not a national estimate.
2. Sample testing of the Public Assistance Program was limited to six states – Alabama, Kansas, Mississippi, Missouri, Nebraska, and North Carolina - in two stages of testing. Collectively, these states account for 36 percent of all FY 2008 payments made nationally. Data listed in the table above is for the states tested and is not a national estimate.
3. Non-payroll expenses only. Fleet and Purchase card transactions were excluded as testing for these payment types was performed under OMB Circular A-123, Appendix B rather than under OMB Circular A-123, Appendix C.

Several programs considered at high-risk based on risk assessment grading were not confirmed as at high-risk based on sample test results. The main reason for the estimated error rates falling below $10 million for these programs was the presence of strong compensating controls such as additional levels of payment review for manually intensive processes. The FY 2009 DHS IPIA Compliance Guidance was updated to reflect the need to consider compensating controls when evaluating programs. The testing for several programs has produced an estimated error amount below $10 million for two successive years.

Based on the results of sample testing, corrective action plans are required for the following nine programs due to estimated error amounts above $10 million: CBP's Refund and Drawback Program, FEMA's Assistance to Firefighters Grants, FEMA's Disaster Relief Program - Individuals and Households Program, FEMA's Disaster Relief Program - Vendor Payments, FEMA's Homeland Security Grant Program, FEMA's National Flood Insurance Program, FEMA's Public Assistance Program, ICE's Detention and Removal Operations, and U.S. Coast Guard's Operating Expenses – Active Duty Military Payroll.

III. Corrective Action Plans

Corrective Action Plans for High-Risk Programs

Following are corrective actions plans for programs with estimated improper error amounts above $10 million.

CBP Custodial - Refund & Drawback

Table 7. Completed Custodial–Refund & Drawback Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. System limitations.	1. Manual controls needed to prevent drawback payments from occurring without proper authorization.	1. Evaluate Automated Commercial System (ACS) business rules for certification of payments.	April 2009	
		2. Update procedures, if necessary, and publish updated standard operating procedures.	April 2009	
		3. Review existing Self Inspection Worksheet and modify questions pertaining to certification of payments.	April 2009	
	2. Procedures not always followed on full desk reviews.	1. Review, update, and publish standard operating procedures related to full desk reviews.	April 2009	Full desk reviews are a form of manual control.
		2. Conduct annual training for drawback chiefs and specialists.	June 2009	

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
2. Insufficient retention period for documents.	1. Length of retention for drawback claims is three years from date of payment.	1. Track status of drawback simplification legislation and meet quarterly with relevant subcommittee.	September 2009	CBP met its FY 2009 goals. Work in this area will be on-going until needed legislation is passed.

Table 8. In Process and Planned Custodial–Refund & Drawback Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. System Limitations	1. Lack of automated controls in ACS.	1. Implement an automated drawback module in a new system.	December 2013	The new system is the Automated Commercial Environment (ACE).
2. Legislative complexity and limitations.	1. Current drawback legislation is complex and contains provisions that may impact IPIA testing.	1. Track status of drawback simplification legislation and meet quarterly with relevant subcommittee.	September 2010	Completion date is very hard to estimate as it is dependent on decision makers outside the Department.

FEMA Assistance to Firefighters Grants (AFG)

Table 9. In Process and Planned AFG Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Insufficient supporting documentation.	1. Missing invoice.	1. Provide applicants with examples of proper supporting documentation when award is granted.	February 2010	Applicant could provide proof of payment but not an invoice showing that purchases were consistent with grant application.
	2. Insufficient training.	2. Require applicants to complete the AFG Grant Management Tutorial available on the AFG website.	May 2010	AFG should explore enhancing the system to verify that each applicant successfully completed the training.

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
2. Purchases outside allowable timeframe.	1. Purchase before or after period of performance.	1. Generate an e-mail notification from the AFG system towards the end of the period of performance. Program staff should also contact applicants prior to the end of the period of performance.	April 2010	Applicants submitted requests for funding during period of performance but invoices were outside period of performance.
		2. Add a question on the payment request form to determine whether the goods or services have been or will be purchased.	January 2010	Provides an additional reminder to applicants to purchase goods and services within the period of performance.
		3. If an advance payment is requested, ask applicants whether arrangements have been made to purchase the goods within 30 days of receipt of funding.	January 2010	Provides an additional reminder to applicants to purchase goods and services within the period of performance.
3. Limited quality checks for supporting documentation.	1. Purchases may not be consistent with grant applications and payment requests.	1. Collect supporting documentation from a random sample of applicants.	May 2010	
		2. Develop and implement a metric for judging an applicant's ability to comply with documentation collection requests timely and sufficiently.	April 2010	Metric should be taken into account when reviewing the applicant's future grant applications.

FEMA Disaster Relief Program - Individuals and Households Program (IHP)

Table 10. Completed IHP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Insufficient system edits.	1. Separated Households policy needs to be reflected in system edits.	1. Clarify policy and develop consistent system edit checks.	March 2009	
2. Inadequate monitoring, training, and quality assurance work.	1. Personnel need training with the Lodging Expense Reimbursement System.	1. Provide training and require employees to pass a certification test.	September 2009	
3. Poor or outdated policy and guidance.	1. Inconsistent application of disaster-specific policy.	1. Develop and implement a process which ensures consistent application of disaster-specific policy.	September 2009	
	2. Separated Households policy is incomplete.	1. Develop policies and guidance needed to approve and make payments to affected individuals and households.	March 2009	

FEMA Disaster Relief Program - Vendor Payments

Table 11. Completed Disaster Relief Program -Vendor Payments Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Inadequate monitoring, training, and quality assurance work.	1. FEMA contracts were not consistently written for similar items.	1. Review procurement contracting language, standardize contracts where practical, and monitor compliance.	September 2009	Lack of consistency created issues with review and approval of payments.

Table 12. In Process and Planned Disaster Relief Program - Vendor Payments Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Contract administration.	1. Payment made outside period of performance.	1. Grant access to ProTrac for appropriate staff.	March 2010	Provides additional guidance to staff to verify payments are made within period of performance.
		2. Provide additional training for contracting staff.	July 2010	
	2. Unauthorized staff approved invoices	1. Document the delegation of authority.	March 2010	The payment process will be strengthened with modifications to policy and documentation of authorized officials.
		2. Enhance signature authority form and policy.	March 2010	
		3. Provide COTR appointment letter for each contract to FEMA Finance Center.	March 2010	
		4. Provide training on modified policies.	June 2010	
2. Payment errors.	1. Improper invoice.	1. Require that specific information be provided on each invoice.	March 2010	The assessment found instances where critical information was missing from invoices or invoice balances were modified without supporting documentation.
		2. Provide access to supporting documentation in ProTrac to verify invoice adjustments.	March 2010	
		3. Provide training to staff.	June 2010	

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
2. Payment errors.	2. Pricing variance errors.	1. Develop policy which prevents payment when discrepancies exist between invoice and contract.	June 2010	Differences between the contract and invoice should be reconciled with supporting documentation before a payment is disbursed.
	3. Missing documents.	1. Require authorized officials to provide supporting documentation with payment requests.	March 2010	Payment technicians should require supporting documentation before making payments.

FEMA Homeland Security Grant Program (HSGP)

Table 13. In Process and Planned HSGP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Insufficient supporting documentation.	1. Sub-grantees could not provide documentation to support payment requests.	1. Incorporate compliance with external documentation requests as a key metric to be taken into account when evaluating future grant applications.	February 2010	
		2. Establish responsiveness and timeliness standards to assess compliance with documentation requests throughout the grant process.	March 2010	
	2. Insufficient or incomplete documentation.	1. Develop a standardized document retention protocol and provide training.	March 2010	

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
2. Grant expenditures outside period of performance.	1. Grantees not holding sub-grantees accountable.	1. Require a certification statement from sub-grantee that all funds will be applied to transactions occurring within the period of performance.	April 2010	
		2. Random sample sub-grantees on an annual basis and/or develop a metric in grant closeout evaluations which will be considered when evaluating future grant applications.	April 2010	

FEMA National Flood Insurance Program (NFIP)

Table 14. In Process and Planned NFIP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Incorrect payment calculations and payment processing errors.	1. Misapplied profit costs and fees; improper determination of scope; incorrect application of coverage; Insufficient itemization on estimates and inventories; Incorrect application of special coverage limits.	1. Training—Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	June 2010	

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Incorrect payment calculations and payment processing errors.	2. Inadequate management controls and lack of re-reviews of litigation claim files.	1. Process improvement—Incorporate elements of the NFIP IPIA Assessment into claims operation review procedures. Continue the current accelerated frequency of claims operation reviews until satisfactory progress is seen.	March 2010	
		2. Tool development—Develop a web-based claims operation review data capture tool.	August 2010	
	3. Outstanding payments not reissued; Payment timeframes not met.	1. System enhancements.	April 2010	To help insurers and flood vendors identify payment processing errors electronically.
2. Insufficient damage documentation.	1. Lack of invoices, inventories, and estimates.	1. Training—Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	June 2010	Note: Risk factors and corrective actions for category, insufficient damage documentation, are inter-related.
	2. Needed third party experts not involved.	2. Process improvement—Incorporate elements of the NFIP IPIA Assessment into claims operation review procedures.	March 2010	
	3. No direct physical damage documentation.	3. Emphasize damage documentation requirements in the adjuster claims manual when it is updated.	May 2010	

FEMA Public Assistance (PA)

Table 15. In Process and Planned PA Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Insufficient costs documentation.	1. Insufficient supporting documentation.	1. Standardize record keeping.	March 2010	
		2. Provide record keeping guidance and training.	April 2010	
2. Out-of-scope payments.	1. Payments were made outside the period of performance.	1. Develop documentation review tools.	March 2010	
		2. Provide documentation review guidance to grantees.	April 2010	
		3. Provide guidance and training for Category Z project worksheets.	April 2010	
3. Unmet work completion deadline.	1. Documentation was not obtained and/or retained to substantiate valid work extensions.	1. Develop documentation review checklists.	February 2010	
		2. Provide guidance and training to grantees on correct invoice review policies.	March 2010	
		3. Develop guidance to store work extension documentation with project worksheet in system of record.	February 2010	
		4. Modify standard operating procedures to include record keeping guidance.	February 2010	
4. Missing payment verification documentation.	1. Documentation was not obtained and/or retained to substantiate that the correct sub-grantee was paid.	1. Develop documentation retention policies.	April 2010	

ICE Detention and Removal Operations (DRO)

Table 16. Completed Detention and Removal Operations Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Lack of Supporting Documentation.	1. Potential incidence of fraud, waste, and abuse of government funds.	1. Implement general oversight and monitoring to verify valid contract and obligation exists.	January 2009	All DRO offices transitioned to a single point of receipt for invoices. This change enables the ICE Office of the Chief Financial Officer (OCFO) to perform an up-front verification that an invoice is associated with a valid contract and obligation.
2. Goods and services received prior to award of contract.	1. Unauthorized use of budgetary resources.	1. Build awareness of regulations and laws through focused training and improved dissemination of policies.	Ongoing	- In August 2008, ICE conducted comprehensive training for its Analysts on obligation recording, monitoring, and management. - Implemented further training to reiterate policies and procedures.
3. Proper invoice did not exist in that the invoice did not contain the vendor's name.	1. Illegitimate invoice that can lead to potential incidence of fraud, waste, and abuse of government funds.	1. Implement up-front verification to ensure invoices received are in compliance with the Federal Acquisition Regulations (FAR).	January 2009	All DRO offices transitioned to a single point of receipt for invoices. This change enables the ICE OCFO to verify that an invoice is compliant with FAR upon receipt.
		2. Improved documentation of award contract that clearly states the elements of a FAR compliant invoice.	January 2009	All DRO specific Contracting Specialists were trained to include instructions for submission of invoice on the contract/award document.
4. Adjustments were not duly authorized.	1. Potential over/under payment of invoice.	1. Implement improved controls for monitoring invoice adjustments.	January 2009	All DRO offices transitioned to a single point of receipt for invoices. This change enables ICE OCFO to monitor the payment of each invoice and assist DRO with invoice adjustment, as needed.

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
4. Adjustments were not duly authorized.	1. Potential over/under payment of invoice.	2. Monitor compliance with the standard operating procedure for processing invoice adjustment.	Ongoing	
5. No receiving report documentation	1. No formal documentation of receipt of goods and services	1. Implement improved controls for receiving and approval process.	January 2009	All DRO offices transitioned to an improved invoice process where invoices are not paid unless authorized receiving and approval documentation is received by ICE OCFO.
6. Under paid interest.	1. Potential violation of Prompt Payment Act.	1. Ensure invoice receipt date is clearly indicated on the invoices.	January 2009	All DRO offices transitioned to a single point of receipt for invoices. This change enables ICE OCFO to stamp each invoice with the 'invoice received date' prior to forwarding it for processing.
		2. Ensure compliance with standard operating procedures.	January 2009	
7. Over paid interest.	1. Potential waste of government funds that could have been utilized for mission support activities.	1. Ensure invoice receipt date is clearly indicated on the invoices.	January 2009	All DRO offices transitioned to a single point of receipt for invoices. This change enables ICE OCFO to stamp each invoice with the 'invoice received date' prior to forwarding it for processing.
		2. Ensure compliance with standard operating procedures.	January 2009	

ICE Federal Protective Service

ICE completed all corrective action milestones for the Federal Protective Service in FY 2008 (see page 224–225 of the FY 2008 DHS Annual Financial Report, available at http://www.dhs.gov/xabout/budget/gc_1210714559908.shtm). Given the exceptionally low estimated error rate produced by this year's testing of FY 2008 payments, no additional corrective actions are required.

U.S. Coast Guard Active Duty Military Payroll (ADMP)

Table 17. Completed ADMP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Lack of supporting documentation.	1. Missing personnel record source documentation.	1. Issue contract to evaluate status of records and recommend corrective actions.	January 2009	90 day contract signed.
		2. Update policy to include the retention of appropriate source documents within military personnel data records.	January 2009	Scanned oath is critical to proving person works at USCG. Final policy included monitoring procedures.
		3. Establish procedures to ensure appropriate source documentation is captured at the Accession points.	July 2009	Involvement of military recruiters and servicing personnel offices was key.
2. USCG organizational issues.	1. Competition for resources with actuarial pension liability testing and other financial statement audit testing.	1. Review, and when possible, synchronize time frames to minimize conflict and maximize efficiency.	December 2008	
	2. Need to reduce and standardize critical personnel source documentation.	1. Reach agreement between all critical parties on required data elements and source documentation.	January 2009	U.S. Coast Guard transformation team hosted joint meetings with human resources, CFO, and CIO.
	3. No single owner of personnel offices.	1. The U.S. Coast Guard Modernization will result in organizational enhancements which will align recruiting, payroll, and personnel under one command.	March 2009	This issue is critical and resolution had proved elusive.

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
3. IPIA testing issues.	1. Delays in producing a correct payment detail file.	1. Reconcile transaction file total to accounting system trial balance.	December 2008	
		2. Increase test time period to allow ample time for retrieval of supporting documentation.	February 2009	

Table 18. In Process and Planned ADMP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Lack of supporting documentation.	1. Missing personnel record source documentation.	1. Develop and implement monitoring procedures to ensure adequacy of personnel record source documentation.	March 2010	
2. Untimely updating of personnel system.	1. Incorrect housing allowance.	1. Through training, ensure payroll systems are updated timely with housing change information.	March 2010	When feeder system is not updated timely, payment systems do not know the housing allowance entitlement has changed. Pay stubs contain a message alerting payee that errors must be brought to the immediate attention of personnel officer.
		2. Expand use of housing report which identifies records with a housing action and housing allotment set to yes.	FY 2005 and Ongoing	

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
3. USCG organizational issues.	1. Improve training for field personnel and housing officers (payroll processing is a secondary duty for majority of transaction processors).	1. Require completion of online training to acquire certification before transactions can be entered into feeder systems.	March 2010	This step will address geographic dispersion and the large number of officers.

IV. Program Improper Payment Reporting

Table 19 summarizes improper payment amounts for DHS high-risk programs and projects future year improvements based on completing corrective actions. Improper payment percent (IP%) and improper payment dollar (IP$) figures are based on statistical estimates for FY 2008. These estimates are then projected for FY 2009 and beyond based on improvements expected from completing corrective actions.

Table 19. Improper Payment Reduction Outlook

Improper Payment Reduction Outlook ($ in millions)															
Program	FY 2008 Outlays	FY 2008 IP%	FY 2008 IP$	FY 2009 Outlays	FY 2009 IP%	FY 2009 IP$	FY 2010 Est. Outlays	FY 2010 IP%	FY 2010 IP$	FY 2011 Est. Outlays	FY 2011 IP%	FY 2011 IP$	FY 2012 Est. Outlays	FY 2012 IP%	FY 2012 IP$
Refund & Drawback (CBP)	$1,245	0.91	$11	$1,418	0.07	$1	$1,350	0.07	$1	$350	0.07	$1	$1,350	0.07	$1
AFG (FEMA)	$505	4.63	$23	$533	4.50	$24	$540	4.25	$23	$410	4.00	$16	$350	3.50	$12
IHP (FEMA)	$638	1.86	$12	$702	1.50	$11	$772	1.25	$10	$849	1.00	$8	$934	0.75	$7
Disaster Relief Program Vendor Payments (FEMA)	$836	8.82	$74	$2,992	6.00	$180	$3,142	4.00	$125	$3,299	2.50	$82	$3,439	2.00	$69
HSGP (FEMA)	$1,390	18.75	$261	$1,390	17.00	$236	$1,390	15.00	$209	$1,390	12.00	$167	$1,390	9.00	$125
NFIP (FEMA)	$819	6.38	$52	$3,300	6.00	$198	$1,400	5.75	$80	$1,400	5.50	$77	$1,500	5.00	$75
PA (FEMA)	$3,325	5.48	$182	$3,325	5.48	$182	$3,325	5.21	$173	$3,325	3.85	$128	$3,325	2.50	$83
DRO (ICE)	$1,202	0.97	$12	$1,238	0.91	$12	$1,275	0.85	$11	$1,313	0.78	$10	$1,353	0.73	$10
FPS (ICE)	$712	0.01	$0	$778	0.01	$0	$778	0.01	$0	$778	0.01	$0	$778	0.01	$0
Active Duty Military Payroll (USCG)	$2,715	0.46	$13	$2,773	0.35	$10	$2,927	0.23	$7	$3,006	0.12	$4	$3,068	0.09	$3
All Programs	**$13,387**	**4.78**	**$640**	**$18,449**	**4.63**	**$854**	**$16,899**	**3.78**	**$639**	**$16,120**	**3.06**	**$493**	**$17,487**	**2.20**	**$385**

Note: For the two FEMA programs which were not tested nationally, HSGP and Public Assistance (PA), the error rate from the state(s) tested was applied to the national payment population to produce the estimated error amounts listed above. The estimated error rate in future years of reporting will likely change more than for other programs due to FEMA expanding testing to more states, gaining experience in testing these programs, and implementing corrective actions.

Recovery of Improper Payments

Sample testing of CBP's Refund & Drawback program identified an improper payment of $6.4 million which was recouped within 30 days.

V. Recovery Auditing Reporting

DHS completed recovery audit work for FY 2008 disbursements and continued collection activities for errors identified in prior year recovery audits. Work was completed at ICE, U.S. Coast Guard, and the Components they cross-service. Work was also completed at CBP and FEMA. In Table 20 which follows, current year (CY) equals FY 2008 disbursements and prior year (PY) covers FY 2005–FY 2007 for DNDO, TSA, and U.S. Coast Guard; and FY 2004–FY 2007 for CBP, ICE, MGMT, NPPD, S&T, and USCIS. FEMA does not list PY figures as they are reporting for the first time. Total Amounts Recovered PYs ($000) were adjusted from $3,561 reported in the FY 2008 DHS Annual Financial Report to $3,524 based on additional improper payment claims research. Adjustments involved MGMT, TSA, and USCG.

Table 20. 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	$2,232	$2,232	$18	$100	$274	$131	$292	$231
DNDO	$200	$200	$1	$0	$0	$0	$1	$0
FEMA	$1,601	$1,601	$178	$0	$0	$0	$178	$0
ICE	$2,335	$2,335	$14	$28	$1,716	$1,529	$1,730	$1,557
MGMT	$341	$341	$16	$84	$156	$69	$172	$153
NPPD	$418	$418	$0	$65	$190	$125	$190	$190
S&T	$370	$370	$0	$0	$54	$54	$54	$54
TSA	$2,200	$2,200	$16	$20	$706	$702	$722	$722
USCG	$2,700	$2,700	$18	$18	$89	$64	$107	$82
USCIS	$654	$654	$2	$16	$903	$850	$905	$866
Totals	**$13,051**	**$13,051**	**$263**	**$331**	**$4,088**	**$3,524**	**$4,351**	**$3,855**

VI. Ensuring Management Accountability

Managers are held accountable for reducing and recovering improper payments in a variety of ways. In FY 2009, Secretary Napolitano included recoupment of improper payments as an efficiency measurement which is tracked quarterly. Also, managers are responsible 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 were tested for their operating effectiveness.

The importance of reducing improper payments was discussed at meetings with all levels of staff. For example, the importance of improper payments was discussed regularly at DHS Senior Assessment Team meetings. Half-day workshops on improper payment topics were held. Presentations on improper payments were made at a New Hire Orientation for Financial Managers and at the annual DHS Financial Managers Conference.

VII. Agency Information Systems and Other Infrastructure

The Department is undertaking a Transformation and Systems Consolidation initiative which is discussed further under the Federal Financial Management Improvement Act on page 203.

CBP is upgrading its system to automate the handling of Refund & Drawback payments. The current Automated Commercial System is outdated and lacks functionality, necessitating a dependence on manual processes.

VIII. Statutory or Regulatory Barriers

CBP is working with a Congressional subcommittee to enact language which simplifies and clarifies current drawback legislation. 19 CFR sets the documentation retention period at three years, while the drawback claim lifecycle is indeterminable.

IX. Overall Agency Efforts

The Department focused its FY 2009 efforts on supporting FEMA's efforts to comply with the *Improper Payments Information Act*. Headquarters and FEMA personnel worked closely to expand payment sample testing to cover all high-risk programs. In addition, improvements were also made to FEMA's risk assessment methodology.

The Department, for the first time, completed recovery audits for all Components that issue more than $500 million in contracts annually. The Department formalized its tracking and reporting processes and increased the recoupment of improper payments identified in current and prior year recovery audits.

In FY 2009, the Department achieved a landmark milestone by complying, for the first time, with the *Improper Payments Information Act*. Compliance was achieved by: performing risk assessments to identify risk susceptible programs; completing payment sample testing to estimate improper payment amounts and error rates; implementing plans to reduce the level of improper payments for high-risk programs; and, annually reporting our results.

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 0.01 percent and 0.03 percent for the period of October 2008 through September 2009, with an annual average of 0.02 percent (Note: MTS statistics are reported with at least a six week lag).

Debt Collection Improvement Act (DCIA)

DHS implemented a debt collection regulation that supersedes Components' legacy agency regulations. In addition, the DHS Office of the Chief Financial Officer (OCFO) issued comprehensive debt collection policies that provide guidance to the components on the administrative collection of debt; referring non-taxable debt; writing off non-taxable debt; reporting debts to consumer reporting agencies; assessing interest, penalties and administrative costs; and reporting receivables to the Department of the Treasury. The regulation and policies will help Components meet the reporting requirements in support of the *Debt Collection Improvement Act of 1996* (DCIA).

FY 2008 Biennial User Charges Review

The Chief Financial Officers Act of 1990 requires each agency's CFO to review, on a biennial bases, 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 of the use of government goods or services.

A preliminary review of DHS user fees was conducted and reported by the CFO in FY 2008. This review was based on Component FY 2007 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 2010 and will be based on FY 2009 data.

Major Management Challenges

Office of Inspector General

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

Homeland Security

NOV 1 3 2009

MEMORANDUM FOR: The Honorable Janet Napolitano
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,* for inclusion in the DHS FY 2009 *Annual Financial Report*. Your office has indicated that formal comments to the report will be included in the *Annual Financial Report.*

Should you have any questions, please call me, or your staff may contact Anne L. Richards, Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

Department of Homeland Security
Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

OIG-10-16

November 2009

Office of Inspector General

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

Homeland Security

NOV 1 3 2009

Preface

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

The attached report presents our FY 2009 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Office of Inspector General

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

Homeland Security

Major Management Challenges Facing the Department of Homeland Security

The creation of the Department of Homeland Security (DHS) on March 1, 2003, was the most significant reorganization of the federal government bringing together twenty-two federal agencies in response to the aftermath of 9/11. Since its inception, the Department of Homeland Security performs a broad range of activities across a single driving mission to secure America from the entire range of threats that we face.

Six years later, the department is moving beyond operating as an organization in transition to a department diligently working to protect our borders and critical infrastructure, preventing dangerous people and goods from entering our country, and recovering from natural disasters effectively. However, while much progress has been done, the department 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.

We have identified the following major management challenges:

- Acquisition Management
- Information Technology Management
- Emergency Management
- Grants Management
- Financial Management
- Infrastructure Protection
- Border Security
- Transportation Security
- Trade Operations and Security

1

Since the major management challenges have tended to remain the same from year to year, we developed scorecards to distinguish the department's progress in selected areas. Our first scorecard, published in the *Semiannual Report to Congress*, October 1, 2006 – March 31, 2007, included an assessment of DHS' acquisition function. This report features scorecards for acquisition management, information technology management, emergency management, grants management, and financial management.

We based the ratings on a four-tiered scale ranging from limited to substantial progress[1]:

- **Limited:** While there may be plans to address critical success factors, few if any have been implemented;
- **Modest:** While some improvements have been made, many of the critical success factors have not yet been achieved;
- **Moderate:** Many of the critical success factors have been achieved; and
- **Substantial:** Most or all of the critical success factors have been achieved.

These five scorecards are summarized in Figure 1 and incorporated in our discussion of the major management challenges.

Figure 1.

DHS' OVERALL PROGRESS IN SELECTED AREAS Ratings are based on a four-tiered scale: Limited, Modest, Moderate, and Substantial.		
	FY 2008	FY 2009
Acquisition Management	**Modest Progress** 	**Moderate Progress** 
Information Technology Management	**Moderate Progress** 	**Moderate Progress** 
Emergency Management	**Moderate Progress** 	**Moderate Progress** 

[1] Financial Management Scorecard uses different criteria to assess limited to substantial progress, and is shown in the Financial Management section of the report.

2

DHS' OVERALL PROGRESS IN SELECTED AREAS Ratings are based on a four-tiered scale: Limited, Modest, Moderate, and Substantial.		
	FY 2008	FY 2009
Grants Management	N/A	**Modest Progress** 
Financial Management	**Modest Progress** 	**Modest Progress** 

ACQUISITION MANAGEMENT

DHS relies on goods and services contractors to help fulfill many of its critical mission areas. As such, effective acquisition management is vital to achieving DHS' overall mission. Acquisition management is much more than simply awarding a contract. It requires a sound management infrastructure to identify mission needs; develop strategies to fulfill those needs while balancing cost, schedule, and performance; and ensure that contract terms are satisfactorily met. A successful acquisition process depends on the following key factors:

- Organizational Alignment and Leadership—ensures appropriate placement of the acquisition function, defines and integrates roles and responsibilities, and maintains clear, strong executive leadership;
- Policies and Processes—partnering with internal organizations, effective use of project management approaches, and establishment of effective internal controls;
- Acquisition Workforce—commitment to human capital management, integration and alignment of human capital approaches with organizational goals, and investment in people; and
- Knowledge Management and Information Systems—tracking of key acquisition data, analysis of supplies and services spending, and data stewardship.

Acquisition Management Scorecard

The following scorecard illustrates areas where DHS improved its acquisition management practices, as well as areas where it continues to face challenges. We based our assessment on our recent audit reports, Government Accountability Office (GAO) reports, congressional testimony, and our broader knowledge of the acquisition function.

Based on the consolidated result of the four acquisition management capability areas, DHS made "**moderate**" overall progress in the area of Acquisition Management.

3

ACQUISITION MANAGEMENT SCORECARD	
Organizational Alignment and Leadership	**Modest Progress** 

DHS made "modest" progress in improving the acquisition program's organizational alignment and defining roles and responsibilities. The department continues to depend on a system of dual accountability and collaboration between the chief procurement officer and the component heads, which may sometimes create ambiguity about who is accountable for acquisition decisions. However, DHS maintains that the dual authority model works because the Office of the Chief Procurement Officer (OCPO) retains central authority over all contracting through its contracting officer warrant program and Federal Acquisition Certification - Contracting program. According to the department, the heads of contracting activities and contracting officers function independently of component influence as their authority flows from OCPO rather than the component. DHS also expects its proposed Acquisition Line of Business Integration and Management Directive to clarify existing authorities and relationships within individual components and the department's Chief Procurement Officer.

According to the Government Accountability Office (GAO),[2] DHS has not effectively implemented or adhered to its investment review process, which requires executive decision making at key points in an investment's life cycle. DHS has not provided the oversight needed to identify and address cost, schedule, and performance problems in its major investments due to a lack of involvement by senior management officials as well as limited monitoring and resources.

Although FEMA has reorganized its acquisition function to operate strategically,[3] FEMA program offices have not adequately integrated the acquisition function into their decision-making activities. Planning strategically requires that the Acquisition Management Division partner with other FEMA components and assist them in assessing internal requirements and the impact of external events. FEMA's Acquisition Management Division has begun to work more closely with program offices to better manage the acquisition process, monitor and provide oversight to achieve desired outcomes, and employ knowledge-based acquisition approaches.

Policies and Processes	**Moderate Progress** 

DHS made "moderate" progress in developing and strengthening its policies and processes related to acquisition management. Although the department has put a great

[2] GAO-09-29, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, November 2008.
[3] DHS-OIG, *FEMA's Implementation of Best Practices in the Acquisition Process*, (OIG-09-31, February 2009).

4

ACQUISITION MANAGEMENT SCORECARD

deal of effort into improving its processes and controls over awarding, managing, and monitoring contract funds, it still needs to do more.

According to a May 2009 report by the GAO,[4] DHS provided guidance on award fees[5] in its acquisition manual, but individual contracting offices developed their own approaches to executing award fee contracts that were not always consistent with the principles in the Office of Management and Budget's guidance on award fees or among offices within DHS. In addition, DHS has not developed methods for evaluating the effectiveness of an award fee as a tool for improving contractor performance. FEMA also needs to accelerate its planned acquisition process improvements for awarding, managing, monitoring, tracking, and closing-out contracts.[6]

DHS is making progress in the oversight of its services contracts. As of March 2009, all DHS professional services contracts greater than $1 million will undergo a mandatory review before a new contract is awarded or an existing contract is renewed to ensure that proposed contract awards do not include inherently governmental functions or impact core functions that must be performed by federal employees. DHS expects this additional review to add a new level of rigor to the DHS contracting process.

Acquisition Workforce	**Moderate Progress** 

DHS made "moderate" progress in recruiting and retaining a workforce capable of managing a complex acquisition program, but continues to face workforce challenges across the department. An April 2009 report by the GAO indicated that the Coast Guard filled 717 of its 855 military and civilian personnel positions in the acquisition branch[7] and planned to expand its acquisition workforce in FY 2011. However, some of its unfilled positions are core acquisition positions such as contracting officers and specialists, program management support staff, and engineering and technical specialists. Although FEMA has improved acquisition training and greatly increased the number of acquisition staff, it still needs to better prepare its acquisition workforce for catastrophic disasters.[8]

---

[4] GAO-09-630, *Federal Contracting: Guidance on Award Fees Has Led to Better Practices but is Not Consistently Applied,* May 2009.
[5] An award fee is an amount of money that a contractor may earn in whole or in part by meeting or exceeding subjective criteria stated in an award fee plan.
[6] DHS-OIG, *Internal Controls in the FEMA Disaster Acquisition Process*, (OIG-09-32, February 2009); DHS-OIG, *Challenges Facing FEMA's Disaster Contract Management*, (OIG-09-70, May 2009); DHS-OIG, *FEMA's Acquisition of Two Warehouses to Support Hurricane Katrina Response Operations*, (OIG-09-77, June 2009); DHS-OIG, *FEMA's Temporary Housing Unit Program and Storage Site Management*, (OIG-09-85, June 2009).
[7] GAO-09-620T, Coast Guard: Update on Deepwater Program Management, Cost, and Acquisition Workforce, April 2009.
[8] DHS-OIG, *Challenges Facing FEMA's Acquisition Workforce*, (OIG-09-11, November 2008).

5

ACQUISITION MANAGEMENT SCORECARD

In its response to our November 2008 management challenges report, DHS highlighted headquarters-level initiatives for building and retaining its acquisition workforce[9]. For example, DHS centralized recruitment and hiring of acquisition personnel, established the Acquisition Professional Career Program to hire and mentor procurement interns, created a tuition assistance program, and structured rotational and development work assignments. However, DHS needs time to complete all of these new initiatives. In the interim, personnel shortages will continue to hamper the department's ability to manage its contracts and workload in an effective and efficient manner.

Knowledge Management and Information Systems	**Modest Progress** 

DHS made "modest" progress in deploying an enterprise acquisition information system and tracking key acquisition data. DHS has not yet fully deployed a department-wide (enterprise) contract management system that is interfaced with the financial system. Many procurement offices continue to operate using legacy systems that do not interface with financial systems. With ten procurement offices and more than $17 billion in annual acquisitions and procurement, DHS needs a consolidated acquisition system to improve data integrity, reporting, performance measurement, and financial accountability.

In recent years, DHS did not ensure contract data was complete and accurate in the Federal Procurement Data System-Next Generation (FPDS-NG).[10] This system is the only consolidated information source for analyzing competition on procurements and is relied on for reporting to the public and Congress. DHS has taken steps to comply with May 2008 guidance, issued by the Office of the Federal Procurement Policy, that requires government agencies to develop a plan for improving the quality of acquisition data entered into FPDS-NG. For example, DHS developed a standard report format and data quality review plans.

INFORMATION TECHNOLOGY MANAGEMENT

Creating a unified information technology (IT) infrastructure for effective integration and agency-wide management of IT assets and programs remains a challenge for the DHS Chief Information Officer (CIO). The CIO's successful management of IT across the department will require the implementation of strong IT security controls, coordination of planning and investment activities across DHS components, and a commitment to ensuring privacy.

---

[9] *Department of Homeland Security FY 2008 Annual Financial Report.*
[10] DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition during Fiscal Year 2007*, (OIG-09-94, August 2009).

6

Security of IT Infrastructure

During our FY 2008 *Federal Information Security Management Act*[11] (FISMA) evaluation, we reported that the department continued to improve and strengthen its security program. Specifically, the department implemented a performance plan to improve on four key areas: Plan of Action and Milestones weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. The department also finalized its Sensitive Compartmented Information Systems Information Assurance Handbook, which provides department intelligence personnel with security procedures and requirements to administer its intelligence systems and the information processed.

Although the department's efforts have resulted in some improvements, components are still not executing all of the department's policies, procedures, and practices. Management oversight of the components' implementation of the department's policies and procedures needs improvement in order for the department to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system certification and accreditation.

Additional information security program areas that need improvement include configuration management, incident detection and analysis, specialized training, and privacy. In 2009, we reported[12] that DHS had implemented effective system controls to protect the information stored and processed by the department's unclassified network, LAN-A. DHS ensures that network patch management and vulnerability assessments are performed periodically. However, DHS did not have an effective process to manage its LAN-A privileged accounts or ensure that security patches were deployed on all applications. The lack of sufficient processes increased the risk that LAN-A security controls could be circumvented.

IT Management

The department faces significant challenges as it attempts to create a unified IT infrastructure for effective integration and agency-wide management of IT assets and programs. Toward that end, DHS has several initiatives underway to improve IT operations and reduce costs. One such program is the development of an enterprise-wide IT disaster recovery program to ensure that the department's operations can continue uninterrupted should its IT systems fail. We reported in April 2009 that DHS had made progress in implementing a disaster recovery program by allocating funds to establish two new data centers.[13] However, we noted that more work was needed to ensure the new data centers were fully capable of meeting the department's significant IT disaster recovery needs.

Another major IT challenge for the DHS CIO is OneNet, an initiative aimed at consolidating existing IT infrastructures into a wide area network. DHS began work on OneNet in 2005, and envisions it will provide the components with secure data, voice, video, tactical radio,

[11] Title III of the E-Government Act of 2002, Public Law 107-347.
[12] DHS-OIG, *Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A*, (OIG-09-55, April 2009).
[13] DHS-OIG, *DHS' Progress In Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

and satellite communications between internal and external DHS resources. We reported in September 2009 that DHS has taken various steps to consolidate existing infrastructures into OneNet, but faces challenges in completing its OneNet implementation.[14] Specifically, we reported that DHS is experiencing delays in meeting its scheduled completion date and that components are reluctant to participate and are not subscribing to the implementation of OneNet. As a result, DHS may not be able to reach its ultimate goal of consolidating and modernizing its existing infrastructures and achieve cost savings.

Component CIOs also face significant challenges in their efforts to improve IT management, budgeting, planning, and investment. In July 2009, we reported[15] that U.S. Citizenship and Immigration Services (USCIS) strengthened overall IT management by restructuring its Office of Information Technology and realigning its field IT staff. However, the department's efforts to enforce overall IT budget authority and improve agency-wide IT infrastructure have been difficult, due to insufficient staffing and funding. The department finalized its Office of the Chief Information Officer (OCIO) Staffing Plan in April 2009, in which it has identified the need to ensure sufficient staff with the right skills, security clearances and experience.

Our April 2008 audit of the Federal Emergency Management Agency's (FEMA) efforts to upgrade its disaster logistics management systems[16] showed that existing systems did not provide complete asset visibility, comprehensive asset management, or integrated logistics information. Since this report, FEMA has yet to finalize its logistic, strategic, and operational plans to guide logistics activities. In addition, FEMA has not developed processes and procedures to standardize logistics activities. Without such plans, processes, and procedures, selection of IT systems to support logistics activities will remain difficult.

Privacy

DHS continues to face challenges in ensuring that privacy concerns are properly addressed throughout the lifecycle of each program and information system. For example, our September 2009 report[17] identified a need for automated privacy tools to monitor the Transportation Security Administration's (TSA) file servers containing personally identifiable information. Without such tools, TSA's OCIO manually checked for personally identifiable information leaks on file servers. However, these manual checks did not prevent regularly occurring classified data spills and unprotected e-mails containing personnel information.

We also reported that TSA made progress in implementing a framework that promotes a privacy culture and complies with federal privacy laws and regulations. Specifically, TSA designated the Office of Privacy Policy and Compliance to oversee its privacy functions.

---

[14] DHS-OIG, *Improved Management and Stronger Leadership are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009).
[15] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90, July 2009).
[16] DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, (OIG-08-60, May 2008).
[17] DHS-OIG, *Transportation Security Administration Privacy Stewardship* (OIG-09-97, August 2009).

This office strengthened TSA's culture of privacy through coordination with managers of programs and systems that contain personally identifiable information to meet reporting requirements, performing Privacy Impact Assessments, preparing public notifications of systems of records, and enforcing privacy rules of conduct. The office also established processes for reviewing and reporting privacy incidents, issuing public notices, addressing complaints and redress for individuals, and implementing and monitoring privacy training for employees.

IT Management Scorecard

The following scorecard demonstrates where DHS' IT management functions have been strengthened. This high-level assessment identifies progress in six IT management capability areas: IT budget oversight, IT strategic planning, enterprise architecture, portfolio management, capital planning and investment control, and IT security. These six elements were selected based on IT management capabilities required by federal and DHS guidelines for enabling CIOs to manage IT department-wide.

Based on the consolidated result of the six IT management capability areas, DHS has made "**moderate**" progress in IT Management overall.

IT MANAGEMENT SCORECARD	
IT Budget Oversight: ensures visibility into IT spending and alignment with the strategic IT direction.	**Modest Progress** 
The DHS CIO has made improvements in managing department-wide IT budgets in accordance with the *Clinger-Cohen Act*[18] and the department's mission and policy guidance. The DHS 2009-2013 IT Strategic Plan emphases the importance of Component IT spending approval by either the Component-level CIO or the DHS CIO. However, gaining a department-wide view of IT spending was difficult due to some Component CIOs not having sufficient budget control and insight. For example, our 2009 report[19] on U.S. Citizenship and Immigration Services (USCIS) found that it was difficult for the USCIS CIO to perform IT budgeting because business units had direct fee revenue or appropriated funds and have not complied with IT budgetary control processes. Due to the limited benefits realized, IT Budget Oversight has made "modest" progress.	
IT Strategic Planning: helps align the IT organization to support mission and business priorities.	**Moderate Progress** 

[18] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Subtitle C, February 10, 1996.
[19] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology*, (OIG-09-90, July 2009).

9

IT MANAGEMENT SCORECARD	
An effective IT strategic plan establishes an approach to align resources and provides a basis for articulating how the IT organization will develop and deliver capabilities to support mission and business priorities. In January 2009, the department finalized its IT Strategic Plan, which aligns IT goals with overall DHS strategic goals. The plan also identifies technology strengths, weaknesses, opportunities, and threats. Due to the finalization and communication of the DHS IT Strategic Plan and plans to align IT with the department's goals, this area has made "moderate" progress.	
Enterprise Architecture: functions as a blueprint to guide IT investments for the organization.	**Moderate Progress** 
The *Clinger-Cohen Act* requires that CIOs develop and implement an integrated IT architecture for the agency to avoid the risk that systems will be duplicative, not well integrated, and limited in optimizing mission performance. DHS has shown continued support of its enterprise architecture program, and has requested over $100 million of funding for fiscal year 2010. In addition, the DHS IT Strategic Plan identifies a performance measure for the percentage of IT investments reviewed and approved through the Enterprise Architecture Board. This should further promote and enforce alignment of IT investments across the department. The department has shown "moderate" progress in implementing its enterprise architecture.	
Portfolio Management: improves leadership's ability to understand interrelationships between IT investments and department priorities and goals.	**Modest Progress** 
The DHS OCIO has made "Modest" progress in establishing the department's portfolio management capabilities as instructed by OMB Circular A-130.[20] The DHS portfolio management program aims to group related IT investments into defined capability areas to support strategic goals and missions. Portfolio management improves leadership's visibility into relationships among IT assets and department mission and goals across organizational boundaries. The DHS IT Strategic Plan identifies a goal to effectively manage IT capabilities and implement cross-departmental IT portfolios that enhance mission and business performance. Although progress is being made, the department has not identified fully opportunities to standardize, consolidate, and optimize the IT infrastructure. Based on the limited benefits realized, the department has shown "modest" progress in implementing department-wide portfolio management.	

[20] Office of Management and Budget Circular A-130, Transmittal 4, *Management of Federal Information Resources*, November 2000.

10

IT MANAGEMENT SCORECARD	
Capital Planning and Investment Control: improves the allocation of resources to benefit the strategic needs of the department.	**Moderate Progress** 
The *Clinger-Cohen Act* requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning. To address this requirement, DHS' IT Strategic Plan communicated the importance of following the IT investment guidance provided by DHS management directive 0007.1.[21] This directive supports and expands on the Act's requirement for technology, budget, financial, and program management decisions. The department has made "moderate" progress with respect to allocation of resources to benefit its strategic needs.	
IT Security: ensures protection that is commensurate with the harm that would result from unauthorized access to information.	**Moderate Progress** 
DHS IT security is rated at "moderate," for progress made during the last 3 years in compliance with FISMA. OMB Circular A-130 requires agencies to provide protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to information and systems assets or their loss, misuse, or modification. Regarding intelligence systems, information security procedures have been documented and controls have been implemented, providing an effective level of systems security.	

EMERGENCY MANAGEMENT

FEMA's mission is to support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. The Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Reform Act),[22] enacted to address shortcomings exposed by Hurricane Katrina, expanded the scope of the agency's mission, enhanced FEMA's authority and gave it primary responsibility for the four phases of comprehensive emergency management: preparedness, response, recovery, and mitigation.

[21] DHS Management Directive 0007.1: *Information Technology Integration and Management* March 2007.
[22] Public Law 109-295, Title VI – National Emergency Management, of the *Department of Homeland Security Appropriations Act of 2007*.

11

In March 2008, we released a report on FEMA's progress in addressing nine key preparedness areas related to catastrophic disasters: overall planning, coordination and support, interoperable communications, logistics, evacuations, housing, disaster workforce, mission assignments, and acquisition management.[23] FEMA's progress in these areas ranged from limited to moderate. FEMA officials said their progress was impacted by budget shortfalls, reorganizations, inadequate IT systems, and confusing or limited authorities. We made several recommendations for improvements in overall planning, coordination, and communications. We plan to update this catastrophic assessment in FY 2010.

As we reported in June 2009, FEMA's response to Hurricane Ike was well organized and effective. Within seven weeks of landfall, FEMA registered more than 715,000 hurricane victims, completed 359,000 housing inspections, installed manufactured housing for 339 families, and disbursed over $326 million for housing and other needs.[24]

While our emphasis in last year's scorecard was catastrophic preparedness, this year's scorecard focuses on three key challenges FEMA faces in meeting its broader emergency management mission.

Emergency Management

The following scorecard highlights FEMA's progress in three key areas: disaster sourcing, housing, and mitigation.

Based on the consolidated result of the three areas presented here, as well as progress made in acquisition management and disaster grants management, FEMA has made "**moderate**" progress in the area of Emergency Management.

EMERGENCY MANAGEMENT SCORECARD	
Disaster Sourcing	**Moderate Progress** 
When disaster strikes, FEMA must be prepared to quickly provide goods and services to help state and local governments respond to the disaster. Disaster resources, ranging from water and meals to tarps and blankets, can be provided directly by FEMA, by another federal agency under direction from FEMA, or by the private sector through a contract with FEMA or another federal agency. In reviewing FEMA's use of its four primary sourcing mechanisms: (1) warehoused goods; (2) mission assignments; (3) interagency agreements; and (4) contracts, we determined that FEMA does not have a clear, overarching strategy that guides decision making on which of these sourcing mechanisms to use to meet a particular need.	

[23] DHS-OIG, *FEMA's Preparedness for the Next Catastrophic Disaster*, (OIG-08-34, March 2008).
[24] DHS-OIG, *Management Advisory Report: FEMA's Response to Hurricane Ike*, (OIG-09-78, June 2009).

12

EMERGENCY MANAGEMENT SCORECARD

FEMA's disaster sourcing decisions are process driven and not compliant with the National Incident Management System. Decision making is stove-piped within the Joint Field Office and among various levels of FEMA. This approach does not allow FEMA to centralize disaster sourcing decision making and limits its ability to: (1) implement an overarching sourcing strategy; (2) minimize unnecessary duplication; (3) take advantage of resource ordering efficiencies; and (4) create transparency and maintain visibility over the entire resource ordering process.[25]

We have also reported that some sourcing decisions are made in response to pressure from internal and external officials and are not necessarily based on actual need or a request from the state affected by a disaster.[26] While often well-meaning, the pressure can result in waste when the goods or services are not needed and can be disruptive to the sourcing process. Implementing single-point ordering and supporting it with IT systems that provide increased visibility and transparency will allow FEMA to provide a focal point for such input and increase the availability of information on what goods and services have been requested, ordered, and delivered.[27]

Housing — **Modest Progress**

While FEMA has made strides in a number of areas since hurricanes Katrina and Rita struck the Gulf Coast, there remains room for improvement, including in the critical area of disaster housing.[28] FEMA does not yet have sufficient tools, operational procedures, and legislative authorities to aggressively promote the cost-effective repair of housing stock, an important element of post-disaster housing.

The repair and restoration of existing housing stocks is one of the most important challenges FEMA and its response and recovery partners face following a catastrophic housing disaster. All other housing decisions and programs hinge on this single variable.

After Hurricane Katrina, Congress required FEMA to develop the National Disaster Housing Strategy. FEMA issued the strategy in January 2009. The strategy summarizes the sheltering and housing capabilities, principles, and policies that will guide the disaster housing process. The strategy promotes engagement of all levels of government, along with nonprofits, the private sector, and individuals to collectively address the housing needs of disaster victims. The goal is to enable individuals, households, and communities

[25] DHS-OIG, *FEMA's Sourcing for Disaster Response Goods and Services,* (OIG-09-96, August 2009).
[26] DHS-OIG, *Management Advisory Report: FEMA's Response to Hurricane Ike,* (OIG-09-78, June 2009).
[27] DHS-OIG, *FEMA's Sourcing for Disaster Response Goods and Services,* (OIG-09-96, August 2009).
[28] DHS-OIG, *Federal Emergency Management Agency's Exit Strategy for Temporary Housing in the Gulf Coast Region*, (OIG-09-02, October 2008); DHS-OIG, *FEMA Response to Formaldehyde in Trailers*, (OIG-09-83, June 2009); DHS-OIG, *Management Advisory Report: Computer Data Match of FEMA and HUD Housing Assistance Provided to Victims of Hurricane Katrina and Rita,* (OIG-09-84, June 2009).

13

EMERGENCY MANAGEMENT SCORECARD

to rebuild and restore their way of life as soon after a disaster as possible.

The strategy is a positive step forward, but it is only an interim step. It outlines a number of potential programs and federal agencies that can help victims find housing solutions. However, the strategy does not describe what would be a favorable outcome or goal in a particular disaster scenario or include action plans designed to achieve specific goals. To be complete, FEMA's action plan must specify what constitutes success under increasingly severe disaster scenarios, especially catastrophic disasters.

FEMA must develop better tools and operational procedures to respond effectively to the next disaster, especially a catastrophic disaster that destroys much housing stock. To better manage expectations and speed housing solutions, FEMA should set achievable housing goals and manage expectations following disasters. It is also critically important that all disaster stakeholders at the federal, state, and local levels maintain momentum and continue to implement needed changes over time.

FEMA needs more flexibility to explore innovative and cost-effective solutions to disaster housing challenges. In our report, *FEMA's Sheltering and Transitional Housing Activities After Hurricane Katrina*, issued in September 2008, we encouraged FEMA to explore alternatives to its traditional housing programs, including providing lump sum payments to disaster victims.[29] This could be a more cost-effective and expeditious way of returning victims to a more normal way of life.

Mitigation

Modest Progress

Mitigation is the effort to reduce loss of life and property by lessening the impact of disasters. In the realm of emergency management, hazard mitigation falls into three broad categories: natural, technological and manmade. Natural hazards are those generally associated with weather and geological events, such as hurricanes, tornadoes or earthquakes. Technological hazards include dams, gas lines and chemical facilities. Manmade hazards are typically associated with a criminal or terrorist attack using devices such as an improvised explosive device, biological weapon or chemical weapon. FEMA's Mitigation Directorate manages the National Flood Insurance Program and a range of programs designed to reduce future losses from natural hazards. Other DHS components have responsibility for mitigation of technological and manmade hazards.

The *Flood Insurance Reform Act of 2004* was enacted to reduce or eliminate future losses to properties in the National Flood Insurance Program by establishing the Repetitive Flood Claims and the Severe Repetitive Loss grant programs. Repetitive loss properties are insured properties that have incurred two or more flood losses greater than $1,000 within any 10-year period. FEMA and its state and local partners have mitigated nearly

[29] DHS-OIG, *FEMA's Sheltering and Transitional Housing Activities After Hurricane Katrina*, (OIG-08-93, September 2008).

14

EMERGENCY MANAGEMENT SCORECARD

15,000 repetitive loss properties since 1978, but an average of 5,188 new repetitive loss properties have been added each year, outpacing FEMA mitigation efforts by a factor of 10 to 1.[30]

Many of the conditions we reported in 2009 regarding the challenges of mitigating repetitive loss properties are the same as those we reported in 2002: (1) FEMA can only promote the notion of mitigation and cannot directly compel property owners in flood hazard areas to mitigate; (2) mitigation professionals need access to accurate information about repetitive loss properties to better manage the repetitive flood loss problem; and, (3) the need to impose actuarial rates on repetitive loss properties is vital to the financial independence of the National Flood Insurance Program. To address these challenges, we have recommended that FEMA apply actuarial insurance rates to properties on leased federal land and implement regulations to expand the use of increased cost of compliance coverage for all qualifying FEMA mitigation programs.

FEMA regulations regarding the implementation of public assistance and mitigation projects located in Coastal Velocity Zones (V Zones) are derived from Executive Order 11988, which requires federal agencies and responsible entities to avoid direct or indirect support to floodplain development wherever there is a practicable alternative. However, FEMA in practice directly supports community development in V Zones by funding recovery projects and providing insurance under the National Flood Insurance Program to properties located in V Zones. This is a significant management challenge for FEMA because it must find a balance between meeting the needs of coastal communities while not inadvertently encouraging settlement in floodplains and hazardous coastal areas. As a result of our review and subsequent recommendations concerning FEMA's recovery assistance and mitigation projects located in Louisiana coastal areas, FEMA is evaluating its policies relating to the application of recovery assistance, insurance, and mitigation projects located in V Zones.[31]

GRANTS MANAGEMENT

FEMA provides disaster assistance to communities through the Public Assistance Grant Program, the Hazard Mitigation Grant Program, and the Fire Management Assistance Grant Program. Under each of these grant programs, the affected State is the grantee, and the State disburses funds to eligible subgrantees. FEMA also awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. However, improvements are needed in FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees.

---

[30] DHS-OIG, *FEMA's Implementation of the Flood Insurance Reform Act of 2004*, (OIG-09-45, March 2009).
[31] DHS-OIG, *FEMA Policy Relating to Coastal Velocity Zones*, (OIG-09-71, May 2009).

15

Given the billions of dollars appropriated annually for preparedness, disaster, and non-disaster grant programs, DHS needs to ensure that internal controls are in place and adhered to, and that grant recipients are sufficiently monitored to achieve successful outcomes. DHS should continue refining its risk-based approach to awarding preparedness grants to ensure that the most vulnerable areas and assets are as secure as possible. Sound risk management principles and methodologies will help DHS prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.

Grants Management

The following scorecard highlights the department's progress in two key areas: disaster and non-disaster grants management. FEMA is taking steps to improve its grant policies, procedures, systems, and processes which when developed and implemented should strengthen its grants management and oversight infrastructure.

Based on the consolidated result of the two areas presented here, FEMA has made "**modest**" progress in the area of Grants Management.

GRANTS MANAGEMENT SCORECARD	
Disaster Grants Management	**Moderate Progress** 
In FY 2008, we issued 25 financial assistance (subgrant) audit reports, identifying more than $23 million in questioned costs. As of August 2009, we had issued 41 subgrant audit reports in FY 2009, with more than $80 million in questioned costs. While FEMA does not directly manage subgrants, it is incumbent on FEMA to make certain that States, as grantees, understand the rules and regulations that govern disaster grants and ensure that subgrantees adhere to these. We plan to issue a report in early FY 2010 that presents some of the most common problems that lead to questioned costs, including inconsistent interpretation of policies by FEMA personnel and, in the case of fire assistance, problems with unsupported charges billed to subgrantees by other federal agencies that provided services.	
Non - Disaster Grants Management	**Modest Progress** 
Monitoring and documenting the effectiveness of DHS' multitude of grant programs continue to pose significant challenges for the department. DHS manages more than 80 disaster and non-disaster grant programs. This challenge is compounded by other federal agencies' grant programs that assist state and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural	

16

GRANTS MANAGEMENT SCORECARD

disasters.

Improvements are needed in FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees. Specifically, FEMA does not consistently and comprehensively execute its two major oversight activities, financial and program monitoring. This occurs, in part, because FEMA does not have sufficient grants management staff. FEMA has not conducted the analyses and developed the plan of action required by Public Law 109-295 Title VI, the *Post Katrina Emergency Management Reform Act of 2006* as part of its strategic human capital plan. In addition, financial and programmatic monitoring policies, procedures, and plans are not comprehensive.

FEMA has formed an Intra-Agency Grants Program Task Force that has developed a FEMA Grants Strategy to drive future enhancements in grants policies, procedures, systems, and processes. The task force has identified projects including the development of comprehensive grant management monitoring policies and procedures for the FEMA directorates with program management and oversight responsibilities.

Many states, as grantees, are not sufficiently monitoring subgrantee compliance with grant terms and cannot clearly document critical improvements in preparedness as a result of grant awards. During FY 2009, we issued audit reports on homeland security grants management by Illinois and California. We are currently reviewing Massachusetts, Maryland, Missouri, South Carolina, West Virginia, and the District of Columbia. These entities generally did an efficient and effective job of administering the grant funds; however, the most prevalent areas needing improvement concerned performance measurement, subgrantee monitoring, financial documentation and reporting, and control of expenditure reimbursement requests.

FINANCIAL MANAGEMENT

DHS continued to improve financial management in FY 2009, but challenges remain. Beginning in FY 2009, our independent auditors performed an integrated financial statement and internal control over financial reporting audit limited to the DHS consolidated balance sheet and statement of custodial activity. As in previous years, our independent auditors were unable to provide an opinion on those statements because the department could not provide sufficient evidence to support its financial statements or represent that financial statement balances were correct. Additionally, the independent auditors were unable to perform procedures necessary to form an opinion on DHS' internal control over financial reporting of the balance sheet and statement of custodial activity due to the pervasiveness of the department's material weaknesses.

17

Although the department has continued to remediate material weaknesses and has reduced the number of conditions contributing to the disclaimer of opinion on the financial statements, all six material weakness conditions were repeated in FY 2009. Furthermore, the increase in audit scope related to auditing internal control over financial reporting resulted in our independent auditor identifying significant departmental challenges that have a pervasive impact on the effectiveness of internal controls over consolidated financial reporting. Specifically:

- The department lacks a sufficient number of accounting and financial management personnel with core technical competencies to ensure that its financial statements are presented accurately and in compliance with generally accepted accounting principals
- DHS' accounting and financial reporting infrastructure, including policies, procedures, processes, and internal controls, have not received investments in proportion to the department's rapid growth in new programs and operations, and changes in mission since the department's inception;
- Field and operational personnel do not always share responsibilities for, or are not held accountable for, matters that affect financial management, including adhering to accounting policies and procedures and performing key internal control functions in support of financial reporting;
- The department's financial Information Technology (IT) system infrastructure is aging and has limited functionality, which is hindering the Department's ability to implement efficient corrective actions and produce reliable financial statements that can be audited.

IT controls and systems functionality conditions at FEMA and ICE deteriorated in FY 2009. The remaining significant component level challenges preventing the department from obtaining an opinion on its consolidated balance sheet and statement of custodial activity are primarily at the Coast Guard and TSA. In both FY 2009 and FY 2008, Coast Guard was unable to assert to any of its account balances; and TSA was unable to fully support the accuracy and completeness of the property, plant, and equipment (PP&E) account balance. However, the Coast Guard has made limited progress implementing the *Financial Strategy for Transformation and Audit Readiness* (FSTAR) in FY 2009. As a result, the auditors have been able to perform limited audit procedures over PP&E and actuarial liabilities. Additionally, the FSTAR calls for substantially more progress after FY 2010, especially in areas necessary to assert to the completeness, existence, and accuracy of PP&E, actuarial liabilities, and fund balance with Treasury balances.

Financial Management Scorecard

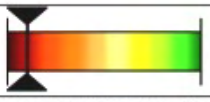
The following scorecard presents the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2008. The scorecard is divided into two categories: (1) Military – Coast Guard and (2) Civilian – all other DHS components. The scorecard lists the six material weaknesses identified during the independent audit of the FY 2008 DHS consolidated balance sheet and statement of custodial activity. These weaknesses continued to exist throughout FY 2009 and were again noted in

the FY 2009 independent auditor's report. For a complete description of the internal control weaknesses identified in the FY 2008 audit, see OIG-09-09.[32] To determine the status, we compared the material weaknesses reported by the independent auditor in FY 2008 with those identified in FY 2009.[33] The scorecard does not include other financial reporting control deficiencies identified in FY 2009 that do not rise to the level of a material weakness, as defined by the American Institute of Certified Public Accountants.

The ratings are based on a four-tiered scale ranging from limited to substantial progress as follows:

- **Limited:** While there may be plans to address internal control weaknesses, few if any have been remediated;
- **Modest:** While some improvements have been made and account balances have been corrected, many systemic internal control weaknesses remain;
- **Moderate:** Many of the internal control weaknesses have been remediated; and
- **Substantial:** Most or all of the internal control weaknesses have been remediated.

Based on the consolidated result of the seven financial management areas included in the report, DHS has made "**modest**" progress overall in financial management.

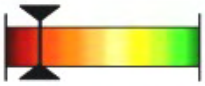
FINANCIAL MANAGEMENT SCORECARD		
Financial Reporting and Management: Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period. Financial management is the planning, directing, monitoring, organizing, and controlling of financial resources, including program analysis and evaluation, budget formulation, execution, accounting, reporting, internal controls, financial systems, grant oversight, bank cards, travel policy, appropriation-related Congressional issues and reporting, working capital funds, and other related functions.		
Military	**Limited Progress**	
	The Coast Guard has demonstrated limited progress in remediating the numerous internal control weaknesses identified by the independent auditors during FY 2008. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2008 included: 1) lack of an effective general ledger system; and 2) lack of effective policies, procedures, and controls surrounding the financial reporting process. In	

[32] DHS-OIG, *Independent Auditors' Report on DHS' FY 2008 Financial Statements*, (OIG-09-09, November 2008).
[33] DHS-OIG, *Independent Auditors' Report on DHS' FY 2009 Financial Statements and Internal Control Over Financial Reporting*, (OIG-10-11, November 2009).

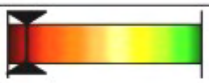
19

FINANCIAL MANAGEMENT SCORECARD		
	FY 2008 the Coast Guard revised its FSTAR; however, most of the actions outlined in the FSTAR were scheduled to occur after FY 2008. During FY 2009, the independent auditors noted that the Coast Guard continued implementation of its FSTAR and made some progress by completing its planned corrective actions over pension liabilities. This allowed management to make assertions on completeness and accuracy on its accrued liabilities, which represents more than 50 percent of the department's total liabilities. However, most corrective actions outlined in the FSTAR are scheduled to occur after FY 2009, and consequently many of the financial reporting weaknesses reported in prior years remained as of the end of FY 09. Among the conditions at Coast Guard that contribute to a material weakness in this area during FY 2009 is the lack of sufficient financial management personnel to identify and address control weaknesses, and develop and implement effective policies, procedures, and internal controls over financial reporting process.	
Civilian	**Limited Progress**	
	FY 2008, the independent auditors found several internal control weaknesses in financial reporting at FEMA and TSA. Those conditions contributed to qualifications of the auditors' opinion on the department's consolidated financial statements. Overall, the department has made limited progress in FY 2009 in addressing the internal controls weakness the auditor identified in this financial reporting in FY 2008. FEMA and TSA, which both contributed to a material weakness in this area in FY 2008, have shown only minimal progress in improving the internal control weaknesses. Conditions at CBP have deteriorated in FY 2009, although less severe than at FEMA and TSA. These internal control deficiencies at CBP, FEMA, and TSA have contributed to a material weakness in this area for the department overall in FY 2009. Among the deficiencies noted in the FY 2009 independent auditor's report is that the department lacks a sufficient number of accounting and financial management personnel with core technical competencies to ensure its financial statements are prepared accurately and in compliance with generally accepted accounting principles. This condition was common among CBP, FEMA, and TSA in FY 2009.	

20

FINANCIAL MANAGEMENT SCORECARD		
Information Technology Controls and Financial Systems Functionality: IT general and application controls are essential for achieving effective and reliable reporting of financial and performance data.		
Military	**Limited Progress**	
	During 2008, the independent auditors identified numerous IT general control deficiencies, of which nearly all were repeat findings from prior years. The most significant IT deficiencies that could affect the reliability of the financials statements related to the development, implementation, and tracking of scripts, and the design and implementation of configuration management policies and procedures. These deficiencies at the Coast Guard contributed to a material weakness for the department in this area in FY 2008. For FY 2009, the Coast Guard has demonstrated limited progress in correcting certain IT general control weaknesses identified in previous years. As a result of the increase in scope of IT testing in FY 2009, the auditors have identified additional weaknesses that were not reported in the prior year. Therefore, although the Coast Guard corrected some deficiencies in IT general controls, the number of IT control weaknesses increased over the prior year. Over 50 percent of the findings the auditors identified in FY 2009 were repeat conditions from the prior year. One key area that remains a challenge for the Coast Guard is its core financial system configuration management process. For 2009, the auditors again noted that the configuration management process is not operating effectively. Financial data in the general ledger may be compromised by automated and manual changes that are not properly controlled. The changes are implemented through the use of IT script process, which was instituted as a solution to address functionality and data quality issues. However, the controls over the script process were not properly designed or implemented effectively from the beginning.	
Civilian	**Limited Progress**	
	Overall, DHS has made limited progress in correcting the IT general and applications control weaknesses identified in the FY 2008 independent auditor's report. During FY 2008, FEMA and TSA contributed to an overall material weakness in IT general and applications control, while CBP, FLETC, and USCIS all had significant deficiencies in this area.	

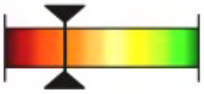
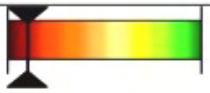
21

FINANCIAL MANAGEMENT SCORECARD		
	As a result of the increase in scope of the IT testing in FY 2009, the auditors have identified additional weaknesses that were not reported in the prior year. Therefore, although the DHS civilian components corrected some deficiencies in IT general controls, which resulted in the closure of more than 60 percent of the IT general controls findings reported in FY 2008, the number of department-wide IT control weaknesses increased over the prior year, with conditions at FEMA and ICE deteriorating. The auditors noted that many of the financial systems in use at DHS components have been inherited from the legacy agencies and have not been substantially updated since DHS' inception. As a result, ongoing financial system functionality limitations are contributing to the department's challenges in addressing systemic internal control weaknesses and strengthening the overall control environment. The FY 2009 independent auditor's report identified the following areas that continue to present risks to the confidentiality, integrity, and availability of DHS' financial data: 1) excessive access to key DHS financial applications, 2) application change control processes that are inappropriate, not fully defined or followed, and are ineffective, and 3) security management practices that do not fully and effectively ensure that financial systems are certified, accredited, and authorized to operation prior to implementation.	
Fund Balance with Treasury (FBwT): FBwT represents accounts held at Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency's FBwT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of various U.S. Government financial reports, and providing a more accurate measurement of budget resources.		
Military	**Limited Progress**	
	The Coast Guard has demonstrated limited progress in addressing the material weaknesses noted in this area in previous years. In FY 2008, the independent auditors reported a material weakness in internal control over FBwT at the Coast Guard. During FY 2009, the Coast Guard corrected some of the control deficiencies related to this area and revised its remediation plan (FSTAR) to include additional corrective actions, which are scheduled to occur after FY 2009. Consequently, most of the conditions which existed in FY 2008 continued to exist throughout FY 2009. For example, the auditors reported that the Coast Guard has not	

22

FINANCIAL MANAGEMENT SCORECARD		
	developed a comprehensive process, to include effective internal controls, to ensure that all FBwT transactions are recorded in the general ledger timely, completely, and accurately.	
Civilian	**N/A**	
	No control deficiencies related to FBwT were identified at the civilian components in FY 2009. Corrective actions implemented in previous years continued to be effective throughout FY 2008 and FY 2009.	
Property, Plant, and Equipment (PP&E) and Operating Materials and Supplies (OM&S): DHS capital assets and supplies consist of items such as property, plant, and equipment, operating materials; and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.		
Military	**Limited Progress**	
	The Coast Guard maintains approximately 52 percent of the department's property, plant, and equipment (PP&E), including a large fleet of boats and vessels. In FY 2008, internal control weaknesses related to PP&E at Coast Guard contributed to a material weaknesses in this area for the department. For FY 2009, the Coast Guard has demonstrated limited progress overall in correcting internal control weaknesses related to PP&E identified in the independent auditor's report in FY 2008. During FY 2009, the Coast Guard continued implementation of its remediation plan (FSTAR) to address the PP&E process and control deficiencies, and began remediation efforts. However, the corrective actions included in the FSTAR are scheduled to occur over a number of years. Consequently, most of the material weakness conditions reported in FY 2008 remained throughout FY 2009. For example, one of the conditions the auditors identified, which is a repeat from prior years, is that the Coast Guard has not established its beginning PP&E balance necessary to prepare the year-end balance sheet. The auditors also identified weaknesses related to operating materials and supplies (OM&S), which the Coast Guard maintains in significant quantities. These consist of tangible personal property to be consumed in normal operation to service marine equipment, aircraft, and other equipment. The auditors reported that the Coast Guard has not	

23

FINANCIAL MANAGEMENT SCORECARD		
	implemented policies, procedures, and internal controls to support financial assertions related to OM&S and related balances for FY 2009.	
Civilian	**Modest Progress**	
	DHS has demonstrated modest progress overall in correcting internal control weaknesses related to capital assets and supplies identified in the independent auditor's report in FY 2008. In FY 2008, FEMA, TSA, and CBP contributed to a material weakness in capital assets and supplies. The conditions that existed at TSA and FEMA prevented the auditors from completing their test work in FY 2008 and led to qualifications in the auditors' report. While FEMA has fully remediated its internal control weakness in this area during FY 2009, internal control conditions have deteriorated at CBP, USCIS, ICE, and NPPD. Although conditions at USCIS, ICE, and NPPD appear less severe that at CBP and TSA, when taken together, they contribute to an overall material weakness for the department in this area for FY 2009. Most of the control weakness conditions in this area are related to PP&E. Common among the components that contributed to the material weakness is the lack of adequate accounting policies, procedures, processes, and controls to properly account for its PP&E.	
Actuarial and Other Liabilities: Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including accounts and grants payable, legal and actuarial, and environmental liabilities.		
Military	**Limited Progress**	
	The Coast Guard maintains medical and post-employment travel benefit programs that require actuarial computations to record related liabilities for financial reporting purposes. Other liabilities include accounts payable, environmental, and legal liabilities. The Coast Guard was able to make financial statement assertions and present auditable balances in actuarial pension liabilities, demonstrating limited progress toward remediation of the control and reporting	

24

FINANCIAL MANAGEMENT SCORECARD		
	deficiencies that existed in this process in FY 2008. Among the conditions that remained throughout FY 2009 is that the Coast Guard has not implemented effective policies, procedures, and controls to ensure the completeness and accuracy of medical cost data and post-employment travel claims provided to, and used by, the actuary for the calculation of the medical and post-employment benefit liabilities.	
Civilian	**Moderate Progress**	
	During FY 2009, the civilian components demonstrated moderate progress overall in remediating internal control weaknesses related to actuarial and other liabilities. Significant internal control weaknesses which the independent auditors identified at FLETC, ICE, and S&T in FY 2008, and which contributed to a material weakness overall for the department, were fully remediated in FY 2009. However internal control deficiencies continue to exist at FEMA and new weaknesses were identified at TSA during FY 2009. These conditions at FEMA and TSA, together with the material weakness conditions at the Coast Guard, resulted in a material weakness for the department overall, in FY 2009. FEMA is recognized as the primary grant-making component of DHS, and the FY 2009 independent auditor's report noted that FEMA does not have sufficient policies and procedures in place to fully comply with the *Single Audit Act Amendments of 1996* and OMB Circular No. A-133, *Audits of States, Local Governments, and Non-profit Organizations.* TSA has numerous types of accounts payable and accrued liabilities that affect the balance sheet, including Other Transactions Agreements (OTA). One of the conditions at TSA that contributed to the department's material weakness is that TSA has not developed policies and procedures to accurately estimate OTA accrued liability at year-end.	
Budgetary Accounting: Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.		
Military	**Limited Progress**	
	The Coast Guard has made limited progress in this area. Many of the internal control weaknesses that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2008 remained throughout FY 2009. For example, the FY 2008 Independent Auditors' Report noted that the policies, procedures, and internal controls over the	

25

FINANCIAL MANAGEMENT SCORECARD		
	Coast Guard's process for validation and verification of some account balances are not effective to ensure that recorded amounts are complete, valid, accurate, and that proper approvals and supporting documentation is maintained. This weakness continues to exist in FY 2009, and remediation of these conditions is not planned for the Coast Guard until after FY 2009.	
Civilian	**Modest Progress**	
	During FY 2008, internal control weaknesses at CBP and FEMA contributed to a departmental material weakness in this area; the material weakness continued to exist throughout FY 2009. For FY 2009, the department made modest progress in correcting the deficiencies that were reported in FY 2008. Although CBP implemented policies and procedures related to deobligation of funds when contracts have expired or been completed, management has not been effective in adhering to these policies or monitoring compliance. CBP has not made substantial progress in correcting the deficiencies that were reported in FY 2008. Additionally, although FEMA improved its processes and internal control over the mission assignment obligation and monitoring process, some control deficiencies remain.	

INFRASTRUCTURE PROTECTION

DHS has direct responsibility for leading, integrating, and coordinating efforts to protect 11 critical infrastructure and key resources (CI/KR) sectors: the chemical industry; commercial facilities; critical manufacturing; 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 seven sectors for which other federal agencies have primary responsibility. The seven sectors for which DHS has an oversight role are 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. 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. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the implementation of protection efforts is a great challenge.

In our FY 2009 report, *Efforts to Identify Critical Infrastructure Assets and Systems*, OIG-09-86, we reported that the National Protection and Programs Directorate (NPPD) is in the process of acquiring the Infrastructure Information Collection System, a replacement for the

26

National Asset Database.[34] It is envisioned that the Infrastructure Information Collection System will greatly reduce critical infrastructure risk management gaps by providing dynamic information collection systems that include a range of relevant sources. In addition, the Infrastructure Information Collection System will allow relevant critical infrastructure partners from federal, state, local, and private entities to access various tools that house infrastructure data. Until this system is fully implemented, decision making regarding CI/KR will continue to be a significant challenge.

Concerning DHS's efforts to protect the cyber infrastructure, we reported in August 2009 that the National Cyber Security Division (NCSD) had implemented its Control Systems Security Program (CSSP) to coordinate the cybersecurity efforts for control systems between the public and private sectors.[35] We reported that while NCSD has made progress in implementing a cybersecurity program for control systems, opportunities exist for improvements to its CSSP. For example, NCSD needs to encourage more information sharing of critical infrastructures needs, threats, and vulnerabilities between the public and private sectors. NCSD also needs to increase the number of cybersecurity vulnerability assessments performed in order to reduce the overall risk to current operational control systems.

Also in FY 2009, we will evaluate how DHS coordinates its infrastructure protection efforts with other federal agencies, state and local governments and industry partners by reviewing the protection of petroleum and natural gas infrastructure within the energy sector. This review will determine (1) to what extent Protective Security Advisors (PSAs) are aligned to support the NPPD's primary national preparedness mission and the department's overall critical infrastructure protection strategy; (2) whether adequate guidance and resources have been provided to support the PSA program's growth; (3) the methods that PSAs use in coordinating efforts to identify, prioritize, and assess critical infrastructure and key resources within the Petroleum and Natural Gas subsectors; (4) how petroleum and natural gas stakeholders use the work that is done by PSAs; and (5) the metrics that the PSA Program uses to assess its own performance.

BORDER SECURITY

A principle DHS challenge is to secure the borders against all threats, including minimizing illegal entry of persons into the U.S. To achieve this goal the U.S. Customs and Border Protection (CBP's) security mission is to obtain operational control of the border. In this effort, CBP is implementing the Secure Border Initiative (SBI), a comprehensive multi-year approach to controlling the border including immigration enforcement within the United States.

SBInet is the program component of the SBI which will integrate personnel, infrastructure, technologies, and rapid response capability into a comprehensive border protection system. SBInet is intended to give our frontline officers the best possible environment to effectively

[34] DHS-OIG, *Efforts to Identify Critical Infrastructure Assets and Systems*, (OIG-09-86, June 2009).
[35] DHS-OIG, *Challenges Remain in DHS' Efforts to Secure Control Systems* (OIG-09-95, August 2009).

27

detect, identify and classify, respond to, and resolve situations that compromise border security.

CBP faces challenges implementing SBI and SBInet. CBP has not established adequate controls and effective oversight of contract workers responsible for providing SBI program support services. Although CBP has recently taken steps to improve SBI program management by hiring knowledgeable and experienced program managers, it continues to rely heavily on contract personnel, who comprise more than 50% of the SBI workforce. Also, CBP has not provided an adequate number of contracting officer's technical representatives to oversee support services contractors' performance resulting in contractors performing functions that should be performed by government workers. [36] We are evaluating controls to ensure effective oversight of the prime contractor's performance in meeting small business goals and SBInet program costs and schedule.

Border Patrol assessments could better document and define operational requirements for tactical infrastructure to ensure that border fence construction is linked to resource decisions and mission performance goals. Furthermore, CPB did not complete 56 (77%) of the 73 rapid response Border Patrol facilities projects it planned to complete in 2008 to support its border security mission. These projects include new facilities, modifications to existing facilities, and temporary solutions to accommodate new agents and shifting agent deployments. CBP also has not replaced Border Patrol vehicles at the required 20% annual rate and does not have a centralized information system to monitor vehicle availability. CBP initiated several actions to improve its design guide, develop a new project management tracking system, and update the space planning and cost estimation tool. In addition, CBP has taken actions to improve its overall management of vehicles.[37]

In addition, DHS needs to focus on improving the policies, processes, and procedures that govern the management and care of its detainee population. Prior reviews of ICE's detention and removal operations identified deficiencies in the oversight of immigration detention facilities. ICE has made efforts to strengthen the oversight of ICE detention assets by establishing a Detention Facilities Inspection Group (DFIG). The DFIG provides ICE with an independent inspection arm dedicated to oversight of ICE's Detention and Removal Operations (DRO) program. Additionally, ICE has contracted with private companies to provide on-site compliance verification of the Performance-Based National Detention Standards at all ICE detention facilities. However, we recently reported that ICE could further improve documenting the transfer of immigrant detainees and ensuring they received timely medial screenings and physical examinations, required by detention standards.[38] Additionally, ICE

---

[36] DHS-OIG, *Better Oversight Needed of Support Services Contractors in Secure Border Initiative Programs*, (OIG-09-80, June 2009); and DHS-OIG, *Progress in Addressing Secure Border Initiative Operational Requirements and Constructing the Southwest Border Fence*, (OIG-09-56, April 2009).
[37] DHS-OIG, *CBP's Construction of Border Patrol Facilities and Acquisition of Vehicles*, (OIG-09-91, July 2009).
[38] DHS-OIG, *Immigration and Customs Enforcement's Tracking and Transfers of Detainees*, (OIG-09-41, March 2009).

28

needs to determine whether its approach to managing the detention facility bed space is cost-effective.[39]

TRANSPORTATION SECURITY

The nation's transportation system is vast and complex, consisting of about 3.9 million miles of roads, over 100,000 miles of rail, almost 600,000 bridges, over 300 sea ports, over 2 million miles of pipeline, about 500 train stations, and over 5,000 public-use airports. The size of the transportation system, which moves millions of passengers and tons of freight every day, makes it both an attractive target for terrorists and difficult to secure. The nation's economy depends upon implementation of effective, yet efficient transportation security measures. The Transportation Security Administration (TSA) is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. Given the "open" environment, effective security strategies must be established, while maintaining quick and easy access for passengers and cargo. Since its inception, TSA has faced challenges with strengthening security for aviation, mass transit and other modes of transportation. TSA has made progress in addressing these challenges; however more needs to be done.

Checkpoint and Checked Baggage

The *Aviation and Transportation Security Act*[40] requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our undercover audit of checked baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items that enter the checked baggage system are not cleared for loading onto a passenger aircraft.[41] We recently issued a classified report on our unannounced, covert testing using fake law enforcement badges and credentials at selected domestic airports.[42] We tested equipment and techniques at the screening checkpoint to assess how well TSA is addressing the related challenges. We released a report on TSA's controls over screener uniforms, badges, and identification cards[43] and determined that TSA does not have adequate controls in place to manage and account for airport security identification display area badges, TSA uniforms, and TSA identification cards. Unauthorized individuals' access to those items increases an airport's level of risk to a wide variety of terrorist and criminal acts.

---

[39] DHS-OIG, *Immigration and Customs Enforcement Detention Bedspace Management*, (OIG-09-52, April 2009).
[40] Public Law 107-71, November 19, 2001.
[41] DHS-OIG, *Audit of the Effectiveness of the Checked Baggage Screening System and Procedures Used to Identify and Resolve Threats*, (OIG-09-42, March 2009).
[42] DHS-OIG, *Penetration Testing of Law Enforcement Credentials Used to Bypass Screening*, (OIG-09-99, September 2009 – Classified "Secret".)
[43] DHS-OIG, *TSA's Controls over SIDA Badges, Uniforms, and Identification Cards,* (OIG-08-92, September 2008).

Passenger Air Cargo Security

Approximately 7,500 tons of cargo are carried on passenger planes each day. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably "known" either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. Our audit determined that the criteria and guidance for evaluating a known shipper are unclear and subject to interpretation, increasing the risk that shippers may be improperly classified as known.[44] TSA's inspection and testing activities do not provide adequate assurance that regulated entities are complying with the program's requirements. Our report contained six recommendations to strengthen the controls and oversight of the program, including providing better criteria and guidance and improving inspection and testing activities. TSA generally concurred with all six recommendations in our report.

Rail and Mass Transit

Recent events on the rail and transit systems in Washington DC, including a derailment, fire, and crash, have raised questions regarding the mass transit agencies' contingency plans and the ability to handle these basic issues, as well as major emergencies. The *Aviation and Transportation Security Act* assigned TSA the responsibility to secure all modes of transportation in the United States. During emergencies, transit agencies rely on well-designed and regularly practiced drills and exercises to respond and recover rapidly. TSA created the Surface Transportation Security Inspection Program in 2005 to provide oversight and assistance to surface transportation modes. Surface Transportation Security Inspectors act as assessors, advisors, and liaisons, primarily in the mass transit and freight rail modes.

In our FY 2009 report, *Effectiveness of TSA's Surface Transportation Security Inspectors*, OIG-09-24, we reported that TSA is improving security in the mass transit and freight rail modes through the inspection program. Inspectors help bus and passenger rail stakeholders identify security gaps through Baseline Assessment for Security Enhancement reviews. They increase TSA's domain awareness by producing station profiles and by acting as liaisons between the Transportation Security Operations Center and transportation systems. They also participate in Visible Intermodal Prevention and Response exercises, which provide an unannounced, high-visibility presence in a mass transit or passenger rail environment. TSA faces important challenges in improving the effectiveness of the Surface Transportation Security Inspectors.

As TSA expands its presence in non-aviation modes, it must look critically at how it is deploying resources. TSA must continue to assess how planned exercises can better use the inspectors and their activities.

[44] DHS-OIG, *TSA's Known Shipper Program, (*OIG-09-35, March 2009).

TRADE OPERATIONS AND SECURITY

CBP is primarily responsible for trade operations and security, with the support of the Coast Guard and ICE. In 2008, approximately 11 million oceangoing cargo containers arrived at the nation's seaports. CBP typically processes more than 70,000 truck, rail, and sea containers per day, along with the personnel associated with moving this cargo across U.S. borders or to U.S. seaports. Modernizing trade systems, using resources efficiently, and managing and forging partnerships with foreign trade and customs organizations pose significant challenges for CBP and DHS.

To manage the threat and ensure the security of this large volume of maritime cargo, CBP employs a multilayered approach including analyzing screening shipment information, and using targeting systems to identify the highest risk cargo on which to focus its limited resources. An effective inspection process includes the screening of shipping information, nonintrusive inspections, and physical examinations. The Automated Targeting System (ATS), which uses a complex model of weighted rules, assists CBP officers in screening shipping information and selecting shipments for inspection.

While targeting high risk shipments continues to be challenge for CBP, it can improve its operations by updating its guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats. In addition, CBP should conduct a risk assessment to determine which pathways, including maritime cargo, pose the highest risk of biological and chemical weapons entering the Nation. [45]

We also reviewed DHS' planning, management oversight, and implementation of security measures to protect against small vessel threats.[46] Overall, the department has made progress in the area of small vessel security, but more remains to be done to provide effective guidance and programs to address small vessel threats and the potential impact these threats could have on our nation's ports and trade operations. DHS should address all the desirable characteristics and elements of an effective national strategy in its Small Vessel Security Strategy and implementation plan and it should evaluate the effectiveness of programs intended to support small vessel security before including them as part of a solution to improve security against the small vessel threats.

Additionally, one of the most significant challenges that remain is CBP's efforts to implement Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which requires DHS to screen all cargo headed for the United States that is loaded on or after July 1, 2012. To meet the goal of 100% screening, CBP has implemented the Secure Freight Initiative to screen 100% of cargo from select ports. However, there are

---

[45] DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*, (OIG-10-01, October 2009).
[46] DHS-OIG, *DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement, (*OIG-09-100, September 2009).

31

numerous challenges that remain before this can be implemented for all cargo inbound to the U.S. Chief among these challenges is obtaining international agreements for 100% scanning and working with the international community to resolve issues concerning resources, costs, timing, and enforcement considerations.

32

Appendix A
Report Distribution

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

33

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please 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

The Reports Consolidation Act of 2000 requires that, annually, the Office of Inspector General (OIG) prepare a statement summarizing the most serious management and performance challenges facing the Department and an assessment of the Department's progress in addressing those challenges. For FY 2009, the OIG considers the following to be the most serious challenges:

- Acquisition Management;
- Information Technology Management;
- Emergency Management;
- Grants Management;
- Financial Management;
- Infrastructure Protection;
- Border Security;
- Transportation Security; and
- Trade Operations and Security.

In addition to the OIG report, the Government Accountability Office (GAO) identifies in a High-Risk Series report, those 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 economic, efficiency, or effectiveness challenges. The GAO maintains these high-risk items until satisfied that acceptable corrective action progress has occurred. An update of the High-Risk Series is provided by GAO at the start of each new Congress. The most recent update is GAO-09-271, dated January 22, 2009. The areas that fall within the Department's purview and the year the issue was identified are listed below.

- Implementing and Transforming the Department of Homeland Security (2003);
- National Flood Insurance Program (2006);
- Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructure (1997); and
- Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security (2005).

The Department carries out multiple complex and highly diverse missions. Although the Department continually strives to improve the efficiency and effectiveness of its programs and operations, the areas identified above merit a higher level of focus and attention. Typically, overcoming challenges in these areas require long-term strategies for ensuring stable operations, sustained management attention, and resources.

The remainder of this section of the report details the Department's efforts in addressing each of the OIG challenges in FY 2009 and the plans it has in place to overcome these significant issues. The Department has published its plans to address the GAO High-Risk Series separately, and this information can be found at http://www.dhs.gov/xabout/budget/gc_1214229806734.shtm.

Challenge #1: Acquisition Management

DHS relies on goods and services contractors to help fulfill many of its critical mission areas. As such, effective acquisition management is vital to achieving DHS's overall mission. A successful acquisition process depends on appropriate placement of the acquisition function and strong executive leadership, policies and processes that establish effective internal controls, investment in people, and systems that track key acquisition data.

Organizational Alignment, Leadership, and Policies and Processes

FY 2009 Accomplishments

In November 2008, DHS released an interim acquisition management directive and associated guidebook (Directive 102-01). The interim directive established a revised acquisition review process, including roles and responsibilities of DHS-approving authorities, threshold levels for acquisition, acquisition decision events, and required supporting documentation. The directive established the Acquisition Review Board (ARB) as the Department's highest review body charged with reviewing and approving all programs at key acquisition decision events that are greater than $300 million in life cycle costs. In FY 2009, the Deputy Secretary chaired 16 major ARBs; the USM chaired 4 major ARBs and 8 mini-ARBs to allow oversight of *American Recovery and Reinvestment Act (ARRA) of 2009* initiatives; while the CPO chaired 2 service contract ARBs. The Department completed seven portfolio reviews, which augment the ARB process by providing executive-level governance support to Component and Departmental leadership. A co-signed memo report is issued by the Under Secretary for Management and the Component Head on the state of the portfolio.

On May 6, 2009, the Under Secretary for Management approved the implementation phase for the next Generation Periodic Reporting System (nPRS). After a rigorous data cleansing effort, nPRS successfully met the requirements established under the implementation phase.

Initiatives Underway and Planned

nPRS was designated operational as of October 1, 2009, as the Department's system of record for acquisition management data and reporting for all acquisition programs. Commencing October 2009, nPRS data will inform leadership in the major acquisition decision-making process.

Publish a revision to Directive 102-01. Complete an aggressive ARB schedule and continue Component Portfolio Reviews. Stand up a Logistics Working Group. Continue Phase 2 of the Transformation and Systems Consolidation (TASC) initiative. Conduct a Program Management Office Staffing Study.

Acquisition Workforce

FY 2009 Accomplishments

In FY 2009, DHS successfully: hired and placed 52 participants in the Acquisition Professional Career Program, for a total of 100 participants; increased the size of the contracting and procurement workforce, experiencing a net gain of 129 contracting professionals (from 1,152 in FY 2008 to 1,281 in FY 2009); increased the number of Program Manager certifications (all levels) issued by 694 (from 1,083 through FY 2008 to 1,777 through FY 2009); and increased the number

of Contracting Officers Technical Representative (COTR) certifications (all levels) issued by 2,116 (from 6,243 to 8,359).

In addition to the courses received from the Federal Acquisition Institute and the Defense Acquisition University, the DHS centralized acquisition training program provided 42 separate course titles, 293 course offerings, with 7,900 slots.

Initiatives Underway and Planned
Continue to build the acquisition intern program by 100 full-time equivalents (from 100 to 200). Expand the DHS acquisition training program to 8,500 slots. Assist the Component acquisition offices in filling existing vacancies through centralized, targeted recruitment efforts.

Knowledge Management and Information Systems

FY 2009 Accomplishments
The DHS Office of the Chief Procurement Officer (OCPO) participated as part of the technical evaluation team for the TASC initiative. DHS OCPO implemented the Enterprise Procurement Information Center, a collaboration and knowledge management tool that allows for HQ personnel to build team and project sites, share documents, calendars, etc. DHS migrated from the National Institutes of Health's Contractor Performance System (CPS) to DOD's Contractor Performance Assessment Reporting System (CPARS) to increase functionality and metrics.

Initiatives Underway and Planned
DHS OCPO initiated a project to develop a Procurement Enterprise Reporting Application (ERA) that provides near real-time access to procurement data allowing for the consolidation, analysis, and review of the data from the disparate contract writing systems and Federal Procurement Data System-Next Generation (FPDS-NG) from across the DHS components. This effort will consolidate procurement data into a repository allowing for better reporting and performance measurement. The OCPO initiated a data integrity project that proactively checks FPDS-NG data for anomalies. Once anomalies are identified, Components will take action to correct. This effort will improve overall data integrity.

Challenge #2: Information Technology Management

Creating a unified information technology (IT) infrastructure for effective integration and agency-wide management of IT assets and programs remains a challenge for the DHS Chief Information Officer (CIO). The CIO's successful management of IT across the Department will require the implementation of strong IT security controls, coordination of planning and investment activities across DHS Components, and a commitment to ensuring privacy.

Security of IT Infrastructure

FY 2009 Accomplishments
DHS achieved 96 percent Federal Information Security Management Act (FISMA) compliance at the Department level for FY 2009. This includes 93 percent compliance for Certification and Accreditation and tracking and managing the closure of approximately 10,000 security weaknesses. Near real-time visibility was implemented for Security Metrics, as well as daily delivery of

Information Security FISMA Reports to Components, resulting in more effective and timely management of more than 9,700 information security weaknesses.

The Department established Focused Operations forensic efforts to identify the sources and methods of the most serious attacks against the Department, and enabled DHS to counter current attacks and protect against future attacks. OCIO provided comprehensive classified threat and incident briefs to DHS management, resulting in the support necessary for needed changes in systems and user activities.

The Department continues to partner with components to strengthen and unify its information security program and now has an enterprise defense in depth strategy that includes:

- Perimeter controls (Trusted Internet Connections with Einstein);
- Network controls (Trust Zones—scheduled for FY 2010);
- Access Controls—Homeland Security Presidential Directive (HSPD)-12 implementation, to include logical access;
- Enhanced Datacenter security controls; and
- System-level controls (FISMA Scorecard activities).

DHS has completed its IT Security 5-year Strategic Plan with enterprise security as one of its core tenets. The four major priorities are: Strengthen IT Security Governance Framework; Improve Compliance Activities; Embrace Enterprise Services; and Enhance Business Acumen and Resource allocation. This plan expands beyond FISMA compliance to embrace enterprise services and improved business processes for developing and delivering enterprise security for the Department's mission technology.

DHS HQ has implemented a Privileged Account Request process in which all administrators must submit a formalized request to the Security Division providing a validated business justification for needing the privileged access. If approved, the privileged access is granted for a period of one year at which point the business justification must be reviewed, vetted, and approved again.

DHS HQ has performed a system wide audit of patch levels and recently invited cleared Microsoft Subject Matter experts in to perform an independent review of patch levels as well as provide recommendations on improving patch saturation. Their review was completed in August 2009. Machines that were identified as lacking proper patch levels were immediately mitigated, recommendations to improve patch management process were identified and projects to implement those recommendations were established. Those projects are projected to be completed by November 11, 2009.

Initiatives Underway and Planned

During FY 2010, DHS will execute the first phase of its IT Security 5-year Strategic Plan to emphasize the use of improved governance and communications to mature the DHS information security program into a cohesive, coordinated, Department-wide "Team Security" program.

IT Management

FY 2009 Accomplishments

The DHS OCIO developed a staffing plan to strengthen the CIO's role for centralized management of IT by providing greater authority and responsibility for overseeing the OCIO's IT acquisitions and address the OCIO's personnel requirements critical to enabling DHS to conduct its operations and deliver service to its customers. The major change resulting from this program change is to shift work from contract employees to Federal employees, with a large portion of employee's responsibilities focused on the performance of contractor management and program oversight.

The DHS OCIO, through the IT Infrastructure Transformation Program, is working to integrate the legacy IT infrastructures of all Components to achieve "One Infrastructure," which includes One Net efforts. The OCIO completed major large-scale migrations with four legacy data centers to the two new DHS Enterprise Data Centers, resulting in increased security and reduction of overall costs. In addition, the OCIO transitioned more than 66 percent of Component network sites under central network management as part of the network consolidation initiative in support of "One Infrastructure."

The DHS IT governance structure establishes the processes that govern and integrate acquisition, capital planning and budgeting, Enterprise Architecture compliance, and portfolio and program management efforts. This initiative focuses on documenting performance measures for key IT initiatives, highlighted in the DHS IT Strategic Plan FY 2009–2013. A long-standing, mature capability of the OCIO is the process whereby Components, DHS OCIO Divisions, and ultimately the DHS CIO review investments, systems, and technologies for alignment to the Department's architecture and identify duplications and deficiencies.

Initiatives Underway and Planned

During the first quarter of FY 2010, the DHS CIO is initiating a series of IT program reviews that will focus on the Department's Major Programs in an effort to improve IT program performance and mature program management capabilities. During FY 2010, DHS will further define its Segment Architectures through coordination with Components to better evolve its governance model. DHS intends to continue its efforts on the Infrastructure Transformation Program and aggressively pursue legacy Data Center consolidation into the two DHS Data Centers.

Privacy

FY 2009 Accomplishments

The OIG reported that TSA designated the Office of Privacy Policy and Compliance to oversee its privacy functions, and that TSA implemented a framework that promotes a privacy culture and complies with Federal privacy laws and regulations.

The OCIO continued to strengthen the information security governance framework. In coordination with the DHS Privacy office, the OCIO is continuing to assess and update its policy, security architecture, and technical standards, and is developing a workflow to address external service providers, such as third party social media websites.

Initiatives Underway and Planned

DHS efforts to improve compliance activities by monitoring emerging laws, mandates, and regulations and updating compliance activities reflect the strong link between security and privacy.

One of DHS's priorities is to comply with Federal mandates—the measurement of success is the percentage of privacy mandates complied, including the percentage of laptops and removable media with encrypted hard drives. This priority includes monitoring and developing strategies to address emerging mandates, including privacy and 508 compliance.

DHS is providing tools that enhance service delivery to CISO stakeholders. The initiative is to gather requirements from key stakeholders (e.g., Components, Privacy, CFO, Section 508, Budget/Acquisitions, Security Operations, Architecture, or OIG) on improving tool capabilities within the Department.

Challenge #3: Emergency Management

FEMA's mission is to support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. The *Post-Katrina Emergency Management Reform Act of 2006* gave FEMA primary responsibility for the four phases of comprehensive emergency management: preparedness, response, recovery, and mitigation.

In June 2009, the OIG reported that FEMA's response to Hurricane Ike was well-organized and effective.

The OIG provided a scorecard which highlighted FEMA's progress in three key areas: 1) disaster sourcing rated moderate progress, 2) housing rated modest progress, and 3) mitigation rated modest progress. Progress in these three areas combined with progress made in acquisition management and disaster grants management earned FEMA a moderate overall progress score for Emergency Management.

Disaster Sourcing

The Joint Field Office Operations Section has the responsibility of reviewing, approving, or denying official requests for assistance from the affected state(s), in collaboration with the Unified Coordination Group consisting of the Federal Coordinating Officer, State Coordinating Officer, and other advisors.

FY 2009 Accomplishments

Immediately after the OIG Sourcing Audit Report, in May 2009, a Single Point Ordering Working Group was established. This group was comprised of all major program areas including operations, logistics, finance, acquisition, and human capital. The group documented critical business processes related to Single Point Ordering. In collaboration with the FEMA Emergency Management Institute, FEMA convened a Single Point Ordering Focus Group of subject matter experts from August 31 to September 3, 2009. This Focus Group further documented business processes, began development of automated system requirements, and wrote a draft field operating guide. A pilot orientation and training course was conducted September 14–18, 2009, to further define the necessary field operating procedures.

Initiatives Underway and Planned

FEMA recently awarded the Logistics Supply Chain Management Systems contract that will include the Single Point Ordering requirements and permanent enterprise solution. In collaboration

with the FEMA Emergency Management Institute, FEMA will award a training support contract not later than December 31, 2009. Initial field implementation is planned for late FY 2010. FEMA has enlisted the assistance of the FEMA Chief Information Office and the DHS Science and Technology Directorate to help identify enterprise technology solutions. FEMA logistics also continues to collaborate with FEMA Disaster Operations in developing logistics support plans for the eight consolidated DHS disaster scenarios. These plans will help standardize operational and sourcing decisions during the onset of a disaster.

Housing

FY 2009 Accomplishments

FEMA released the 2009 Disaster Housing Plan. The plan serves as an operational bridge from the National Disaster Housing Strategy and describes the specific types of assistance that FEMA will provide to state, local, and tribal governments. The plan shows how to meet the housing needs of disaster survivors when Individual Assistance Programs are authorized under a presidentially declared disaster.

FEMA worked with the Centers for Disease Control (CDC) and DHS Office of Health Affairs (OHA) to write new specifications for temporary housing units that restrict high emitting construction materials and to develop a construction Indoor Air Quality standard that includes ventilation requirements that exceed industry standards. Specifically, the temporary housing unit manufacturer is required to appoint a third party Industrial Hygienist to conduct 100 percent air quality tests on each unit prior to acceptance by FEMA.

In April 2009, FEMA awarded four contracts for the manufacture of low emissions travel trailers with improved air exchange. These contracts may be extended for up to five years.

FEMA evaluates alternative housing units through the Joint Housing Solutions Group. This group completed an initial assessment of numerous candidate alternative units and awarded a contract for seven different models. Each vendor built and installed a prototype unit at the National Emergency Training Center in Emmitsburg, Maryland. These units are closely monitored and evaluated for quality and durability as students occupy these units throughout the year. A limited number of alternative units were installed and are occupied by displaced households in Galveston, Texas.

FEMA executed a rental repair pilot program for two disasters. This pilot provided funding for repairs to privately owned, multi-family complexes in exchange for use of the repaired units as temporary housing. In March 2009, FEMA issued a report to Congress evaluating the pilot program and offering recommendations for future implementation.

FEMA worked closely with the U.S. Department of Housing and Urban Development (HUD) to develop and implement a Disaster Housing Assistance Program pilot following Hurricanes Gustav and Ike. This pilot program leveraged the local public housing agencies and helped displaced, eligible applicants locate rental housing in and around the damaged communities.

Initiatives Underway and Planned

FEMA will continue to test new manufactured housing alternatives and work to identify housing innovations that will support the timely transition of disaster survivors into long-term housing.

The National Disaster Housing Task Force will continue to identify all forms of housing options in partnership with HUD, other Federal agencies, and state and local jurisdictions.

FEMA and HUD will continue to look for further partnering opportunities using the Disaster Housing Assistance Program collaboration as a model. Areas for continued improvement will include: 1) performance parameters and criteria for the provision of housing assistance and case management; 2) incentives for assisting applicants in finding housing quickly; 3) more detailed justification of program costs; and 4) clarification of program ownership throughout the registration process, eligibility reviews, and period of assistance.

Mitigation

Mitigation is the effort to reduce loss of life and property by lessening the impact of disasters. In the realm of emergency management, hazard mitigation falls into three broad categories: natural, technological, and manmade. Natural hazards are those generally associated with weather and geological events. Technological hazards include dams, gas lines, and chemical facilities. Manmade hazards are typically associated with a criminal or terrorist attack using devices such as an improvised explosive device, biological weapon, or chemical weapon. FEMA's Mitigation Directorate manages the National Flood Insurance Program. Other DHS Components have responsibility for mitigation of technological and manmade hazards.

FY 2009 Accomplishments

FEMA issued three clarification memoranda explaining the limits upon which the Agency can support reconstruction activities in V Zones under the current regulations implementing Executive Order 11988. The memoranda issued in June 2009 addressed reconstruction activities in V Zones supported by FEMA's Public Assistance Grant Program and Hazard Mitigation Grant Program.

FEMA piloted a basic Executive Order 11988 implementation course on June 2009. The course included materials and policy explanations on FEMA's restrictions on the V Zone. The instruction presented an explanation of why FEMA allowed flood insurance in these areas but does not allow Federal grants to be used for new construction in V Zones.

Initiatives Underway and Planned

On October 1, 2009, FEMA implemented the provision that properties on leased Federal lands now must pay actuarial insurance rates. FEMA worked with the Army Corps of Engineers to establish a list of its leased properties and will see that this list is kept current. Many of these properties have flooded multiple times.

FEMA implemented rate and rule changes effective October 1, 2009, that increased subsidized premiums 9.7 percent. Since Hurricane Katrina, FEMA has increased premiums for subsidized policyholders a cumulative 34 percent. FEMA plans to continue to reduce the amount of subsidy in these rates through additional periodic future rate increases.

FEMA is drafting the needed regulations to expand increased cost of compliance coverage to all qualifying FEMA mitigation grant programs. In acknowledgement of the administrative complexity and fiscal solvency implications of implementing this change for all properties at once, FEMA is pursuing a graduated approach to extending initial increased cost of compliance coverage to certain properties and/or programs.

FEMA is working on, and expects to finalize in the Fall of 2009, a strategy to address Executive Order 11988. Implementation of this strategy will begin shortly thereafter. This strategy includes measures to address the OIG report and other implementation issues in this area, including regulatory revisions, training, outreach, policy development, and human capital needs for the adequate evaluation of projects in light of the Executive Order 11988 requirements.

FEMA believes, however, that providing flood insurance in V Zones increases the effectiveness of floodplain management. Without the availability of flood insurance, the effective enforcement of floodplain building codes in V Zones could be expected to deteriorate, placing individuals and property at greater risk. Any new construction is required to be built in compliance with those ordinances and is charged premiums that fully reflect their long-term risk of flooding. For the occasional building that is built in noncompliance, its full-risk premium is quite substantial—in some cases exceeding $10,000 per year.

Program reform legislation will be required to solve the issue of repetitive loss properties outpacing mitigation properties by ten to one. As the NFIP program is currently set up in statute, management cannot resolve this problem.

Challenge #4: Grants Management

FY 2009 Accomplishments

FEMA formed an Intra-Agency Grants Program Task Force that has developed a FEMA Grants Strategy to drive future enhancements in grants policies, procedures, systems, and processes.

The Grant Development and Administration Division added six additional staff to manage the growing number of grants. The Division expanded the use of an existing Access database monitoring tool, developed a monitoring protocol, and conducted a pilot program of monitoring visits with transit and port grantees.

FEMA conducted 22 state and 32 urban area on-site monitoring visits. The Assistance to Firefighters Grant staff conducted 295 monitoring visits. A full-time equivalent was added to develop monitoring protocols and procedures for preparedness grants.

Initiatives Underway and Planned

Fully staff the Transportation Infrastructure Security Branch. Develop a monitoring module for a single, comprehensive non-disaster grants system.

Challenge # 5: Financial Management

FY 2009 Accomplishments

The DHS Financial Management Community has many initiatives underway to continue to build the 'One DHS' culture, including our commitment to strengthening internal controls and realigning business processes for improved efficiencies and effectiveness. We value our partnership with the Office of Inspector General in implementing the *Department of Homeland Security Financial Accountability Act*. With the passage of the Act, we launched an ambitious multi-year effort to improve financial management and reporting and build assurances that internal controls are in place and working effectively. DHS has worked to standardize business practices and to execute systematic plans to correct recognized weaknesses. In FY 2009, the Independent Auditor

performed the Department's first ever integrated financial statement and internal control audit. In addition, standalone financial statement audits were expanded to five DHS Components: CBP, USCIS, FLETC, ICE, and TSA. Although these audits indicate that DHS still faces serious financial management challenges, for the third consecutive year the Department has made progress by implementing effective corrective actions, as evidenced by the following achievements:

- DHS established financial reporting working groups to uniformly address financial management and business process challenges. In addition, DHS improved a "Component Requirements Guide" that contains approximately 40 standard financial reporting processes.
- DHS is moving forward with a financial system modernization effort. This will greatly improve the quality of and control over DHS financial data, make the financial accounting process more efficient throughout DHS, and reinforce standard business and financial management practices.
- DHS issued the Financial Management Policy Manual, which is designed to ensure DHS maintains efficient and transparent operations and our resources are not vulnerable to waste, fraud, and mismanagement.
- DHS and Components completed the Department's multi-year plan to implement OMB Circular No. A-123, *Managements Responsibility for Internal Control*, reducing the number of Component conditions that contributed to our material weaknesses in internal controls over financial reporting by more than half. In addition, we completed an assessment of processes that provide internal control over the Balance Sheet and Statement of Custodial Activity.
- DHS achieved compliance with the *Improper Payments Information Act, Debt Collection Improvement Act*, and *Government Performance and Results Act*.
- DHS provided training for all new employees in the DHS financial management community. This program welcomes new employees into DHS, provides a comprehensive introduction to financial management at DHS, and trains employees on a common set of core competencies, including the responsibilities of all financial managers to support and reinforce strong internal controls and the principles of fiscal law.
- The U.S. Coast Guard and FEMA maintained "Tone at the Top" and continued to make control environment progress and to implement corrective actions.
- The U.S. Coast Guard developed and implemented policies and procedures and performed data validations to assert to the Department's Actuarial Pension Liabilities in the amount of $28.2 billion.
- FEMA and TSA determined auditable amounts to capitalize for internal use software projects, ensuring long-term sustainment for the overall process.
- USCIS developed, defined, and tested a Deferred Revenue measurement plan to correct a significant deficiency in internal control.
- FLETC, ICE, and S&T corrected deficiencies that contributed to the Department's Actuarial and Other Liabilities material weakness condition.
- FEMA implemented corrective actions to reduced portions of the prior year Budgetary Accounting deficiencies.
- TSA implemented corrective actions to reduce the severity of the prior year Financial System Security deficiency condition.

Financial management has come a long way at DHS since its inception. We have established a culture of integrity, accountability, and excellence in all we do. This foundation supported the

transition of the new administration, and our success will continue to provide influential financial management leadership to support the Department's mission.

Initiatives Underway and Planned

Significant internal control challenges remain at U.S. Coast Guard, FEMA, TSA, CBP, and ICE. To support these Components, the Department's Chief Financial Officer will conduct recurring oversight meetings with senior management and staff. In addition, to ensure corrective action progress continues, DHS will:

- Analyze the structures of essential financial management offices and the skill sets of key financial management personnel to improve core competencies and implement internal controls.
- Expand the annual risk assessment to include identification of weaknesses in accounting and financial reporting, where problems are likely to occur due to changing operations and programs. In addition, DHS will use the results of the risk assessment to decide how to allocate resources and mitigate risks and what types of control activities and management involvement are needed.
- Improve information and communications related to roles and responsibilities of field and operational personnel to enable financial managers to carry out internal control and financial reporting responsibilities.

Continue efforts to implement a long-term financial management system modernization. In the interim, implement compensating controls designed to help ensure completeness, accuracy, authorization, and validity of financial transactions.

Challenge # 6: Infrastructure Protection

FY 2009 Accomplishments

In 2009 the Regional Resiliency Assessment Program conducted five pilot assessments to mitigate vulnerabilities in the Chicago Financial District, New York State Bridges, New Jersey Turnpike Exit 14 Chemical Corridor, Raleigh-Durham Research Triangle Area, and the Tennessee Valley Authority. Multi-Jurisdictional Improvised Explosive Device (IED) security plans were completed in Houston, Detroit, Oklahoma City, Norfolk, and Boston. An Evacuation Planning Guide for stadiums was prepared and field tested. The Dams sector developed a comprehensive framework and strategies document, "Roadmap to Secure Control Systems in the Dams Sector," for use in protecting industrial control systems.

Initiatives Underway and Planned

The Office for Bombing Prevention will begin work to implement a single sign-on feature between the FBI's Law Enforcement Online (LEO) portal and the DHS TRIP*wire* system. This information-sharing work will enhance the ability of the Nation to prevent explosive attacks. A Protective Measures Guide will be published for the U.S. Lodging Industry in FY 2010. DHS will perform compliance inspections at the highest risk chemical facilities. The security and protection of industrial control systems and cybersecurity in the Dams sector will be improved by implementation of the "Roadmap to Secure Control Systems in the Dams Sector."

Infrastructure Information Collection

FY 2009 Accomplishments
The Office of Infrastructure Protection (IP) developed the initial prototype Infrastructure Information Collection System (IICS) test and development system and capabilities, and subsequently reached initial operating capability. IP piloted the IICS prototype system with IP stakeholders and obtained feedback from critical IP stakeholders on the features, toolsets, and requirements that need to exist within the IICS for stakeholder needs to be met.

Initiatives Underway and Planned
IP will deploy the IICS Production system, allowing the respective entities to conduct critical infrastructure and key resources (CIKR) decision-making and reduce critical infrastructure risk management gaps. IP will identify and integrate additional relevant data sources in the system in an effort to continue to reduce critical infrastructure risk management and decision making gaps.

Protect the Cyber Infrastructure

FY 2009 Accomplishments
An Information Sharing Subgroup was formed under the auspices of the Industrial Control Systems Joint Working Group (ICSJWG) to address challenges associated with protecting sensitive and proprietary information. This subgroup developed a charter and is working with the CIKR sector community to develop a process for improving cybersecurity information sharing among control system stakeholders. The Control Systems Security Program completed 12 on-site assessments. The Protective Security Advisor (PSA) Program coordinated with the National Cyber Security Division (NCSD) to conduct 50 combined physical and cybersecurity vulnerability assessments across the United States. In addition, NCSD and the PSA Program collaborated to integrate general cybersecurity vulnerability assessment questions into a web-based tool. Inclusion of these cyber questions enables PSAs to collect basic cybersecurity data during Enhanced Critical Infrastructure Protection surveys which helps NCSD to determine whether a more comprehensive cybersecurity vulnerability assessment is needed.

Initiatives Underway and Planned
The Information Sharing Subgroup plans to develop a recommendations document to address gaps in current information sharing mechanisms.

Challenge # 7: Border Security

Internal Controls Over Contracting

FY 2009 Accomplishments
In response to agency requirements and in anticipation of program and contract growth, the SBI community has increased the number of trained COTRs. Currently CBP has trained and certified 47 COTRs: 33 COTRs are assigned to 31 active contracts and interagency agreements, and there are 14 unassigned COTRs available to accommodate future contract growth.

Other oversight tools are being employed to oversee SBInet contractors. For example, the Defense Contract Management Agency has been under contract to provide management oversight of the

SBInet contractor since 2008, and the Defense Contract Auditing Agency is under contract to review SBInet contractor costs and billing.

Initiatives Underway and Planned
An updated definition of inherently governmental functions is due from OMB in October 2009 per Congressional mandate. CBP and DHS will address the issue of roles and responsibilities of contractors and government employees based on the new definition.

To further ensure that inherently governmental functions are not performed by contractors, CBP will more fully distinguish between the roles and responsibilities of Federal employees and those of SBI contractors once a revised definition of inherently governmental functions is available from OMB.

Border Patrol Assessments

FY 2009 Accomplishments
CBP's Office of Border Patrol expanded its Analysis of Alternatives (AoA) methodology as a requirements gathering tool for all tactical infrastructure (TI) projects in direct compliance with the 2009 House Appropriations Bill. The analysis focuses on threats, vulnerabilities, and risks; solution alternatives are then recommended as requirements for CBP leadership approval. These validated requirements then become a set of TI requirements. The requirements become the basis, in part, for resourcing decisions and mission performance goals.

CBP developed a more standardized and methodological AoA evaluation matrix that was recently deployed, as well as a simple cost estimation tool designed to produce rough order of magnitude estimates for use in the AoA evaluation process.

Initiatives Underway and Planned
The Office of Border Patrol is developing a revised version of AoA that attempts to incorporate qualitative and quantitative analytical approaches in order to translate expert opinion into quantitative assessments of alternatives.

In 2010, OBP plans to incorporate AoA into the OBP Operational Requirements–Based Budgeting Program process for TI. OBP will develop new types of performance measures that provide better indicators of operational return on investment.

In the next few years, OBP plans to develop and provide an integrated enterprise framework for program, operational, and business analytics that would connect AoA, threat-based analysis, operational evaluations, and other types of enterprise analysis.

Rapid Response Facilities

FY 2009 Accomplishments
CBP's Facilities Management and Engineering (FM&E) leads an integrated projects team (IPT) that includes members from U.S. Army Corps of Engineers (USACE), General Services Administration (GSA), CBP's Office of Border Patrol, and other CBP support offices to provide high-level oversight, change control, and risk management through program completion. CBP FM&E is continuing to partner with USACE and GSA to complete the remaining rapid response projects.

CBP has an assigned FM&E project manager coupled with a USACE or GSA project manager to oversee the day-to-day management of each project through its completion.

By the end of CY 2009, CBP expects to have completed 47 (65 percent) of the 73 originally planned rapid response Border Patrol facilities projects.

Initiatives Underway and Planned
In addition to the IPT, FM&E is establishing improved information management and tracking capabilities. The tracking system used to report on the secure border fence activities is being adapted to incorporate tracking and reporting capabilities for Border Patrol facilities projects. FM&E is currently piloting the system using a subset of the major construction program to help define requirements for the system.

Border Patrol Vehicles

FY 2009 Accomplishments
CBP's Office of Border Patrol has completed the pilot implementation and testing of the Asset Works M5 software in two large sectors: San Diego and Tucson. This system is also referred to as the Vehicle Maintenance Information System (VMIS). To date, all Border Patrol vehicles have been loaded into VMIS. A training and implementation schedule has been developed for implementation of VMIS in all Southwest border sectors by January 2010.

Initiatives Underway and Planned
OBP Fleet Management is currently working with UNICOR to develop a process for all sectors to input commercial maintenance costs into VMIS. No training will be required for this implementation so the tracking of commercial maintenance costs will begin immediately. This process will provide almost complete implementation of VMIS for those Border Patrol sectors that do not have their own maintenance facilities or staff.

After full implementation, long-term use of VMIS will allow fleet managers to project vehicle replacement needs and to track and identify trends such as vehicle usage, fuel consumption, and maintenance costs within the large Border Patrol fleet.

Identities and Citizenship of All Air and Land Passengers Entering the United States

FY 2009 Accomplishments
The US-VISIT Program replaced 2-fingerprint capture devices at overseas consulates and U.S. ports of entry with new 10-fingerprint capture devices. The use of 10-fingerprint capture devices increases the likelihood of correctly identifying individuals—including persons of interest to DHS and law enforcement agencies and those individuals on US-VISIT watch lists.

Effective January 18, 2009, the Additional Aliens Rule took effect, expanding the scope of US-VISIT's biometric collection to include additional classes of aliens, including U.S. lawful permanent residents. The inclusion of these classes of aliens expands DHS's ability to establish and verify the identity of an individual.

Initiatives Underway and Planned
US-VISIT conducted an air exit pilot at two U.S. airports to test biometric collection during an individual's exit from the United States. The evaluation of this pilot is currently under review by

the Department. Once complete, the pilot evaluation is expected to provide the Secretary with findings relative to the potential Air/Sea Solution for Exit. DHS Plans to publish a final rule relative to Exit Biometric collection in the Air/Sea environment in 2010.

US-VISIT will seek to expand the biometric holdings that its customers can screen against through interoperability with the Department of Defense's Automated Biometric Identification System.

DHS will complete air and sea entry for all remaining areas where air and sea entry is not deployed (e.g., general aviation, small crafts, all cruise ships, and cargo). DHS is considering the most cost-effective option to address the need to record the departure of an alien in the air and sea environments as it pertains to immigration reform. The Exit pilot conducted in FY 2009 is expected to provide findings to inform a cost benefit analysis for this solution.

US-VISIT will work with the rest of the U.S. Government to implement Homeland Security Presidential Directive 24 to enhance biometric screening for known or suspected terrorists

Challenge # 8: Transportation Security

TSA is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. Since its inception, TSA has faced challenges with strengthening security for aviation, mass transit, and other modes of transportation. The OIG divided this challenge into three areas: 1) Checkpoint and Checked Baggage, 2) Passenger Air Cargo Security, and 3) Rail and Mass Transit. The OIG noted that TSA has made progress in addressing the challenges of improving training; equipment and technology; policy and procedures; and management and supervision. The OIG also noted that more needs to be done.

Checkpoint and Checked Baggage

FY 2009 Accomplishments

TSA developed the Screening Procedures for Armed Personnel training program. This training will be available to supervisory transportation security officers, law enforcement officers, and designated TSA representatives.

As of July 15, 2009, except under extraordinary conditions, TSA no longer accepts paper letters of authority for law enforcement officers flying while armed on commercial flights. State, local, territorial, and tribal law enforcement officers with a need to fly armed on commercial flights are required to pre-register their travel with TSA. These new procedures significantly enhance the verification process and provide TSA with situational awareness of the flying armed community.

An operational pilot tested five ID/credential/boarding pass verification systems.

The Office of Finance and Administration/Chief Financial Officer, through the Office of Property Management, has added a 14-item uniform management performance assessment to its annual inventory protocol conducted at TSA airport operations throughout the country. This process not only assesses the status of uniform control at airports on a routine basis but also offers opportunities for system improvements. Several aspects of uniform management are now being surveyed, including authorized personnel access controls, documentation practices, and internal controls.

Version 3 of the Asset Tracking Module (now called the Employee Uniform Tracking Module) was created, tested, and will soon be piloted. This module allows for a consistent user experience within the larger enterprise effort identified in the March 2009 TSA Update.

Initiatives Underway and Planned
In October 2009, Indianapolis International Airport became TSA's first airport to begin using the Uniform Tracking Module as the sole means of data collection and reporting.

Teaching the Screening Procedures for the Armed Personnel training program will begin in FY 2010.

TSA will leverage the requirement that all Federal employees have Personal Identity Verification (PIV) credentials. This long-term strategy supports secure, electronic, real-time identity verification and authentication. TSA plans to begin deployment of PIV reading systems using results from the FY 2009 operational pilot.

A new Management Directive is slated for release that will seek to ensure that badges are returned immediately upon an employee's separation from TSA. The directive details the collection, audit, reporting, and analysis of badging data.

Passenger Air Cargo Security

FY 2009 Accomplishments
TSA devised and implemented four special emphasis inspections which focused on the most common violations. TSA purchased cell phones whose numbers will periodically change. Previously, the phone numbers used were known to the tested entity, thereby compromising the covertness of the testing.

A National Investigation Enforcement Manual and a TSA Inspector Hand Book were drafted in FY 2009 and released in October 2009. These documents define baseline documentation requirements that must be met to be a known shipper. Four basic testing techniques (surveillance, interview, document review, and testing) are detailed. These documents were incorporated into TSA's inspector training program.

An on-the-job training program was formalized. This program links inspectors with certified instructors. Quarterly training webinars were offered to cargo inspectors. Recurring training now includes a dedicated session on the Known Shipper Program.

Initiatives Underway and Planned
TSA will continue to refine its testing program. Inspectors will be granted access early in FY 2010 to a Known Shipper Management System. Use of this system will become mandatory to vet a shipping location.

Rail and Mass Transit

FY 2009 Accomplishments
In FY 2009, more than 500 inspections of freight, passenger, and transit operators were conducted to determine compliance with rail security regulations issued in 2009. These regulations codified TSA's inspection authority in surface transportation and required regulated parties to establish

security coordinators, report significant security incidents to DHS, and develop specific procedures for the handling of rail sensitive-security materials. Additional, voluntary assessments were performed. An Assessment Tool database was developed to automate field data collection, processing, and reporting. Additional training was provided to surface inspectors and senior management on the database tool and accompanying new procedures.

TSA created six regional security inspectors to serve as senior-level liaisons to the rail industry and to provide leadership and oversight over the inspection process.

Initiatives Underway and Planned
TSA plans to widen the scope of the Assessment Tool to include underwater tunnels, train stations, freight rail corridors, and mass transit and passenger rail risk assessments.

TSA is developing a dedicated Surface Transportation Security Training Center in Pueblo, Colorado. The center will allow for the training of more field employees and managers and increase internal awareness of the mission of the surface inspectors.

TSA expects to issue a Notice of Proposed Rule-making that will require training for mass transit and passenger rail, freight rail, intercity bus, and motor carriers. Once these regulations are final, inspectors will monitor industry compliance.

Challenge #9: Trade Operations and Security

High Risk Shipments

FY 2009 Accomplishments
CBP is working with the developer of a biodetection device, and chemical and biological experts, to field and laboratory test a handheld biodetection device. Tests using simulants provided promising results for sensitive and reliable detection of biothreat agents in international passenger luggage and hand-carry packages, as well as in international mail and cargo.

Initiatives Underway and Planned
Field and laboratory testing of the biodetection device will continue, using a new model that is equipped with a sensor that can rapidly and reliably detect and identify specific biothreat agents. "Live" biothreat agents, as well as simulants, will be used in biocontainment facility testing to improve utility of the device for field testing and use in multiple environments. Future modifications of the biodetection device will focus on more sensitive detection capabilities in multiple field environments, lighter weight/more compact device construction, and expanded number of biothreat agents for detection. CBP also plans to deploy the biodetection device to the field for routine testing and use by front-line employees.

Risk Assessments

FY 2009 Accomplishments
CBP worked on developing new rule indicators in CBP's Automated Targeting System (ATS) for targeting cargo.

Initiatives Underway and Planned
CBP will continue to meet with other government agency subject matter experts to determine risk pathways related to biological and chemical weapons and determine rule and rule indicators to update ATS targeting of cargo for biological and chemical threats.

CBP will develop, test, and implement updated rules and a corresponding weight set in ATS to assist in targeting cargo shipments for these threats.

CBP will continue to maintain and update the rules and weight set for targeting cargo shipments that present the highest risk for biological and chemical weapons by analyzing targeted shipments and evaluating examination results in relation to the rules implemented in ATS.

Secure Freight Initiative

FY 2009 Accomplishments
CBP maintains Secure Freight Initiative operations in five ports. CBP anticipates the limited testing of the Secure Freight Initiative to the port of Salalah, Oman, in February 2010.

Acronym List

Acronym List

AC&I – Acquisition, Construction & Improvements
ADMP – Active Duty Military Payroll
AFG – Assistance to Firefighters Grants
AFR – Annual Financial Report
AoA – Analysis of Alternatives
ARB – Acquisition Review Board
ARRA – American Recovery and Reinvestment Act of 2009
ARTF – Aquatic Resources Trust Fund
ATS – Automated Targeting Systems
BPD – Bureau of Public Debt
B&SA – Bureau & Statistical Agent
C&A – Certification and Accreditation
CBP – U.S. Customs and Border Protection
CDC – Centers for Disease Control
CDL – Community Disaster Loan
CDSOA – Continued Dumping and Subsidy Offset Act
CFO – Chief Financial Officer
C.F.R. – Code of Federal Regulations
CIKR – Critical Infrastructure and Key Resources
CIO – Chief Information Officer
CISO – Chief Information Security Officer
COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985
COE – U.S. Army Corps of Engineers
COTR – Contract Officers Technical Representative
COTS – Commercial Off-the-Shelf
CPS – Contractor Performance System
CSI – Container Security Initiative
CSRS – Civil Service Retirement System
CY – Current Year
DADLP – Disaster Assistance Direct Loan Program
DCIA – Debt Collection Improvement Act
DHS – U.S. Department of Homeland Security
DHS FAA – Department of Homeland Security Financial Accountability Act
DNDO – Domestic Nuclear Detection Office
DOC – Department of Commerce
DOD – Department of Defense
DOI – Department of Interior
DOL – Department of Labor
DRO – Detention and Removal Operations
ECIP – Energy Conversation Investment Program
EDS – Explosive Detection System
EMI – Emergency Management Institute
ERA – Enterprise Reporting Application
ESCM – Entry Summary Compliance Measurement
ETD – Explosives Trace Detection
FAR – Federal Acquisition Regulation
FASAB – Federal Accounting Standards Advisory Board
FBwT – Fund Balance with the 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
FERS – Federal Employees Retirement System
FFMIA – Federal Financial Managers' Improvement Act
FIRA – Flood Insurance Reform Act
FISMA – Federal Information Security Management Act
FLETC – Federal Law Enforcement Training Center
FMA – Flood Mitigation Assistance
FM&E – Facilities Management and Engineering

FMFIA – Federal Managers' Financial Integrity Act
FMLoB – Financial Management Line of Business
FPDS-NG – Federal Procurement Data System-Next Generation
FPS – Federal Protective Service
FSIO – Financial Systems Integration Office
FY – Fiscal Year
GAAP – U.S. Generally Accepted Accounting Principles
GAO – Government Accountability Office
GSA – General Services Administration
HHS – Health and Human Services
HQ – Headquarters
HSA – Homeland Security Act of 2002
HSGP – Homeland Security Grant Program
HSPD – Homeland Security Presidential Directive
HUD – U.S. Department of Housing and Urban Development
ICCB – Internal Control Coordination Board
ICE – U.S. Immigration and Customs Enforcement
IDI – Injured Domestic Industries
IED – Improvised Explosive Device
IEFA – Immigration Examination Fee Account
IHP – Individuals and Household Programs
IICS – Infrastructure Information Collection System
INA – Immigration Nationality Act
IP – Improper Payment
IPIA – Improper Payments Information Act of 2002
IPT – Integrated Project Team
IT – Information Technology
LOI – Letters of Intent
MD&A – Management's Discussion and Analysis
MERHCF – Medicare-Eligible Retiree Health Care Fund
MGMT – Management Directorate
MRS – Military Retirement System
MTS – Metric Tracking System
NCSD – National Cyber Security Division
NEMIS – National Emergency Management Information System
NFIP – National Flood Insurance Program
NIMS – National Incident Management System
NPPD – National Protection and Programs Directorate
nPRS – Next Generation Periodic Reporting System
NSC – National Security Cutter
OCAO – Office of the Chief Administrative Officer
OCFO – Office of the Chief Financial Officer
OCIO – Office of the Chief Information Officer
OCPO – Office of the Chief Procurement Officer
OHA – Office of Health Affairs
OIG – Office of Inspector General
OMB – Office of Management and Budget
OM&S – Operating Materials and Supplies
OPEB – Other Post Retirement Benefits
OPM – Office of Personnel Management
ORB – Other Retirement Benefits
OTA – Other Transaction Agreements
PA – Public Assistance
PIV – Personal Identity Verification
P.L. – Public Law
PP&E – Property, Plant, and Equipment
PSA – Protective Security Advisor
PY – Prior Year
QHSR – Quadrennial Homeland Security Review
RDT&E – Research, Development, Test and Evaluation
RSSI – Required Supplementary Stewardship Information
SAT – Senior Assessment Team
SBI – Secure Border Initiative
SBR – Statement of Budgetary Resources

SFFAS – Statement of Federal Financial Accounting Standards
SMC – Senior Management Council
SFRBTF – Sport Fish Restoration Boating Trust Fund
S&T – Science and Technology Directorate
TASC – Transformation and Systems Consolidation
TAFS – Treasury Account Fund Symbol
TI – Tactical Infrastructure
TSA – Transportation Security Administration
USACE – U.S. Army Corps of Engineers
UAS – Unmanned Aerial System
U.S. – United States
U.S.C. – United States Code
USCG – U.S. Coast Guard
USCIS – U. S. Citizenship and Immigration Services
USM – Under Secretary of Management
USSS – U.S. Secret Service
US-VISIT – U.S. Visitor and Immigrant Status Indicator Technology
VMIS – Vehicle Maintenance Information System
WYO – Write Your Own

The *U.S. Department of Homeland Security FY 2009 Annual Financial Report* is available at the following website:
http://www.dhs.gov/xabout/budget/editorial_0430.shtm

For more information, contact:

Department of Homeland Security
Office of the Chief Financial Officer
Program Analysis and Evaluation
245 Murray Lane, SW
Mailstop 200
Washington, D.C. 20528

Information may also be requested by sending an email to par@dhs.gov or calling (202) 447-0333.

Homeland
Security