



## Other Accompanying Information

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

*Unaudited, see accompanying Auditors' Report*



## Tax Burden/Tax Gap

### *Revenue Gap*

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

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

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



## Summary of Financial Statement Audit and Management Assurances

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

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

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

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



**Table 2. FY 2011 Summary of Management Assurances**

Effectiveness of Internal Control Over Financial Reporting (FMFIA Section 2)						
Statement of Assurance	No Assurance					
Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Financial Reporting at USCG	1					1
Financial Systems at USCG and FEMA	1					1
Fund Balances with Treasury at USCG	1				✓	0
Property Management at USCG and TSA	1					1
Environmental and Other Liabilities at USCG	0	✓				1
Budgetary Resource Management at USCG	1					1
<b>Total Material Weaknesses</b>	<b>5</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>(1)</b>	<b>5</b>
Effectiveness of Internal Controls over Operations (FMFIA Section 2)						
Statement of Assurance	Qualified					
Material Weaknesses	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Property Management at DHS and TSA	1				✓	0
Financial Assistance Awards Policy and Oversight at DHS and FEMA	1					1
Acquisition Management at DHS	1					1
Funds Control at USCG, ICE, and USSS	1					1
Entity Level Controls at NPPD	0	✓				1
<b>Total Material Weaknesses</b>	<b>4</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>(1)</b>	<b>4</b>
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
<b>Total Non-conformances</b>	<b>3</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>3</b>
Compliance with Federal Financial Management Improvement Act (FFMIA)				DHS	Auditor	
<b>Overall Substantial Compliance</b>				No	No	
<b>1. System Requirements</b>					No	
<b>2. Accounting Standards</b>					No	
<b>3. USSGL at Transaction Level</b>					No	

In FY 2011, DHS renamed the previously reported Financial Reporting and Other Liabilities material weakness to better align with the title used by the Independent Auditors. As such, Environmental and Other Liabilities was added as a new title in FY 2011.

### *Effectiveness of Internal Control Over Financial Reporting*

Pursuant to the *Department of Homeland Security Financial Accountability Act (FAA)*, the Department has focused its efforts on evaluating corrective actions to assess whether previously reported material weaknesses continue to exist. In cases where material weaknesses continue to exist, the Department focused on identifying significant financial reporting areas where assurance can be provided and developed interim compensating measures to support the Secretary’s commitment to obtain a balance sheet opinion. Since FY 2005 DHS has reduced audit qualifications from 10 to 1 and material weaknesses by half. For the sixth consecutive year, we have made tremendous progress in strengthening Department-wide internal controls over financial reporting, as evidenced by the following FY 2011 achievements:

- The U.S. Coast Guard successfully executed the FY 2011 *Financial Strategy for Transformation and Audit Readiness*, providing financial reporting assertions to support the Department’s Consolidated Balance Sheet. In addition, U.S. Coast Guard corrective actions significantly reduced risk related to financial scripts and Fund Balance with Treasury



reconciliations. Most significantly, the U.S. Coast Guard corrected a longstanding entity level control deficiency based on the Commandant’s leadership to set the tone at the top and delegation of responsibility for internal control from senior management to all financial management staff levels and across business lines of the U.S. Coast Guard enterprise.

- The Offices of the Chief Financial Officer and Chief Information Security Officer partnered to provide direct assistance to Components in executing financial system security corrective actions and performing validation and verification procedures, resulting in a significant deficiency correction at FLETC, a material weakness downgrade at ICE, and substantial risk reductions of system security vulnerabilities at FEMA and scripting risks at U.S. Coast Guard.
- FEMA executed corrective actions to correct a Financial Reporting significant deficiency by implementing processes and controls to support account balances and adjustments, including improving financial disclosure procedures.
- CBP implemented corrective actions to correct a significant deficiency in budgetary accounting by implementing controls to improve the timeliness of undelivered orders deobligations.

Significant internal control challenges remain at the U.S. Coast Guard, FEMA, and TSA. To support these Components, the Department’s Deputy Chief Financial Officer conducts weekly risk management meetings with Senior Management and Staff. Table 3 below summarizes financial statement audit material weaknesses in internal controls as well as planned corrective actions with estimated target correction dates.

**Table 3. FY 2011 Internal Control Over Financial Reporting Corrective Actions**

Material Weakness	Component	Year Identified	Target Correction Date
	USCG	FY 2003	FY 2012
<b>Financial Reporting</b>	U.S. Coast Guard has not established an effective financial reporting process due to the lack of integrated financial processes and systems. In addition, significant deficiencies were identified at TSA, which contribute to the overall material weakness.		
<b>Corrective Actions</b>	The DHS OCFO will continue to support U.S. Coast Guard and TSA in implementing corrective actions to establish effective financial reporting control activities.		

Material Weakness	Component	Year Identified	Target Correction Date
	USCG and FEMA	FY 2003	FY 2012
<b>IT Controls and System Functionality</b>	The Department’s Independent Public Auditor has identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to inherited control deficiencies surrounding general computer and application controls. In addition, significant deficiencies were identified at CBP, ICE, and USCIS, which contribute to the overall material weakness. The <i>Federal Information Security Management Act</i> mandates that federal agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance. In addition, the Department’s financial systems do not conform to the <i>Federal Financial Management Improvement Act</i> .		



<b>Corrective Actions</b>	The DHS OCFO and OCIO will support the U.S. Coast Guard, FEMA, and other Components to design and implement internal controls in accordance with DHS 4300A, Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Financial Systems. In addition, the Department will continue to move forward with financial system modernization.
---------------------------	---

Material Weakness	Component	Year Identified	Target Correction Date
	USCG and TSA	FY 2003	FY 2012
<b>Property, Plant, and Equipment</b>	The controls and related processes surrounding U.S. Coast Guard and TSA Property, Plant, and Equipment (PP&E) to accurately and consistently record activity are either not in place or contain errors and omissions. In addition, significant deficiencies were identified at CBP and MGMT, which contribute to the overall material weakness.		
<b>Corrective Actions</b>	U.S. Coast Guard will implement policies and procedures to support completeness, existence, and valuation assertions for PP&E. The DHS OCFO will continue efforts to support U.S. Coast Guard and TSA implementing corrective actions to address capital asset conditions and develop policies and procedures to establish effective financial reporting control activities.		

Material Weakness	Component	Year Identified	Target Correction Date
	USCG	FY 2006	FY 2012
<b>Environmental and Other Liabilities</b>	U.S. Coast Guard did not have policies and procedures to fully support the completeness, existence, and accuracy assertions of data used in developing environmental liability estimates.		
<b>Corrective Actions</b>	Corrective actions for environmental liabilities will be taken in coordination with PP&E corrective actions to develop a complete population of locations where environmental liabilities exist.		

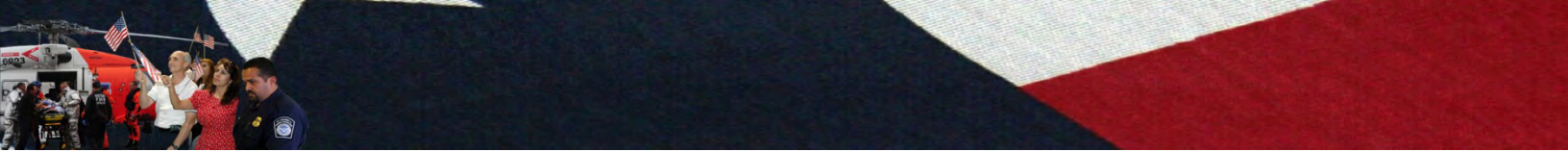
Material Weakness	Component	Year Identified	Target Correction Date
	USCG	FY 2004	FY 2012
<b>Budget Resource Management</b>	U.S. Coast Guard policies and procedures over obligations, disbursements, and validation and verification of undelivered orders for accurate recording of accounts payable were not effective. In addition, significant deficiencies were identified at CBP and FEMA, which contribute to the overall material weakness.		
<b>Corrective Actions</b>	Use lessons learned in FY 2011 from the Audit Command Language to develop corrective actions for budgetary accounts.		



## *Effectiveness of Internal Control Over Operations*

The DHS Management Directorate is dedicated to ensuring that Departmental offices and Components perform as an integrated and cohesive organization, focused on the Department's frontline operations to lead efforts to achieve a safe, secure, and resilient homeland. Critical to this mission is a strong internal control structure. As we strengthen and unify DHS operations and management, we will continually assess and evaluate internal controls to ensure the effectiveness and efficiency of operations and compliance with laws and regulations. For the sixth consecutive year, we have made tremendous progress in strengthening Department-wide internal controls over operations, as evidenced by the following FY 2011 achievements:

- Supported the Deputy Secretary with the “Improving the Health of DHS Financial Assistance” initiative to establish a unified financial assistance line of business. An Executive Steering Committee was also established to create five working groups to improve audits and assessments, program development and implementation, programmatic goals and objectives, reporting and post-award administration, and financial assistance program requirements.
- Strengthened internal controls over government charge cards by establishing a Bankcard Assessment Team to prevent waste, fraud, and abuse of resources. The Bankcard Assessment Team implemented and actively monitored the effectiveness of these controls to ensure government charge card programs and operations are instilled with the highest level of integrity and accountability. Internal control assessments are currently under way to baseline government charge card processes and controls. These assessments will help to better define the roles and responsibilities of cardholders, program officials, management, and those charged with coordinating charge card activities.
- Received a grade of “A” from the Small Business Administration for our success in contract awards. Achieved a competition rate of 67 percent, exceeding the goal of 60 percent. Conducted oversight reviews at three Components as well as six DHS-wide special reviews and three Component-specific special reviews, resulting in performance improvement opportunities and identification of best practices. Updated the Homeland Security Acquisition Manual to reflect new regulatory and policy requirements.
- Graduated 30 contracting employees from the Acquisition Professional Career Program, resulting in 191 active employees in the Acquisition Professional Career Program as of September 30, 2011. There were 3,020 acquisition certifications issued and 6,734 individuals trained across 319 classes in 61 different acquisition courses.
- Conducted in-depth technical reviews for 20 percent of the Department's IT systems to assess quality assurance and validate compliance with DHS security requirements. The Office of the Chief Information Security Office conducts rotating assessments over a five year schedule to achieve 100 percent coverage of the Department's IT systems.
- Increased the level of IT program and portfolio governance across the Department by establishing seven program Executive Steering Committees (ESCs) and five Domain ESCs, executing annual Portfolio Reviews in support of the OCFO FY 2013 Program Review Board, and conducting four Departmental TechStat reviews and 25 Accelerated TechStats in support of OMB's 25 Point Plan.
- Migrated the Email Security Gateway to each DHS enterprise data center and discontinued Directory Services Exchange Services at the Operations Support Center in Martinsburg, West Virginia.



- Achieved internal control program efficiencies by leveraging enterprise-wide business processes documentation project that was initiated and completed in FY 2011 and led by the Chief Administrative Officer's Records Management Program Division.
- Made substantial improvements to Office of the Chief Administrative Officer (OCAO)-wide communications and information delivery processes through the development and implementation of a comprehensive website plan. In addition, the OCAO successfully established improved communications across DHS-wide Administrative Service groups.
- Successfully implemented five out of seven of the President's Hiring Reform Initiatives and will continue to simplify the hiring process to increase efficiencies and increase the quality of candidates. Training of hiring managers is a significant element of the DHS hiring reform action plan, and we will continue to train, engage, and hold all hiring managers accountable for the effective and efficient hiring of talented individuals.
- Coordinated a collaborative process to develop a new DHS Coordinated Recruiting and Outreach Strategy, which is currently in the review process. This streamlined approach will leverage recruiting assets from around the country and will strengthen the unity of the DHS brand. Moreover, recruiting efforts will target all underrepresented groups, including individuals with disabilities and veterans.
- Developed a comprehensive Leader Development framework relevant for all levels of employees. For example, the Cornerstone program, a top priority for the Deputy Secretary, provides a single framework of requirements for the development of some 27,000 supervisors across the Department, and encompasses pre-supervisory awareness, supervisor onboarding, 40 hours of development during the first 11 months of appointment, and an annual requirement to give back 12 hours in "leader as teacher" activity.
- Surpassed the target of 3,500 contractor conversions through Balanced Workforce Strategy activity and launched a related Strategic Workforce Planning model. Elements of the new model include: revalidated Mission Critical Occupations (MCOs) aligned with each major DHS mission articulated in the Quadrennial Homeland Security Review (QHSR); a prototype of human capital indicators linked to MCOs, to be piloted and evaluated in FY 2012 as a means for assessing basic risk to mission accomplishment; and a general framework for validating and measuring competencies for the Department's MCOs, which will be evaluated and implemented in FY 2012.
- The DHS HSPD-12 Program, under the direction of the Office of the Chief Security Officer, has fostered greater collaboration and opportunities for improving how DHS handles employee identification information through all business processes. Accomplishments included: issuing a cumulative total of 262,881 Personal Identity Verification cards to DHS employees and contractors and deploying Personal Identity Verification card issuance workstations to more than 650 DHS locations in support of card issuance surge activities.

To address challenges to internal control over operations, the Department's Under Secretary for Management conducts quarterly Internal Progress Review oversight meetings. Table 4 summarizes material weaknesses in internal control over operations as well as planned corrective actions with estimated target correction dates.





**Table 4. FY 2011 Internal Control Over Operations Corrective Actions**

Material Weakness	Component	Year Identified	Target Correction Date
	DHS and FEMA	FY 2008	FY 2014
<b>Financial Assistance Awards Policy and Oversight</b>	There are four basic conditions affecting stewardship of federal assistance funding across DHS: (1) the lack of published department-wide financial assistance policy to guide Components' and Awardees' actions; (2) the lack of Component oversight and monitoring to ensure their adherence to such policy; (3) the lack of Office of the Inspector General and DHS Management actions to resolve and close annual awardee audit findings; and (4) the lack of basic information regarding how DHS goes about conducting its financial assistance line of business, including identification of high areas of risk and gaps in key controls; in established areas of responsibility, business models; and systems and efficient and effective operations.		
<b>Corrective Actions</b>	The Deputy Secretary has formed an Executive Steering Committee to oversee corrective actions with audits and assessments, program development and implementation, programmatic goals and objectives, reporting and post-award administration, and requirements for financial assistance programs.		

Material Weakness	Component	Year Identified	Target Correction Date
	DHS	FY 2008	FY 2012
<b>Acquisition Management</b>	There are six conditions affecting acquisition management at DHS: (1) inability to effectively achieve proper organizational alignment from achieving mission; (2) systems oversight and accountability within the acquisition function which has improved, but is still not sufficient; (3) investment decision models need to be strengthened to better manage risks to ensure programs meet needed mission capabilities and are delivered within cost, benefit, and schedule considerations; (4) program cost growth and the inadequacy of the cost-estimating process at DHS; (5) gaps identified in an acquisition workforce survey; and (6) use of suspension and debarment actions for poorly performing contractors.		
<b>Corrective Actions</b>	To improve organizational alignment, DHS developed a Management Directive that recognizes the Under Secretary for Management as the Chief Acquisition Officer. In addition, DHS is working to improve the effectiveness of the acquisition lifecycle and provide better linkages between requirements development, resource allocation, procurement, and program management, with S&T as a full partner to the Management Directorate. S&T will continue to play a key role in each phase of the acquisition life cycle, especially in the earliest phases of concept development through program execution. S&T will evaluate new and emerging technologies to address capability gaps, which ultimately enhances department-wide technology expertise and assists the department in making better technology decisions.		



Material Weakness	Component	Year Identified	Target Correction Date
		USCG, ICE, and USSS	FY 2006
<b>Funds Control</b>	U.S. Coast Guard repeated the prior year Antideficiency Act (ADA) controls material weakness. ICE made progress against prior-year conditions by developing an Administrative Control of Funds Directive; however, additional work is needed to implement the Directive across ICE program offices. Finally, USSS has not completely implemented funds control policies and procedures to address prior-year ADA violations reported by GAO.		
<b>Corrective Actions</b>	U.S. Coast Guard is developing enterprise-wide policies and procedures for assessing ADA risks, testing effectiveness of controls, and monitoring to fully implement DHS policy. ICE plans to conduct verification and validation procedures to ensure their Administrative Control of Funds Directive is effectively implemented. USSS will complete implementation of policies and procedures regarding the administrative control of funds.		

Material Weakness	Component	Year Identified	Target Correction Date
		NPPD	FY 2011
<b>Entity Level Control at NPPD</b>	NPPD has recently undergone major organizational change with new responsibilities, reorganization, and expansion of programs. NPPD Component management does not always address indicators of problems or manage risks to ensure top management is aware of actions taken or needed at components of the NPPD organization. The organization structure is inefficient, and it is difficult to determine the organizations or individuals that control parts of NPPD management functions.		
<b>Corrective Actions</b>	NPPD will implement corrective actions to improve its control environment.		



## Improper Payments Information Act

The *Improper Payments Information Act (IPIA) of 2002* (Pub. L. 107-300) requires agencies to review their programs and activities to identify those susceptible to significant improper payments. The IPIA was amended on July 22, 2010, by the *Improper Payments Elimination and Recovery Act (IPERA) of 2010* (Pub. L. 111-204). IPERA strengthened the requirement for government agencies to carry out cost-effective programs for identifying and recovering overpayments made to contractors, also known as “recovery auditing.” OMB has established specific reporting requirements for agencies with programs that possess a significant risk of improper payments and for reporting on the results of recovery auditing activities. As noted below, DHS will implement corrective action plans for all programs with estimated improper error amounts above \$10 million. Key achievements for FY 2011 include: a reduction in estimated improper payments for FEMA’s high-risk programs; targeted recovery audit contract work examining telecommunications payments, which identified significant improper payments eligible for recoupment and cost savings opportunities; and a 94 percent cumulative recoupment rate for high-dollar overpayments identified in the Secretary’s quarterly report to the DHS OIG, OMB, and the public. In the tables which follow, all table amounts are rounded to the nearest whole dollar.

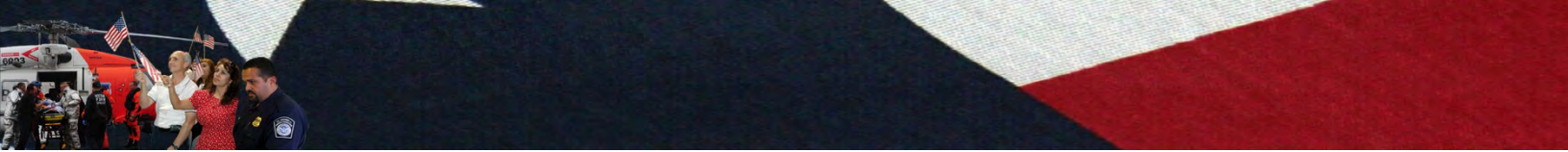
### I. Risk Assessments

In FY 2011, DHS conducted risk assessments on 96 DHS programs, totaling \$53 billion in FY 2010 disbursements. We completed risk assessments for all programs unless total disbursements were less than \$10 million or testing was required based on prior years results. We assessed all payment types except for federal intragovernmental payments which were excluded based on changes to the definition of an improper payment contained in IPERA and as listed in the resulting OMB implementing guidance and government charge card payments which are separately tested under OMB Circular A-123 Appendix B, *Improving the Management of Government Charge Card Programs*. Agencies were also given the option of excluding payroll payments. This option was exercised at one Component.

Improper payment estimates in this section are based on statistical estimates for FY 2010 payments. These estimates are then projected for FY 2011 and beyond based on the timing and significance of improvements expected from completing corrective actions.

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

- Payment Processing Controls – Management’s implementation of internal controls over payment processes, including existence of current documentation, the assessment of design and operating effectiveness of internal controls over payments, the identification of deficiencies related to payment processes and whether or not effective compensating controls are present, and the results of prior IPIA payment sample testing.
- Quality of Internal Monitoring Controls – Periodic internal program reviews to determine if payments are made properly. Strength of documentation requirements and standards to support test of design and operating effectiveness for key payment controls. Presence or absence of compensating controls.



- Human Capital – Experience, training, and size of payment staff. Ability of staff to handle peak payment requirements. Level of management oversight and monitoring against fraudulent activity.
- Complexity of Program – Time program has been operating. Complexity and variability of interpreting and applying laws, regulations, and standards required of the program.
- Nature of Payments and Recipients – Type, volume, and size of payments. Length of payment period. Quality of recipient financial infrastructure and procedures. Recipient experience with federal award requirements.
- Operating Environment – Existence of factors that necessitate or allow for loosening of financial controls. Any known instances of fraud. Management’s experience with designing and implementing compensating controls.
- Additional Grant Programs Factors – Federal Audit Clearinghouse information on quality of controls within grant recipients. Identification of deficiencies or history of improper payments within recipients. Type and size of program recipients and sub-recipients. Maturity of recipients’ financial infrastructure, experience with administering federal payments, number of vendors being paid, and number of layers of sub-grantees.

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

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

**Table 5. Programs at High-Risk for Improper Payments Based on FY 2011 Risk Assessments and Prior Year Payment Sample Testing**

Component	Program Name	FY 2011 Disbursements (Based on FY 2010 Actual Data) (\$ Millions)
CBP	Border Security Fencing	\$251
	Custodial – Refund & Drawback	\$1,198
FEMA <sup>1</sup>	Disaster Relief Program – Individuals and Households Program (IHP)	\$679
	Disaster Relief Program – Vendor Payments	\$582
	Insurance – National Flood Insurance Program (NFIP)	\$1,085
	Grants – Public Assistance Programs (PA)	\$3,532
	Grants – Homeland Security Grant Program (HSGP)	\$1,516
	Grants – Assistance to Firefighters Grants (AFG)	\$385
	Grants – Emergency Food and Shelter Program (EFSP)	\$201
	Grants – Transit Security Grants Program (TSGP)	\$109
ICE <sup>2</sup>	Enforcement and Removal Operations (ERO)	\$1,332
NPPD <sup>3</sup>	Federal Protective Service (FPS)	\$811
TSA	Aviation Security – Payroll	\$2,458
USCG	Active Duty Military Payroll (ADMP)	\$2,918
<b>Total Disbursements</b>		<b>\$17,057</b>

Notes:

1. All FEMA disbursement totals are national figures. Selected states and territories were tested for the state-administered programs HSGP, PA, TSGP. See Table 6 for a listing of states and territories tested for these programs.
2. ERO was listed as Detention and Removal Operations (DRO) in the FY 2010 DHS Annual Financial Report. Only the non-payroll portion of this program was found to be high-risk. Disbursement figures are for non-payroll disbursements.



3. FPS transferred from ICE to NPPD in FY 2010. The Office of Management and Budget IPERA implementing guidance allowed agencies the option of excluding payroll payments. This option was invoked for the FPS program. Consequently, the disbursement total listed excludes payroll payments.

## II. Statistical Sampling

For FY 2011 reporting, a stratified sampling design was used to test payments based on FY 2010 disbursement amounts and the assessed risk of the program. The design of the statistical sample plans and the extrapolation of sample errors across the payment populations were completed by a statistician under contract.

Sampling plans provided an overall estimate of the percentage of improper payment dollars within +/-2.5 percent precision at the 90 percent confidence level, as specified by OMB M-03-13 guidance. An expected error rate of 3 to 10 percent of total payment dollars was used in the sample size calculation.

Using a stratified random sampling approach, payments were grouped into mutually exclusive “strata,” or groups based on total dollars. A stratified random sample typically required a smaller sample size than a simple random sample to meet the specified precision goal at any confidence level. Once the overall sample size was determined, the individual sample size per stratum was determined using the Neyman Allocation method.

The following procedure describes the sample selection process:

- Grouped payments into mutually exclusive strata;
- Assigned each payment a randomly number generated using a seed;
- Sorted the population by stratum and random number within stratum; and
- Selected the number of payments within each stratum (by ordered random numbers) following the sample size design. For the certainty strata, all payments are selected.

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

DHS sample test results are listed in Table 6.



**Table 6. DHS Sample Test Results**

Component	Program	FY 2011 Payment Population (Based on FY 2010 Actual Data) (\$ millions)	FY 2011 Sample Size (Based on FY 2010 Actual Data) (\$ millions)	FY 2011 Est. Error Amount (Based on FY 2010 Actual Data) (\$ millions)	FY 2011 Est. Error Percentage (Based on FY 2010 Actual Data) (%)
CBP	Border Security Fencing	\$251	\$202	\$0	0.01%
	Refund & Drawback	\$1,198	\$91	\$3	0.28%
FEMA	Disaster Relief Program – Individuals and Households Program (IHP)	\$679	\$2	\$2	0.31%
	Disaster Relief Program – Vendor Payments	\$582	\$222	\$17	2.87%
	Insurance – National Flood Insurance Program (NFIP)	\$1,085	\$39	\$13	1.21%
	Grants – Public Assistance Programs (PA) <sup>1</sup>	\$238	\$109	\$0	0.32%
	Grants – Homeland Security Grant Program (HSGP) <sup>2</sup>	\$510	\$225	\$1	0.34%
	Grants – Assistance to Firefighters Grants (AFG)	\$385	\$57	\$20	5.09%
	Grants – Transit Security Grants Program (TSGP) <sup>3</sup>	\$40	\$22	\$0	0.68%
	Grants – Emergency Food and Shelter Program (EFSP)	\$201	\$34	\$15	7.64%
ICE	Enforcement and Removal Operations (ERO)	\$1,332	\$319	\$108	8.12%
NPPD	Federal Protective Service	\$811	\$131	\$27	3.27%
TSA	Aviation Security – Payroll	\$2,458	\$1	\$0	0.01%
USCG	Operating Expenses - Active Duty Military Payroll	\$2,918	\$6	\$4	0.13%
<b>DHS</b>	<b>All Programs<sup>4</sup></b>	<b>\$12,688</b>	<b>\$1,460</b>	<b>\$210</b>	<b>1.66%<sup>5</sup></b>
<b>DHS</b>	<b>High-Risk Programs</b>	<b>\$4,396</b>	<b>\$802</b>	<b>\$200</b>	<b>4.55%<sup>5</sup></b>

Notes:

1. Sample testing of the Public Assistance Program was done in two stages covering seven states (AK, MA, MD, ME, PA, WA, and WY) and Puerto Rico. These states and territory paid out \$238 million out of a national total of \$3,532 million. The totals in the table are the stage two payment populations for the states and territory tested. See Table 11 Improper Payment Reduction Outlook for the national estimated error of \$11 million.
2. Sample testing of the Homeland Security Grant Program was done in two stages covering 17 states (AL, HI, IA, ID, IL, IN, KS, ND, NY, OK, RI, SC, TN, VA, WI, WV, and WY). These states paid out \$510 million out of a national total of \$1,516 million. The totals in the table are the stage two payment populations for the states tested. See Table 11 Improper Payment Reduction Outlook for the national estimated error of \$5 million.
3. Sample testing of the Transit Security Grant Program was done in two stages covering nine states (AZ, DE, GA, IN, KY, LA, NY, TN, and WI). These regions paid out \$40 million out of a national total of \$109 million. The totals in the table are the stage two payment populations for the nine regions. See Table 11 Improper Payment Reduction Outlook for the national estimated error of \$1 million.
4. Program total of \$12,668 in this table differs from \$17,057 total in Table 11 Improper Payment Reduction Outlook. For state-administered grant programs, the table above lists the population totals for the states tested, while Table 11 Improper Payment Reduction Outlook lists the national payment populations.
5. Percentage figures based on cumulative totals.

Several programs considered at high risk based on risk assessment grading were not confirmed as high risk based on sample test results. The main reason for the estimated error rates falling below \$10 million for these programs was the presence of strong compensating controls such as additional levels of payment review for manually intensive processes.



Based on the results of sample testing, corrective action plans are required for the following seven programs due to national estimated error amounts above \$10 million:

- FEMA’s Assistance to Firefighters Grants.
- FEMA’s Disaster Relief Program - Vendor Payments.
- FEMA’s Emergency Food and Shelter Program.
- FEMA’s National Flood Insurance Program.
- FEMA’s Public Assistance Program.
- ICE’s Enforcement and Removal Operations Program.
- NPPD’s Federal Protective Service Program.

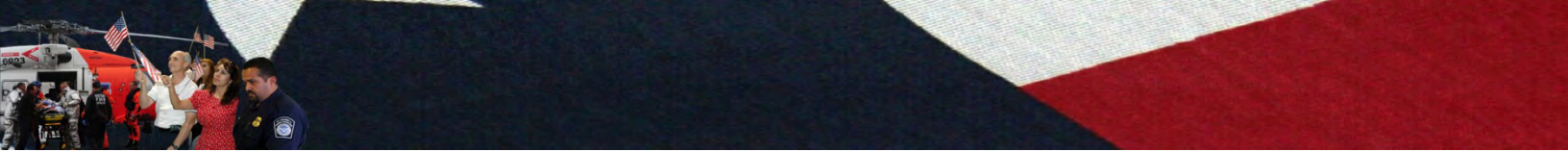
### III. Corrective Actions

The following tables list corrective actions for programs with estimated improper error amounts above \$10 million. These corrective actions are targeted at addressing the root causes behind administrative and documentation errors caused by the absence of the supporting documentation necessary to verify the accuracy of the claim; or inputting, classifying, or processing applications or payments incorrectly by DHS, a state agency, or a third party who is not the beneficiary. Authentication and medical necessity errors and verification errors were either not identified or were immaterial to the estimated error rates and amounts of DHS high-risk programs.

#### Corrective Action Plans for FEMA High-Risk Programs

**Table 7. Planned Assistance to Firefighters Grant Program Corrective Actions**

Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Incorrect Information on Application</b>		
1. Failure to Provide Accurate Information on Application	1. Update AFG Program Guidance and tutorials to instruct potential applicants to register in the National Fire Incident Reporting System and provide required information in support of their grant application.	March 2012
	2. Perform additional grantee outreach and direct applicants to include their Fire Department Identification Number as part of their grant application.	May 2012
<b>Category of Error: Purchase Outside Allowable Timeframe</b>		
1. Purchase Made Outside the Period of Performance	1. Conduct semi-annual grantee outreach and include language in the correspondence reminding grantees to monitor their disbursement progress as it relates to their respective grant’s period of performance.	March 2012
	2. Develop and deliver training for program staff to include a notification in Comments section in the AFG system when reviewing payments during or after the tenth month of a grantee’s period of performance.	March 2012



Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Unallowable Use of Excess Funds</b>		
1. Use of Excess Funds without Supporting Amendment or to Purchase Ineligible Goods and/or Services	1. Require each applicant to complete the <i>AFG Grant Management Tutorial</i> that is currently available on the AFG Program website.	March 2012
<b>Category of Error: Insufficient Documentation</b>		
1. Failure to Submit Supporting Documentation	1. Develop grantee documentation organization and retention guidance and offer associated record keeping training.	March 2012
	2. Develop a plan that outlines procedures for conducting annual audits of grantee supporting documentation.	May 2012

**Table 8. Planned Disaster Relief Fund Vendor Payments Program Corrective Actions**

Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Insufficient Policies to Prevent Improper Payments</b>		
1. Acquisition manual needs to be strengthened	1. Update acquisition manual to include a chapter on procurement roles and responsibilities for contract payments. Specific points to include: contracting officer delegations; invoice requirements including reviews against regulations, contract terms and conditions; requirements for adequate supporting documentation; procedures for establishing billing rates; and a description of billing mechanisms required for different contract types.	March 2012
	2. Revise acquisition manual sections on standard billing language, procedures for product substitution and/or pricing variances, and requirements and procedures for issuing contract modifications.	March 2012
2. COTR manual needs to be strengthened	1. Add a chapter on how to review invoices for approval.	March 2012
3. Vendor payments standard operating procedures need to be strengthened	1. Add a chapter on invoice reviews required in each step of the invoice payment cycle.	March 2012
4. Training needed on invoicing roles and responsibilities throughout the contract life-cycle	1. Institute mandatory and refresher training for contracting officers, contracting officer's technical representatives, and accounting technicians.	May 2012





Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Non-Contract Payments</b>		
1. Standard operating procedures needed	1. Develop a process and standard operating procedures for authorizing and paying non-contract payments such as lease payments and bills of lading.	June 2012
<b>Category of Error: Acceptance and Receiving</b>		
1. Reports and contract file maintenance needs improvement	1. Develop a standard inspection, acceptance, and receiving report for contracting officer's technical representatives and complete training on its proper completion and use.	June 2012
	2. Implement an electronic contract file maintenance system.	June 2012

**Table 9. Planned Emergency Food and Shelter Program Corrective Actions**

Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Insufficient Supporting Documentation</b>		
1. Missing Proof of Purchase	1. Develop guidance around the supporting documentation checklist to state that unless the checklist is completely satisfied, the documentation will not be accepted by EFSP.	December 2011
2. Missing Proof that Payment Still Due	1. Develop improved guidance for utility or rent assistance to clarify that the local recipient organization (LRO) must have proof that payment is still due if paid beyond 60 days after the LRO was notified of the request for assistance.	March 2012
3. Missing LRO Documentation: a. Missing required certification documents, b. Missing Proof of Payment	1. Establish a filing system to maintain required LRO certification documents, including but not limited to the following forms: (1) Local Board Certification, (2) Local Board Roster, (3) Lobbying Certification, (4) Local Board Plan, (5) Interim Report, and (6) Final Report.	December 2011
4. Missing All Supporting Documentation	1. Review the existing National Board Program requirements training for possible modification of documentation requirements and other grant management improvement opportunities.	March 2012
	2. Provide grantees with technical assistance on maintaining adequate documentation for transactions using EFSP funds.	December 2011



Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Purchase Outside Allowable Timeframe</b>		
1. Purchase Made Outside the Period of Performance	1. Require local boards to conduct outreach activities with LROs throughout the period of performance.	December 2011
	2. Require LROs to perform a self assessment of the purchase and/or initiation dates on all supporting documentation before submission to the local board to ensure that all expenditures are within the specified period of performance of the appropriate spending phase.	March 2012
<b>Category of Error: Spending Condition Non-compliance</b>		
1. Spending Condition Errors	1. Develop a mandatory on-line training course to be taken and passed by all local boards and LROs awarded funding.	May 2012
2. Incorrect Rent, Mortgage or Utility Payment: a. Current Payments Made Too Early b. Allowable Assistance Payment Exceeded	1. Leverage existing LRO rent/mortgage and utility assistance letters to create standardized forms for spending and other categories where compliance problems persist with submission of LRO supporting documentation.	March 2012

**Table 10. Planned National Flood Insurance Program Corrective Actions**

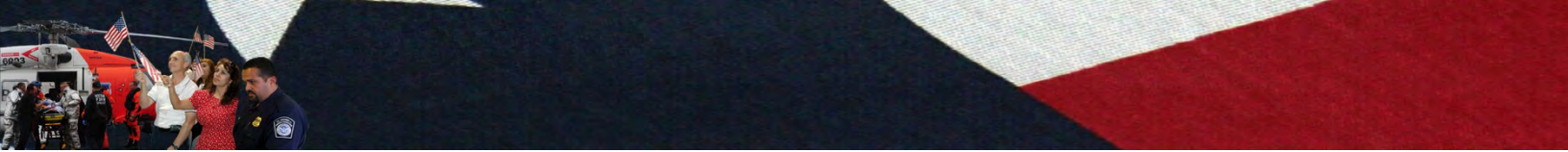
Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Incorrect Estimate / Worksheet Calculation Errors</b>		
1. Insurance coverage incorrectly applied by adjusters. Claim estimates included items not covered under Flood insurance policy.	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	May 2012
	2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	
<b>Category of Error: Payment Processing Errors</b>		
1. Incorrect Application of Salvage	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences	May 2012
	2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	
	3. System Enhancements: Develop process to leverage the current transaction record reporting and processing reports and other NFIP financial and statistical data mechanisms to help insurers and flood vendors identify payment processing errors electronically.	



Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Insufficient Damage Documentation</b>		
1. Lack of supporting documentation for adjuster estimates on lump-sum items. Increased Cost Compliance claims not supported with required claim documentation.	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	May 2012
	2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	

**Table 11. Planned Public Assistance (PA) Program Corrective Actions**

Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Incorrect Entity Paid</b>		
1. Incorrect Federal Information Processing Standards Number	1. Improve grantee project worksheet (PW) development procedures by incorporating a quality check after the initial PW is completed to confirm all information within the PW is relevant and correct prior to submitting the final version into the system of record.	October 2011
<b>Category of Error: Unmet Work Completion Deadline</b>		
1. Failure to Complete Work During Period of Performance	1. Increase grantee documentation review guidance and create and conduct Public Assistance payment processing training.	March 2012
<b>Category of Error: Scope Discrepancy between Project Worksheet Scope of Work (SOW) and Supporting Documentation</b>		
1. Discrepancies Found between PW SOW and Supporting Documentation	1. Require FEMA project specialists and Public Assistance coordinators to take training courses on proper PW data entry and development, project writing skills, and audit review requirements.	October 2011
	2. Develop reference guides and/or checklists for costs documentation reviews to improve consistency of scope reviews.	October 2011
	3. Offer grantee invoice and force account documentation review guidance or training to ensure the scope of supporting documentation falls within the scope of the PW/SA.	October 2011
<b>Category of Error: Calculation Error between Force Account Summary Sheet and Closeout PW</b>		
1. Mathematical Calculation Error	1. Develop guidance for grantees to eliminate use of rounding in payment calculations to improve accuracy of disbursements of grant funds to sub-grantees.	March 2012



Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error:</b> Direct Administrative Costs Not Supported in Closeout PW		
1. Direct Administrative Costs Not Included in Closeout PW	1. Improve guidance and outreach to grantees on payment calculations, quality control, and overall accuracy of information when closing out a PW.	October 2011

### Corrective Action Plan for ICE High-Risk Program

The corrective actions implemented by ICE for the ERO Program will strengthen documentation, invoicing, contract quality, payment quality and accuracy, discount and interest accuracy, and travel payment quality and accuracy.

**Table 12. Completed ERO Corrective Actions**

Risk Factors	Corrective Actions	Completed Date
<b>Category of Error:</b> Invalid / Improper Invoice		
1. Vendor payments delayed or made incorrectly due to inadequate information	1. Discontinue the use of the invoice adjustment form. If an invoice is incorrect, the invoice must be rejected and resubmitted by the vendor.	February 2011
<b>Category of Error:</b> Contract Quality		
2. Improper processing of contracts and obligations; not in compliance with the Federal Acquisition Regulation	1. Align receipt and acceptance policies and procedures with federal requirements.	September 2011
<b>Category of Error:</b> Discount and Interest Accuracy		
3. Improper management of funds	1. Establish a policy to maximize cost-effective discounts.	May 2011
	2. Develop appropriate tools to communicate and monitor the status of invoices with discounts offered.	July 2011
	3. Conduct refresher training related to interest penalty payments and vendor discounts.	July 2011
	4. Develop monitoring and testing criteria to monitor the effectiveness of all procedural updates.	July 2011



**Table 13. Planned ERO Corrective Actions**

Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Missing Documentation</b>		
1. Insufficient documentation to support and/or validate financial transactions	1. Provide payment documentation requirements and instructions to the program offices. Instructions to detail the following: (1) invoices that do not contain all invoice backup documentation must be rejected by the receiving and acceptance official, (2) compliance required with record retention guidelines according to National Archives and Records Administration (NARA), and (3) the need for program offices to maintain and have readily available all service agreements and memoranda of understanding.	December 2011
	2. Automate FY 2012 IPERA documentation collection by establishing a central SharePoint collaboration site.	March 2012
<b>Category of Error: Invalid / Improper Invoice</b>		
1. Vendor payments delayed or made incorrectly due to inadequate information	1. Conduct refresher training for payment technicians on elements of a proper invoice and ensure that improper invoices are rejected upon receipt.	March 2012
<b>Category of Error: Contract Quality</b>		
1. Improper processing of contracts and obligations; not in compliance with the Federal Acquisition Regulation	1. Implement new receipt and acceptance requirements.	March 2012
	2. Establish and provide “Subject to Availability of Funds” guidance regarding notification to vendor for funds availability, receipt of invoice, and payment of interest.	May 2012
<b>Category of Error: Payment Quality and Accuracy</b>		
1. Improper processing of vendor payments and disbursements	1. Conduct refresher training for contracting officer, contracting officer’s technical representative (COTR), and/or program manager to ensure review of invoices to contracted pricing, invoice alignment to correct obligations, and accurate and complete supporting documentation.	March 2012
	2. Conduct refresher training for finance centers and implement an updated checklist to incorporate the review of invoices for date (discount/penalty), correct contract, and correct obligation lines.	March 2012



## Corrective Action Plan for NPPD High-Risk Program

The corrective actions implemented by NPPD and FPS will strengthen contract oversight and improve the review and processing of invoices and contract modifications.

**Table 14. Planned Federal Protective Service Program Corrective Actions**

Risk Factors	Corrective Actions	Target Completion Date
<b>Category of Error: Contract Oversight</b>		
1. Contractor approving payment of invoices on behalf of the COTR	1. Remove contractors from the process of paying invoices, including terminating contractor access to Webview. Coordinate all Webview access requests through NPPD.	November 2011
	2. Provide COTRs with support to review and approve payments within Webview.	May 2012
1. Contract administration weakness	1. FPS Acquisition Division will establish a team of senior procurement officials and operational procurement staff to identify improvements to contract administration including invoicing and documentation.	December 2011
	2. FPS Acquisition Division will coordinate with program offices and contracting officers to identify and provide written delegations of authority to federal employees which facilitate an efficient invoice review and approval process.	January 2012
	3. Provide training to contracting officers, COTRs, and appropriate program officials on invoice review and contract modifications. Emphasis will be on the timely correction of errors on invoices and contract lines.	February 2012

## Funds Stewardship

FEMA worked closely with primary grant recipients to ensure proper stewardship of funds at the sub-recipient levels. For example, on the Emergency Food and Shelter Program, FEMA worked closely with The United Way's National Board. As a result, the National Board issued a memo highlighting that additional rounds of funding to local boards would be dependent upon receipt of timely supporting documentation for tested sample payments. Significant additional documentation came in which supported as proper many test sample payments. FEMA also assisted states in improving the guidance they provide local entities for several state administered FEMA grant programs.



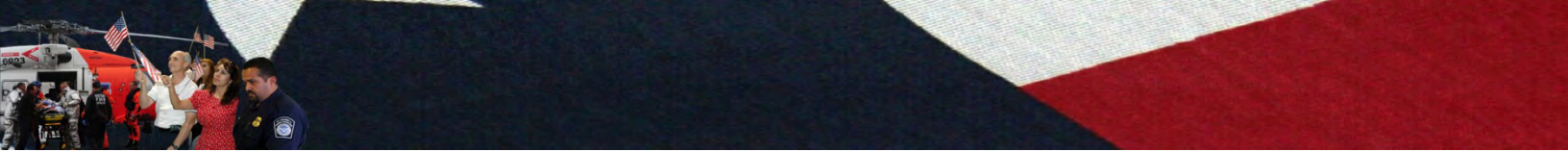
#### IV. Program Improper Payment Reporting

Table 15 summarizes improper payment amounts for DHS high-risk programs. Improper payment percent (IP%) and improper payment dollar (IP\$) results are provided from last year's testing of FY 2009 payments and this year's testing of FY 2010 payments. Data for projected future-year improvements is based on the timing and significance of completing corrective actions.

**Table 15. Improper Payment Reduction Outlook**

Improper Payment Reduction Outlook (\$ in millions)															
Program	PY Outlays	PY IP%	PY IP\$	CY Outlays	CY IP%	CY IP\$	CY+1 Outlays	CY+1 Est. IP%	CY+1 Est. IP\$	CY+2 Est. Outlays	CY+2 Est. IP%	CY+2 Est. IP\$	CY+3 Est. Outlays	CY+3 Est. IP%	CY+3 Est. IP\$
	(Based on FY 2009 Actual Data)			(Based on FY 2010 Actual Data)			(Based on FY 2011 Actual and Estimated Data)			(Based on 2012 Estimated Data)			(Based on 2013 Estimated Data)		
Border Security Fencing (CBP)	\$638	0.03%	\$0	\$251	0.01%	\$0	\$396	0.01%	\$0	\$528	0.01%	\$0	\$458	0.01%	\$0
Refund & Drawback (CBP)	\$1,436	0.20%	\$3	\$1,198	0.28%	\$3	\$1,405	0.17%	\$2	\$1,300	0.17%	\$2	\$1,300	0.17%	\$2
IHP (FEMA)	\$848	2.72%	\$23	\$679	0.31%	\$2	\$722	0.31%	\$2	\$722	0.31%	\$2	\$722	0.31%	\$2
Disaster Relief Program Vendor Payments (FEMA)	\$1,382	3.32%	\$46	\$582	2.87%	\$17	\$933	2.00%	\$19	\$933	1.50%	\$14	\$933	1.00%	\$9
NFIP (FEMA)	\$3,287	2.22%	\$73	\$1,085	1.21%	\$13	\$1,730	1.10%	\$19	\$1,730	1.00%	\$17	\$1,730	0.90%	\$16
PA (FEMA)	\$5,070	0.21%	\$11	\$3,532	0.32%	\$11	\$3,976	0.21%	\$8	\$3,976	0.21%	\$8	\$3,976	0.21%	\$8
HSGP (FEMA)	\$1,300	2.20%	\$29	\$1,516	0.34%	\$5	\$1,402	0.34%	\$5	\$1,402	0.34%	\$5	\$1,402	0.34%	\$5
AFG (FEMA)	\$429	6.32%	\$27	\$385	5.09%	\$20	\$440	4.25%	\$19	\$440	3.50%	\$15	\$440	2.50%	\$11
TSGP (FEMA)	\$119	0.09%	\$0	\$109	0.68%	\$1	\$114	0.09%	\$0	\$114	0.09%	\$0	\$114	0.09%	\$0
EFSP (FEMA)	\$86	6.18%	\$5	\$201	7.64%	\$15	\$251	5.00%	\$13	\$251	4.00%	\$10	\$251	3.50%	\$9
ERO (ICE)	\$1,320	0.53%	\$7	\$1,332	8.12%	\$108	\$1,414	7.95%	\$112	\$1,442	4.10%	\$59	\$1,471	2.00%	\$29
FPS (NPPD)	\$760	0.10%	\$1	\$811	3.27%	\$27	\$835	2.50%	\$21	\$943	2.00%	\$19	\$1,009	1.50%	\$15
Aviation Security – Payroll (TSA)	\$2,383	0.00%	\$0	\$2,458	0.01%	\$0	\$2,619	0.01%	\$0	\$2,841	0.01%	\$0	\$2,951	0.01%	\$0
ADMP (USCG)	\$2,766	0.13%	\$4	\$2,918	0.13%	\$4	\$3,006	0.13%	\$4	\$3,006	0.13%	\$4	\$3,006	0.13%	\$4
<b>All Programs</b>	<b>\$21,824</b>	<b>1.05%</b>	<b>\$229</b>	<b>\$17,057</b>	<b>1.32%</b>	<b>\$226</b>	<b>\$19,243</b>	<b>1.17%</b>	<b>\$224</b>	<b>\$19,628</b>	<b>0.80%</b>	<b>\$157</b>	<b>\$19,763</b>	<b>0.56%</b>	<b>\$111</b>

Note: For the three FEMA programs that were not tested nationally—HSGP, PA, and TSGP—the error rate from the state(s) tested was applied to the national payment population to produce the estimated error amounts listed above. Estimated outlays for FEMA programs were calculated by averaging the total disbursements for the past three fiscal years, due to the volatile nature of the programs tested. TSGP estimated outlay figures were based on the past two fiscal years that this program was tested.



## Overpayments and Underpayments Details

The table that follows provides overpayment and underpayment breakouts for the Department’s high-risk programs. The table shows that 98 percent of the Department’s estimated improper payments are due to overpayments, and 2 percent are due to underpayments.

**Table 16. Overpayment and Underpayment Detail on DHS Sample Test Results**

Component	Program	FY 2011 Gross Total (Based on FY 2010 Actual Data)		FY 2011 Overpayment Total (Based on FY 2010 Actual Data)		FY 2011 Underpayment Total (Based on FY 2010 Actual Data)	
		Est. Error Amount (\$ millions)	Est. Error Percentage (%)	Est. Error Amount (\$ millions)	Est. Error Percentage (%)	Est. Error Amount (\$ millions)	Est. Error Percentage (%)
CBP	Border Security Fencing (CBP)	\$0	0.01%	\$0	0.01%	\$0	0.00%
	Refund & Drawback (CBP)	\$3	0.28%	\$3	0.28%	\$0	0.00%
FEMA	IHP (FEMA)	\$2	0.31%	\$0	0.00%	\$2	0.31%
	Disaster Relief Program Vendor Payments (FEMA)	\$17	2.87%	\$17	2.87%	\$0	0.00%
	NFIP (FEMA)	\$13	1.21%	\$12	1.15%	\$1	0.06%
	PA (FEMA)	\$11	0.32%	\$11	0.31%	\$0	0.01%
	HSGP (FEMA)	\$5	0.34%	\$5	0.34%	\$0	0.00%
	AFG (FEMA)	\$20	5.09%	\$20	5.09%	\$0	0.00%
	TSGP (FEMA)	\$1	0.68%	\$1	0.68%	\$0	0.00%
	EFSP (FEMA)	\$15	7.64%	\$15	7.64%	\$0	0.00%
ICE	ERO (ICE)	\$108	8.12%	\$108	8.11%	\$0	0.01%
NPPD	FPS (NPPD)	\$27	3.27%	\$27	3.27%	\$0	0.00%
TSA	Aviation Security – Payroll (TSA)	\$0	0.01%	\$0	0.00%	\$0	0.01%
USCG	ADMP (USCG)	\$4	0.13%	\$3	0.09%	\$1	0.04%
<b>DHS</b>	<b>All Programs</b>	<b>\$226</b>		<b>\$222</b>		<b>\$4</b>	

## V. Recapture of Improper Payments

DHS completed recovery audit work for FY 2010 disbursements and continued collection activities for errors identified in prior-year recovery audits. Work was completed at CBP, FEMA, ICE (and the Components they cross-service), and U.S. Coast Guard. Given the highly productive findings from the U.S. Coast Guard’s targeted recovery audit work (details below), completing this work was given priority over completing a general recovery audit over all payments. The U.S. Coast Guard will complete a general recovery audit over FY 2010 and FY 2011 contract payments in FY 2012. This audit will also cover DNDO, TSA, and Components cross-serviced by the U.S. Coast Guard. The U.S. Secret Service will complete a recovery audit over FY 2010 and FY 2011 payments in FY 2012. FLETC performed a cost analysis which determined that a general recovery audit would not be cost effective at this time. In Table 17, which follows, current year (CY) equals FY 2010 disbursements, and prior year (PY) covers FY 2005–FY 2009 for DNDO, TSA, and U.S. Coast Guard; FY 2004–FY 2009 for CBP, ICE, MGMT, NPPD, OHA, S&T, and USCIS; and FY 2009–FY 2010 for FEMA.

The U.S. Coast Guard hired a recovery audit contractor to perform a targeted in-depth examination of telecommunications invoices. An examination of 14,000 telecommunications invoices from





FY 2005 to FY 2010 identified errors totaling \$4,144,859, of which \$64,460 has been recovered, and \$4,080,399 is undergoing collection. All of the \$4,144,859 improper payment errors were caused by overpayments (no underpayments). The low rate of recoupment of these errors reflects: (1) the fact that this was the first time the U.S. Coast Guard performed a targeted recovery audit of telecommunications payments, (2) the complexity of the invoices examined, (3) the need to centralize the collection of the overpayments within a decentralized procurement activity, and (4) the desire to complete full due diligence with the vendor community to validate the correctness of potential claims.

Telecommunications invoices were selected for a targeted recovery audit due to: (1) inconsistent billing practices and invoice format between carriers, (2) pricing complexities including multiple pages with numerous pricing elements (3) charges listed in “lump sum” amounts with discounts generally applied making it difficult to establish true price points, (4) multiple telecom companies and services billing on a single invoice, and (5) inability of staff to perform in-depth reviews of invoices due to technical proficiency and monthly payment volume.

Identified payment errors for telecommunications invoices include: (1) international and domestic rate charges in excess of published rates, (2) plan errors due to pricing not following requested General Services Administration (GSA) discounted plan, (3) inconsistent rate charges for the same service in the same geographic region, (4) charges for federal and state taxes, (5) discovery of unauthorized third-party billings (i.e., cramming), (6) unexplained increases in land line charges, and (7) zero usage charges.

Immediate benefits from this work included the dropping of long distance services from accounts where it was not required, producing an immediate cost savings of \$102,335 and the identification of numerous circuits, telephone lines, and data pipes suspected to no longer be in use. Estimated future cost savings could be in excess of two million dollars. In addition to following up on these items, the U.S. Coast Guard is evaluating procurement policy, acquisition procedures, and payment controls to fully leverage the benefits of this recovery audit contract work. An operations team consisting of specialists in telecommunications and information technology, procurement, financial management, and legal has been assembled to rectify known billing issues and to develop a corrective action plan to correct systemic process and payment errors to ensure non-recurrence going forward. The U.S. Coast Guard will apply the lessons learned from these recovery auditing activities to develop automated monitoring controls. Vendor-wide memos will be distributed requesting rate changes for all accounts with non-GSA rates. Internal certifications and ongoing training will also be provided to the designated account representatives who order telecommunications services. Language eliminating the use of third party billings will also be added to telecommunications contracts where appropriate.

FEMA conducts regular audits to assess the effectiveness of its controls, identify improper payments or risk areas, and consider new procedures to reduce risk. This continued self-assessment and vigilance significantly reduced the improper payment error rate from 14 percent following Hurricane Katrina in 2005 to less than one percent in FY 2010. In instances of improper payments, new procedures implemented in 2011 allow FEMA to request the return of any improperly awarded disaster assistance payments while maintaining each disaster survivor’s due process rights and offering opportunities to appeal, which may include the opportunity for an oral hearing.



**Table 17. Payment Recapture Audit Reporting**

Component	Type of Payment (contract, grant, benefit, loan, or other)	Amount Subject to Review for CY Reporting (\$ millions)	Actual Amount Reviewed and Reported (CY) (\$ millions)	Amount Identified for Recovery (CY) (\$000)	Amount Recovered (CY) (\$000)	% of Amount Recovered out of Amount Identified (CY)	Amount Outstanding (CY) (\$000)	% of Amount Outstanding out of Amount Identified (CY)	Amount Determined Not to be Collectable (CY) (\$000)	% of Amount Determined Not to be Collectable out of Amount Identified (CY)	Amounts Identified for Recovery (PYs) (\$000)	Amounts Recovered (PYs) (\$000) <sup>1</sup>	Cumulative Amounts Identified for Recovery (CY + PYs) (\$000)	Cumulative Amounts Recovered (CY + PYs) (\$000)	Cumulative Amounts Outstanding (CY + PYs) (\$000)	Cumulative Amounts Determined Not to be Collectable (CY + PYs) (\$000)
CBP	Contract	\$2,345	\$2,345	\$0	\$0	100%	\$0	100%	\$0	0%	\$250	\$246	\$250	\$246	\$2	\$2
DNDO <sup>2</sup>	Contract	\$369	\$0	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$1	\$1	\$1	\$1	\$0	\$0
FEMA	Contract	\$1,067	\$1,067	\$3	\$0	0%	\$3	100%	\$0	0%	\$178	\$0	\$181	\$0	\$3	\$178
ICE	Contract	\$2,837	\$2,837	\$7	\$0	0%	\$7	100%	\$0	0%	\$1,748	\$1,607	\$1,755	\$1,607	\$45	\$103
MGMT <sup>3</sup>	Contract	\$472	\$472	\$36	\$36	100%	\$0	0%	\$0	0%	\$174	\$172	\$210	\$208	\$2	\$0
NPPD <sup>3</sup>	Contract	\$553	\$553	\$26	\$17	65%	\$9	35%	\$0	0%	\$190	\$190	\$216	\$207	\$9	\$0
OHA <sup>3</sup>	Contract	\$49	\$49	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$0	\$0	\$0	\$0	\$0	\$0
S&T <sup>3</sup>	Contract	\$433	\$433	\$1	\$0	0%	\$1	100%	\$0	0%	\$54	\$54	\$55	\$54	\$1	\$0
TSA <sup>2</sup>	Contract	\$2,178	\$0	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$722	\$722	\$722	\$722	\$0	\$0
USCG	Contract	\$2,308	\$78	\$4,145	\$65	2%	\$4,080	98%	\$0	0%	\$107	\$91	\$4,252	\$156	\$4,096	\$0
USCIS <sup>3</sup>	Contract	\$913	\$913	\$0	\$0	n/a	\$0	n/a	\$0	n/a	\$904	\$892	\$904	\$892	\$4	\$8
<b>DHS Totals</b>		<b>\$13,524</b>	<b>\$8,747</b>	<b>\$4,218</b>	<b>\$118</b>	<b>3%</b>	<b>\$4,100</b>	<b>97%</b>	<b>\$0</b>	<b>0%</b>	<b>\$4,328</b>	<b>\$3,975</b>	<b>\$8,546</b>	<b>\$4,093</b>	<b>\$4,162</b>	<b>\$291</b>

Notes:

1. The format for the Recovery Audit Results table published in the FY 2010 DHS Annual Financial Report included all collections accomplished in the current fiscal year in one column (Amounts Recovered CY). Reporting in the table above distinguishes between FY 2011 collections which relate to current year claims (Amount Recovered CY) from collections from prior year claims (Amounts Recovered PYs).
2. DNDO and TSA are cross-serviced by the U.S. Coast Guard.
3. MGMT, NPPD, OHA, S&T, and USCIS are cross-serviced by ICE.



The next two tables highlight the productivity of the targeted recovery audit work performed at the U.S. Coast Guard relative to general recovery audits performed elsewhere.

**Table 18. Payment Recapture Audit Targets**

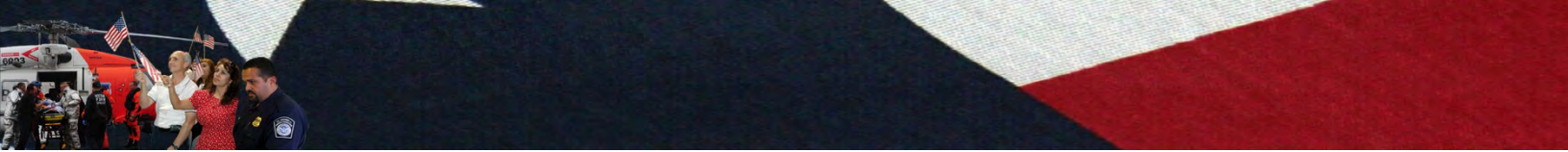
Component	Type of Payment (contract, grant, benefit, loan, or other)	CY Amount Identified (\$000)	CY Amount Recovered (\$000)	CY Recovery Rate (Amount Recovered / Amount Identified)	CY + 1 Recovery Rate Target	CY + 2 Recovery Rate Target	CY + 3 Recovery Rate Target
FEMA	Contract	\$3	\$0	0%	100%	100%	100%
ICE	Contract	\$7	\$0	0%	100%	100%	100%
MGMT	Contract	\$36	\$36	100%	100%	100%	100%
NPPD	Contract	\$26	\$17	65%	100%	100%	100%
S&T	Contract	\$1	\$0	0%	100%	100%	100%
USCG	Contract	\$4,145	\$65	2%	50%	80%	100%
<b>DHS Totals</b>		<b>\$4,218</b>	<b>\$118</b>	<b>3%</b>			

**Table 19. Aging of Outstanding Overpayments**

Component	Type of Payment (contract, grant, benefit, loan, or other)	CY Amount Outstanding (0 – 6 months) (\$000)	CY Amount Outstanding (6 months to 1 year) (\$000)	CY Amount Outstanding (over 1 year) (\$000)
FEMA	Contract	\$3	\$0	\$0
ICE	Contract	\$7	\$0	\$0
NPPD	Contract	\$9	\$0	\$0
S&T	Contract	\$1	\$0	\$0
USCG	Contract	\$4,080	\$0	\$0
<b>DHS Totals</b>		<b>\$4,100</b>	<b>\$0</b>	<b>\$0</b>

**Table 20. Disposition of Recaptured Funds**

Component	Type of Payment (contract, grant, benefit, loan, or other)	Agency Expenses to Administer the Program (\$000)	Payment Recapture Auditor Fees (\$000)	Financial Management Improvement Activities (\$000)	Original Purpose (\$000)	Office of Inspector General (\$000)	Returned to Treasury (\$000)
MGMT	Contract	\$0	\$6	\$0	\$30	\$0	\$0
NPPD	Contract	\$0	\$3	\$0	\$14	\$0	\$0
USCG	Contract	\$0	\$11	\$0	\$54	\$0	\$0
<b>DHS Totals</b>		<b>\$0</b>	<b>\$20</b>	<b>\$0</b>	<b>\$98</b>	<b>\$0</b>	<b>\$0</b>



The table that follows shows the importance of the Secretary’s quarterly high-dollar overpayments reporting. These reports began with January-March 2010 reporting. Recoverable errors from IPIA high-risk program testing are mainly from FEMA’s testing of the National Flood Insurance Program and U.S. Coast Guard’s testing of Active Duty Military Payroll. Post-payment review figures are from U.S. Coast Guard.

**Table 21. Overpayments Recaptured Outside of Payment Recapture Audits**

Source of Recovery	Amount Identified (CY) (\$000)	Amount Recovered (CY) (\$000)	Amount Identified (PY) (\$000)	Amount Recovered (PY) (\$000)	Cumulative Amount Identified (CY+PYs) (\$000)	Cumulative Amount Recovered (CY+PYs) (\$000)
High-Dollar Overpayments Reporting	\$8,183	\$7,493	\$6,063	\$5,956	\$14,246	\$13,449
IPIA High-Risk Program Testing	\$190	\$43	\$880	\$202	\$1,070	\$245
Post Payment Reviews	\$2,620	\$2,582	\$0	\$0	\$2,620	\$2,582
<b>DHS Totals</b>	<b>\$10,993</b>	<b>\$10,118</b>	<b>\$6,943</b>	<b>\$6,158</b>	<b>\$17,936</b>	<b>\$16,276</b>

**VI. Ensuring Management Accountability**

The goals and requirements of IPERA were communicated to all levels of staff throughout the Offices of the Chief Financial Officer and to relevant program office and procurement staff. The Department’s Deputy Chief Financial Officer and senior staff and FEMA’s Chief Financial Officer and senior staff have incorporated improper payment reduction targets in their annual performance plans. FEMA grant program managers have communicated to primary recipients that continued funding is contingent upon supporting the Department’s improper payments efforts.

Continuing an initiative begun in FY 2009, Secretary Napolitano includes recoupment of improper payments as an efficiency measure which is tracked quarterly. Additionally, managers are responsible for completing internal control work on payment processing as part of the Department’s OMB Circular A-123 effort.

**VII. Agency Information Systems and Other Infrastructure**

The Department’s agency information systems efforts are discussed under the section related to the *Federal Financial Management Improvement Act*.

**VIII. Statutory or Regulatory Barriers**

None.

**IX. Overall Agency Efforts**

The Department is striving to leverage lessons learned from the battle to reduce and recover improper payments to other operational areas. At FEMA, for example, improper payment corrective actions support improvements to grants management and better coordination between



recipients and sub-recipients. At NPPD, close cooperation between finance and procurement shops will help the Department address contract management administration weakness that does not directly lead to improper payments but raises risks. At U.S. Coast Guard, an audit of telecommunications bills supports the strengthening of acquisition practices and the identification of cost savings.



## Other Key Regulatory Requirements

### *Prompt Payment Act*

The *Prompt Payment Act* requires federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's Components submit prompt payment data as part of data gathered for the OMB CFO Council's Metric Tracking System (MTS). Periodic reviews are conducted by the DHS Components to identify potential problems. Interest penalties as a percentage of the dollar amount of invoices subject to the *Prompt Payment Act* have been measured between 0.002 percent and 0.073 percent for the period of October 2010 through September 2011, with an annual average of 0.009 percent. *Note: MTS statistics are reported with at least a six-week lag.*

### *Debt Collection Improvement Act (DCIA)*

In compliance with the *Debt Collection Improvement Act of 1996 (DCIA)*, DHS manages its debt collection activities under the DHS DCIA regulation. The regulation is implemented under DHS's comprehensive debt collection policies that provide guidance to the Components on the administrative collection of debt; referring non-taxable debt; writing off non-taxable debt; reporting debts to consumer reporting agencies; assessing interest, penalties and administrative costs; and reporting receivables to the Department of the Treasury.

### *FY 2010 Biennial User Charges Review*

The *Chief Financial Officers Act of 1990* requires each agency CFO to review, on a biennial basis, the fees, royalties, rents, and other charges imposed by the agency for services and items of value provided to specific recipients, beyond those received by the general public. The purpose of this review is to identify those agencies assessing user fees and to periodically adjust existing charges to: 1) reflect unanticipated changes in costs or market values; and 2) to review all other agency programs to determine whether fees should be assessed for government services or the use of government goods or services.

In addition, on October 28, 2009, the *FY 2010 Department of Homeland Security Appropriations Act* (Pub. L. 111-83) and accompanying House Report 111-157 was passed, requiring the Department to provide to Congress a quarterly report on actual FY 2009 user fee collections and future projections across all relevant DHS Components. Therefore, to ensure consistency in reporting, the OCFO conducted the above DHS user fee assessment based on the Component's review, validation, and confirmation of actual cash collections and user fee structures, as identified in the Department of Homeland Security User Fees Report to Congress. This review was reported by the CFO in the Department's FY 2010 Annual Financial Report. The next biennial review of user fees to be performed by DHS is scheduled to take place in FY 2012 and will be based on FY 2011 data.



# Major Management Challenges Facing the Department of Homeland Security

*Office of Inspector General*

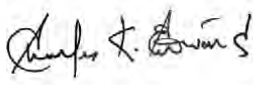
U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

November 10, 2011

MEMORANDUM FOR: The Honorable Janet Napolitano  
Secretary

FROM: Charles K. Edwards   
Acting Inspector General

SUBJECT: *Major Management Challenges  
Facing the Department of Homeland Security*

Attached for your information is our annual report, *Major Management Challenges Facing the Department of Homeland Security*, for inclusion in the Department of Homeland Security 2011 *Annual Financial Report*.

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

Attachment



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

## Major Management Challenges Facing the Department of Homeland Security



OIG-12-08

November 2011





Office of Inspector General

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



Homeland  
Security

November 10, 2011

Preface

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

The attached report presents our fiscal year 2011 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

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

Charles K. Edwards  
Acting Inspector General



*Office of Inspector General*

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



**Homeland  
Security**

## **Major Management Challenges Facing the Department of Homeland Security**

At its establishment in 2003, the Department of Homeland Security (DHS) faced the difficult task of building a cohesive, effective, and efficient Department from 22 disparate agencies while simultaneously performing the mission for which it was created. That mission, to secure the nation against the entire range of threats that we face, is itself an arduous assignment. The Department has made progress in coalescing into an effective organization, as well as addressing its key mission areas to secure our nation's borders, increase our readiness and resiliency in the face of a terrorist threat or a natural disaster, and implement increased levels of security in our transportation systems and trade operations.

As in previous years, the Department's major challenges lie in nine broad areas, which we address below:

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



## ACQUISITION MANAGEMENT

Although the Department continues to make progress in improving its acquisition management, it remains a significant challenge facing DHS, in part because of the magnitude of the number, dollar value, and complexity of its acquisition activity. Below, we identify where DHS improved its acquisition management process, as well as areas where it continues to face challenges.

### Organizational Alignment and Leadership

In fiscal year (FY) 2011, DHS improved the acquisition program's organizational alignment and maintained strong executive leadership, but more needs to be done. In January, DHS reorganized the reporting structure of the procurement management and program management functions to provide a layered approach to acquisition oversight. Now the Office of the Chief Procurement Officer (OCPO) leads procurement management functions and the Under Secretary for Management leads program management functions. Components continue to maintain their own acquisition and procurement staff. At the component level, the Chief Acquisition Executive is responsible for acquisition program management and the Head of Contracting Activity is responsible for acquisition procurement. There are currently eight chief acquisition executives and nine heads of contracting activity in DHS. The chief acquisition executives and the heads of contracting activity report informally to the Under Secretary for Management and OCPO, respectively.

According to the Government Accountability Office (GAO),<sup>1</sup> DHS has not fully planned for or acquired the workforce needed to implement its acquisition oversight policies. A GAO report issued in February 2011 states that, DHS needs to implement its Integrated Strategy for High Risk Management and continue its efforts to (1) identify and acquire resources needed to achieve key actions and outcomes; (2) implement a program to independently monitor and validate corrective measures; and (3) show measurable, sustainable progress in implementing corrective actions and achieving key outcomes. DHS needs to demonstrate sustained progress in all of these areas to better strengthen and integrate management functions throughout the Department and its components' acquisition functions.

### Policies and Processes

DHS continues to develop and strengthen its acquisition management policies and processes. However, the Department needs to further refine its policies to provide detailed guidance, and improve oversight and internal controls in some key areas. For example, the Department needs to improve internal control procedures to mitigate the inherent risks associated with purchase card use. Our review of the Department's purchase card program<sup>2</sup> found that the post-payment audit process did not ensure that component personnel were meeting minimum internal control requirements established by the Office of Management and Budget (OMB). Nor did the process effectively target high-risk transactions. Ninety-three percent of the purchase card transactions we reviewed did not fully comply with OMB requirements, and

<sup>1</sup> GAO-11-278, *High Risk Series - An Update*, February 2011.

<sup>2</sup> DHS-OIG, *Use of DHS Purchase Cards*, (OIG-11-101, August 2011).



the Department's purchase card manual and components' guidance were incomplete and inconsistent. Based on our audit, the Department's Office of the Chief Financial Officer has initiated corrective actions to improve internal controls over the purchase card program.<sup>3</sup>

The Department can also improve management of its use of strategic sourcing. In March 2011, we found that the Department did not have a logistics process in place to facilitate strategic sourcing of detection equipment. Strategic sourcing would require that management standardize equipment purchases for explosive, metal, and radiation detection equipment; identify common mission requirements among components; and develop standard data elements for managing the inventory accounts of detection equipment. Improving its management of detection equipment will offer the Department opportunities to streamline the acquisition process and improve efficiencies.<sup>4</sup>

Although the Federal Emergency Management Agency (FEMA) has developed and strengthened acquisition management policies and processes, it continues to face challenges. Weak internal controls resulted in multi-million dollar contracts with vague and questionable requirements.<sup>5</sup> In addition, task monitors, agency employees responsible for managing and monitoring the contractors, had not received written guidance or training on how to evaluate contractor performance or certify billing invoices. Substantial improvements are needed in FEMA's oversight of contracts, including the prompt implementation of corrective actions.

In response to presidentially-declared disasters, FEMA's Public Assistance-Technical Assistance Contract firms (PA-TACs) provide technical assistance to state, local, and tribal governments awarded grants to fund debris removal and repair structures such as schools, medical facilities, and bridges. The *Brooks Act*<sup>6</sup> requires engineering and architectural firms to be selected based on competency, qualifications, and performance, but FEMA chose between its three PA-TACs with the goal of ensuring the firms were paid equal sums over the life of their FEMA contracts. FEMA had no performance measures for its PA-TACs and failed to monitor or evaluate their performance. FEMA's contract files were not in compliance with regulations. Insufficient oversight of the contracts creates an environment ripe for waste, fraud, and abuse.<sup>7</sup>

#### Acquisition Workforce

DHS made progress in the recruitment and retention of a workforce capable of managing a complex acquisition program. The number of procurement staff has more than doubled since 2005. In addition, participation in the Acquisition Professional Career Program, which seeks to develop acquisition leaders, increased 62% from 2008 to 2010. Nevertheless, DHS continues to face workforce challenges across the Department.

<sup>3</sup> DHS-OIG, *Improving FEMA's Disaster Purchase Card Program*, (OIG-10-91, May 2010).

<sup>4</sup> DHS-OIG, *DHS Department-wide Management of Detection Equipment*, (OIG-11-47, March 2011).

<sup>5</sup> DHS-OIG, *Improving FEMA's Individual Assistance, Technical Assistance Contracts*, (OIG-11-114, September 2011), and *Improvements Needed in FEMA's Management of Public Assistance-Technical Assistance Contracts*, (OIG-11-02, October 2010).

<sup>6</sup> *Brooks Architect-Engineer Act*, 40 U.S.C. §1101, et seq.

<sup>7</sup> DHS-OIG, *Improvements Needed in FEMA's Management of Public Assistance-Technical Assistance Contracts*, (OIG-11-02, October 2010).



According to GAO, the United States Coast Guard (Coast Guard) reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent,<sup>8</sup> and had filled 832 of its 951 acquisition positions as of November 2010. Although acquisition workforce vacancies have decreased, program managers have ongoing concerns about staffing program offices. For example, the HH-65 Aircraft Program Office had only funded and filled 10 positions out of an identified need for 33 positions. Also, according to its August 2010 human-capital staffing study, program managers reported concerns with staffing adequacy in program management and technical areas. To make up for shortfalls in hiring systems engineers and other acquisition workforce positions for its major programs, the Coast Guard uses support contractors, which constituted 25 percent of its acquisition workforce as of November 2010.

FEMA continues to make progress in the recruitment and retention of a workforce capable of managing complex acquisition programs. However, significant challenges remain. Acquisition staff turnover in FEMA has exacerbated file maintenance problems and resulted in multimillion-dollar contracts not being managed effectively or consistently. One of FEMA's challenges is hiring experienced contracting officers to work at disasters. The majority of FEMA staff at a disaster site work on an on-call, intermittent basis. FEMA categorizes all its disaster assistance employees in the occupational series 301, regardless of the function the employee will perform for FEMA. As such, a Disaster Assistance job announcement will not appear in a search for open contracting officer positions, limiting FEMA's ability to attract seasoned contracting officers. Secondly, by being categorized as a 301, Disaster Assistance contracting officers will only be able to administer contracts up to \$150,000. Thirdly, the Office of Personnel Management has allowed waivers for retired annuitants who return classified as contracting officers; however, these same waivers are not available to employees classified as 301s. Consequently, Disaster Assistance employees classified as 301s are not encouraged to continue working after the first 120 days after a disaster declaration. This increases turnover, which is detrimental to smooth contract execution.<sup>9</sup>

FEMA has made great strides in improving its contracting officer's technical representatives (COTRs) cadre. FEMA has dedicated staff to oversee the COTR program; developed a tiered system, which ties training requirements to dollar values of contracts a COTR can monitor; and established an intranet site containing tools for COTRs' use. However, many trained COTRs have never been assigned a contract, and are unsure of their ability to be effective doing so. And, although they represent the contracting officer, the COTR's appraisal is completed by their supervisor in their program office, rather than the applicable contractor officer, thus leading to divided loyalties.<sup>10</sup>

<sup>8</sup> GAO-11-480, *Coast Guard: Opportunities Exist to Further Improve Acquisition Management Capabilities*, April 2011.

<sup>9</sup> DHS-OIG, *FEMA's Contracting Officer's Technical Representative Program*, (OIG-11-106, September 2011).

<sup>10</sup> DHS-OIG, *FEMA's Contracting Officer's Technical Representative Program*, (OIG-11-106, September 2011).



## Knowledge Management and Information Systems

DHS made progress in deploying an enterprise acquisition information system and tracking key acquisition data. The Department's acquisition reporting system of record, known as nPRS (next-Generation Period Reporting System), tracks components' level 1, 2, and 3 acquisition investments. It also has capabilities to store key acquisition documents, earned value management information, and risk identification. Component personnel are responsible for entering and updating information, which includes cost, budget, performance, and schedule data. However, components did not complete and report all key information in nPRS. In *DHS Oversight of Component Acquisition Programs*,<sup>11</sup> we reported that only 7 of 17 programs (41%) reported Acquisition Program Baseline required milestones. These milestones establish the acquisition cost, schedule, and performance values. Only 13 (76%) programs reviewed contained required key documentation such as a mission needs statement, acquisition plan, operational requirements document, and integrated logistics support plans.

## INFORMATION TECHNOLOGY MANAGEMENT

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

### IT and Cyber Security

During our FY 2010 *Federal Information Security Management Act*<sup>12</sup> (FISMA) evaluation, we reported that the Department continued to improve and strengthen its security program. Specifically, the Department implemented a performance plan to improve on four key areas: Plan of Action and Milestones (POA&Ms) weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. Although the Department's efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. Management oversight of the components' implementation of the Department's policies and procedures needs improvement in order for the Department to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system certification and accreditation.

Further, over the past year, we have reported on the challenges specific components face in strengthening IT security. For example, in July 2011, we reported that the Transportation Security Administration (TSA) has implemented effective physical and logical security controls to protect its wireless network and devices.<sup>13</sup> However, we identified high-risk

<sup>11</sup> DHS-OIG, *DHS Oversight of Component Acquisition Programs*, (OIG-11-71, April 2011).

<sup>12</sup> Title III of the *E-Government Act of 2002*, Public Law 107-347.

<sup>13</sup> DHS-OIG, *Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices*, (OIG-11-99, July 2011).



vulnerabilities involving TSA's and Federal Air Marshal Service's patch and configuration controls. In September 2011, we reported that U.S. Customs and Border Protection (CBP) needs to strengthen enterprise wireless infrastructure security by remediating its open POA&Ms in a timely manner, enabling the wireless intrusion detection system to protect its network, and by performing regular vulnerability assessments to evaluate the effectiveness of wireless security.<sup>14</sup> In March 2011, we reported on the steps the U.S. Citizenship and Immigration Services (USCIS) needs to take to protect its systems and information from the IT insider threat posed by employees and contractors.<sup>15</sup> Specifically, USCIS needs to institute an enterprise risk management plan and incorporate insider threat risk mitigation strategies into its new business processes, institute a logging strategy to preserve system activities, and consistently enforce employee exit procedures.

In the area of cybersecurity, we reported in June 2011 that the National Protection and Programs Directorate (NPPD) has made progress in sharing cybersecurity threat information and raising cybersecurity awareness.<sup>16</sup> However, significant work remains to address the open actions and recommendations and attain the goals outlined in *The National Strategy to Secure Cyberspace*, National Infrastructure Protection Plan, and Comprehensive National Cybersecurity Initiative. In addition, NPPD must ensure that systems personnel receive required Protected Critical Infrastructure Information training and that configuration and account access vulnerabilities are mitigated to protect the department's critical infrastructure information and sensitive data.

### **IT Management**

Management of IT to ensure that it integrates well with other department-wide systems and federal partner agency systems and that it supports users' needs fully has been a challenge for several components. For example, the United States Coast Guard's command center and partner agency systems are not sufficiently integrated.<sup>17</sup> These limitations had a variety of causes, including technical and cost barriers, aging infrastructure that is difficult to support, and stove-piped system development. As a result, field personnel relied on inefficient workarounds to accomplish their mission. Additionally, the IT systems developed by DHS to share information between DHS and state and local fusion centers did not support their needs fully.<sup>18</sup> For example, the Homeland Security Information Network and the Homeland Security State and Local Community of Interest systems, both developed by DHS, are not integrated. As a result, users must maintain separate accounts, and information cannot easily be shared across the systems. Fusion center personnel also expressed concern that there were too many federal information sharing systems that were not integrated.

<sup>14</sup> DHS-OIG, *Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure*, (OIG-11-118, September 2011).

<sup>15</sup> DHS-OIG, *Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services (Redacted)* (OIG-11-33, January 2011).

<sup>16</sup> DHS-OIG, *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure*, (OIG-11-89, June 2011).

<sup>17</sup> DHS-OIG, *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG-11-108), September 2011).

<sup>18</sup> DHS-OIG, *Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain* (OIG-11-04, October 2010).



In addition, several components involved in IT transformation activities did not have updated IT strategic plans to help guide IT investments decisions. For example, the U.S. Secret Service's IT strategic plan had not been updated since 2006 and did not reflect and guide its modernization efforts, address identified IT weaknesses, or integrate its IT with the DHS-wide enterprise infrastructure.<sup>19</sup> In addition, FEMA's IT strategic plan was not comprehensive enough to coordinate and prioritize its modernization initiatives and IT projects.<sup>20</sup> The plan did not include clearly defined goals and objectives, nor did it address program office IT strategic goals.

DHS and its components also face challenges in upgrading their respective IT infrastructures, both locally and enterprise wide. In February 2011, we reported that CBP did not properly plan and implement the System Availability project, which was aimed at upgrading the local area networks at over 500 locations.<sup>21</sup> Specifically, it did not ensure that adequate funding was available, include all at-risk sites, or develop planning documents needed to justify project requirements and cost. Subsequently, CBP ran out of funding and ended the project in February 2010. As a result, hundreds of field sites did not receive the needed upgrades and remain vulnerable to network outages.

Additionally, in September 2011, we reported that the Department has made some progress toward consolidating the existing components' infrastructures into OneNet, the Department's wide area network initiative.<sup>22</sup> Specifically, it has established a centralized Network Operations Center/Security Operations Center incident response center and established a redundant network infrastructure and offers essential network services to its components. However, the Department still needs to establish component connections (peering) to OneNet and ensure that all components transition to the redundant trusted Internet connection.

### Privacy

DHS continues to face challenges to ensure that uniform privacy procedures and controls are properly addressed and implemented throughout the lifecycle of each process, program, and information system that affects personally identified information (PII). In May 2011, we reported that USCIS demonstrated an organizational commitment to privacy compliance by appointing a privacy officer, establishing its Privacy Office, and making progress in implementing a privacy program that complies with privacy laws. However, we identified specific areas in privacy training, as well as technical and physical safeguards, to improve the protection of PII and the overall culture of privacy.<sup>23</sup>

<sup>19</sup> DHS-OIG, *U.S. Secret Service's Information Technology Modernization Effort (Redacted)* (OIG-11-56, March 2011).

<sup>20</sup> DHS-OIG, *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69, April 2011).

<sup>21</sup> DHS-OIG, *Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project (Redacted)* (OIG-11-42, February 2011).

<sup>22</sup> DHS-OIG, *DHS Continues to Face Challenges in the Implementation of Its OneNet Project* (OIG-11-116, September 2011).

<sup>23</sup> DHS-OIG, *U.S. Citizenship and Immigration Services Privacy Stewardship* (OIG-11-85, May 2011).





## EMERGENCY MANAGEMENT

Although FEMA has made great strides in improving its disaster preparedness and recovery, challenges remain, including in the areas of emergency support functions, mass care and debris removal.

### Emergency Support Functions

The National Response Framework is a guide to how the Nation conducts all-hazards response. FEMA is the coordinator or primary agency for eight Emergency Support Functions and is responsible for ensuring that activities for these functions are accomplished as outlined in the National Response Framework. In November 2010, we released a report evaluating FEMA's readiness to fulfill its Emergency Support Function roles and responsibilities.<sup>24</sup> The review focused on three major areas of responsibility: (1) Coordination with Emergency Support Function Stakeholders, (2) Operational Readiness, and (3) Financial Management.

We found that FEMA generally fulfilled its roles and responsibilities under the Emergency Support Functions. Specifically, the agency manages mission assignments, executes contracts, and procures goods and services for its Emergency Support Function activities. We also concluded, however, that the agency can improve its coordination with stakeholders and its operational readiness. For example, FEMA should be coordinating with stakeholders for all Emergency Support Functions. There was little evidence that support agencies were regularly included in planning meetings for Emergency Support Function 3: Public Works and Engineering, even though agency officials said that such coordination would be beneficial. The agency must coordinate these activities with all relevant federal departments and agencies, state and local officials, and private sector entities to effectively execute the Emergency Support Function mission.

FEMA also should be fully prepared to provide community assistance after a disaster. At the time of our review, it was not conducting long-term recovery exercises, and one Emergency Support Function did not have clearly defined procedures to identify and deploy needed recovery services to disaster affected communities. FEMA did include a long-term recovery component in the National Level Exercise 2011. FEMA told us that since our report, they have increased engagement with Emergency Support Function partner agencies and have reinvigorated the Emergency Support Function Leadership Group.

### Mass Care and Emergency Assistance

We evaluated FEMA's progress in two Emergency Support Function sections: mass care and emergency assistance.<sup>25</sup> Mass care includes sheltering, feeding, emergency first aid, distribution of emergency items, and collecting and providing information on victims to family members. Emergency assistance is the assistance necessary to ensure that immediate

<sup>24</sup> DHS-OIG, *Assessment of Federal Emergency Management Agency's Emergency Support Function Roles and Responsibilities*, (OIG-11-08, November 2010).

<sup>25</sup> DHS-OIG, *Opportunities to Improve FEMA's Mass Care and Emergency Assistance Activities*, (OIG-11-77, April 2011).



needs beyond the scope of the traditional mass care services are addressed. These services include evacuation support, aid and services to special needs populations, reunification of families, as well as a host of other evacuation, sheltering, and other emergency services, as well as coordination of voluntary agency assistance.

FEMA continues to improve its mass care and emergency assistance program. It has coordinated more effectively with state and local governments and voluntary organizations; developed planning tools to build the mass care and emergency assistance capacities of these governments and organizations; and created an internal infrastructure to plan, coordinate, and provide direct mass care and emergency assistance, as needed.

While FEMA has taken steps to improve, additional actions are needed to ensure that the program is implemented effectively in future disasters. Mass care and emergency assistance standard operating procedures are in draft form, years after being developed. The effectiveness of developed planning tools and initiatives have not always been evaluated. Mass care and emergency assistance activities have not always been included in national and regional exercises. In addition, an opportunity exists for improved efficiency by creating automated computer interfaces between FEMA and American Red Cross National Shelter System databases. Each of these databases track sheltering information needed during a disaster. At this time, these two databases do not interface.

#### **Debris Removal Operations**

FEMA's Public Assistance program has expended more than \$8 billion over the past 11 years reimbursing applicants, primarily cities and counties, for removing debris resulting from natural disasters. In general this has been a successful effort; vast amounts of debris have been removed and disposed of, allowing communities to proceed with recovery efforts. Better planning, contracting, and oversight of debris removal operations, however, would enable these operations to be conducted in a more cost-effective manner.

Debris planning allows communities to be better prepared for a disaster by identifying debris collection and disposal sites, preparing debris removal contracts, and identifying potential debris contractors in advance of a disaster. Only a minority of states and local governments currently have such plans in place. A pilot program that operated in 2007–2008 was successful in encouraging the development of debris plans, but this momentum has been lost since the pilot program ended.

Decisions made in the first few days after a disaster strikes are critical in determining the success of a debris removal operation. Despite improved federal and state efforts to ensure that local governments are prepared for debris removal operations, they are often unprepared. FEMA debris advisers can help local governments determine what needs to be done, but qualified advisers are not always available when needed.

While FEMA has made significant strides in this area, opportunities remain for further improvement. Federal disaster response teams need to address debris expertise. Debris removal guidance is often unclear and ambiguous. Finally, an integrated performance



measurement system would provide federal and state officials and stakeholders with the data and tools to measure, analyze, and improve debris operations in a fact-based manner.

FEMA will be consolidating and updating the *Debris Monitoring Guide* and the *Debris Policy and Management Guide* into a single, comprehensive *Debris Policy and Management Guide* which will include detailed contracting guidance in FY 2012. FEMA will continue to make debris training available through the Emergency Management Institute, FEMA regional offices, and online. In addition, FEMA is currently developing a computer-based training course on debris management plan development that will be available to the public in FY 2012.

Since 2005, FEMA has worked to develop automated digital systems that will enhance FEMA's debris estimating and data collection capabilities in the field. FEMA is also developing a debris cost database to assist Public Assistance staff and applicants in determining whether a cost is reasonable. The debris cost database will also allow FEMA to analyze costs for debris operations across FEMA regions, disasters, states, and contractors. FEMA plans to implement these systems in FY 2012.

#### **Fraud Prevention**

Between January and September 2011, 10 separate billion dollar disasters have occurred in the United States.<sup>26</sup> The speed with which FEMA disburses individual and household disaster assistance results in the program's susceptibility to fraud. FEMA has established a Fraud Prevention and Investigation Branch to assist in the prevention and detection of fraud, but its operations are hindered by inadequate staffing and a lack of the latest technology tools to detect fraud. FEMA needs to improve its internal controls, provide fraud prevention training to all employees and support the Fraud Branch.<sup>27</sup>

<sup>26</sup> National Climate Data Center, <http://www.ncdc.noaa.gov/oa/reports>, accessed September 13, 2011.

<sup>27</sup> DHS-OIG, *Assessment of FEMA's Fraud Prevention Efforts*, (OIG-11-84, May 2011).



## GRANTS MANAGEMENT

FEMA's grants management and oversight infrastructure is challenged by the need to improve monitoring of grantees.<sup>28</sup> FEMA has taken the following steps to improve grants management and its oversight infrastructure:

- Began a multi-year effort to improve programmatic and financial monitoring. The Programmatic Grants Monitoring Improvement Initiative will expand and enhance programmatic monitoring capacity, as well as form comprehensive plans for future grants monitoring. In conjunction with this initiative, FEMA has launched a web-based system for its non-disaster grants, called ND Grants, to consolidate the entire preparedness (non-disaster) grants management lifecycle into a single system. In addition, the initiative will transition monitoring data to a web-based environment that will allow for greater ease of use, more sophisticated analytics, and greater data coordination with other reporting efforts. To enhance financial monitoring, FEMA has refined criteria for deciding which grants to monitor, standardized Regional financial monitoring activities, and expanded ongoing oversight activities to ensure early identification of issues.
- Increased regional management of grant programs to improve customer service to grantees, increase grants administration efficiencies, and build more robust regions. A recent GAO review indicates that FEMA is making progress in managing regionalization of preparedness grants.
- Established performance measures for the FY 2011 Homeland Security Grant Program and the Emergency Management Performance Grant Program, and is in the process of creating metrics for the remaining preparedness grant programs. FEMA states that internal and external management and administrative performance measures are being developed to track how well grants are being managed. However, until FEMA finalizes these measures, we are unable to evaluate their effectiveness.

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

### Disaster Grants Management

While FEMA does not directly manage subgrants, it is incumbent on FEMA to make certain that States, as grantees, understand the rules and regulations that govern disaster grants and ensure that subgrantees adhere to these. We issued a report in August 2011 that recapped the reports we issued in FY 2010 and presented some of the most common findings that lead to questioned costs, including improper contracting practices, inadequate subgrantee contract monitoring, costs not adequately supported, and ineligible work and project charges. We

<sup>28</sup> *The Post Katrina Emergency Management Reform Act of 2006* centralized most of DHS' grant programs under FEMA's Grant Programs Directorate (GPD).



also reported five instances in which grantee management could be improved. Grantees: (1) did not have procedures in place to ensure that cash advances to subgrantees were expended timely and excess funds were recovered promptly, (2) did not have a documented or standard payment processing policy or needed to strengthen controls to prevent overpayments, (3) had no procedures in place to follow up on material deficiencies reported in Single Audits, (4) were unaware of significant budget and scope increases, or (5) did not adequately monitor and report subgrantee program performance.

In FY 2011, we issued 61 subgrant audit reports with nearly \$308 million in questioned costs and over \$23 million in funding that could be deobligated or collected and be put to better use.

### **Preparedness Grants Management**

FEMA faces challenges in mitigating redundancy and duplication among preparedness grant programs, including barriers at the legislative, departmental, and state levels. The preparedness grant application process risks being ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects. We made recommendations designed to improve the management of these grant programs, with which FEMA agreed. In FY 2010, FEMA added Operation Stonegarden to the cluster of programs comprising the Homeland Security Grant Program. For FY 2011, activities previously included in the former Buffer Zone Protection Program and Interoperable Emergency Communications Program became eligible in the Homeland Security Grant Program.

FEMA should be able to accomplish our recommendations by addressing the specific grant-related recommendations of the October 2010 report of the congressionally mandated Local, State, Tribal and Federal Preparedness Task Force. However, until FEMA finalizes implementation plans with target dates for the Task Force recommendations, we cannot adequately evaluate the corrective actions to our recommendations.

Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*, required the OIG to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the audits we have completed to date, we have determined that the states have generally done an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used. We have identified several instances of states, as grantees, insufficiently monitoring subgrantee compliance with grant terms. Further, most states could not clearly document critical improvements in preparedness as a result of grant awards. In addition, we noted a need for improvement in the areas of timeliness of grant fund obligations and expenditures, compliance with procurement and inventory requirements, and identification of long-term capability sustainment options.



## FINANCIAL MANAGEMENT

In FY 2010, the Department committed to obtaining a qualified opinion on the Balance Sheet and Statement of Custodial Activity. To that end, DHS continued to improve financial management in FY 2011 and has achieved a significant milestone. For FY 2011, DHS was able to produce an auditable balance sheet and statement of custodial activity; and the independent auditors rendered a qualified opinion on those financial statements. However, challenges remain. In order to sustain or improve its opinion, the Department must continue remediating the remaining control deficiencies. Additionally, in FY 2012 the auditors could identify additional control deficiencies in areas that had not been tested previously due to the increase in audit scope to all of the financial statements. Additional deficiencies could also cause the department to lose its opinion.

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

During FY 2010, the independent auditors identified four department-wide control environment weaknesses that had a pervasive impact on the effectiveness of internal controls over consolidated financial reporting. In FY 2011, the independent auditors noted that only one of the four conditions still existed – the Department's financial information technology system infrastructure is aging and has limited functionality, which is hindering the Department's ability to implement efficient corrective actions and produce reliable financial statements. This issue is further discussed in the Information Technology Controls and Financial Systems Functionality section below.

The independent auditors noted that the DHS civilian components continued to make some progress in the remediation of IT findings that were reported in FY 2010. The Department closed approximately 31% of prior year IT findings. In FY 2011, the independent auditors issued approximately 135 findings, of which more than 65% are repeated from last year.

The remaining significant component-level challenges are primarily at the Coast Guard. In FY 2011, the Coast Guard made progress with implementing aspects of its *Financial Strategy for Transformation and Audit Readiness (FSTAR)* in the areas necessary to assert to



the auditability of its balance sheet, except for Property, Plant, & Equipment (PP&E), environmental liabilities, and related effects on other balance sheet line items. FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012.

### Managerial Cost Accounting

The Department does not have the ability to provide timely cost information by major program, and strategic and performance goals as required by Office of Management and Budget Circular No. A-136, *Financial Reporting Requirements*, as amended. The Department does not have financial management systems that allow for the accumulation of costs, at the consolidated level, by major program, or allow for the accumulation of costs by responsibility segments that align directly with the major goals and outputs described in the entity's strategic and performance plans. Further, the Department has not developed a plan to implement managerial cost accounting, including necessary information systems functionality. Currently, the Department must use manual data calls to collect cost information from the various components and compile data on a consolidated basis.

The OIG conducted several audits during FY 2011 and found that a number of components did not have the ability to provide various cost data when requested. For example:

- In January 2011, we reported that CBP was unable to capture or track data related to the time officers and agents spend specifically on transportation and guard services for illegal aliens. Not having this data available prohibited CBP from having complete cost information to determine the most cost effective solution.<sup>29</sup> *U.S. Customs and Border Protection's Ground Transportation of Detainees*, OIG-11-27, January 2011.
- In March 2011, we issued a report on CBP's Efficacy of Controls Over Drug Seizures. During the course of the audit we learned that CBP was unable to estimate the cost of its drug seizure efforts.<sup>30</sup> *CBP's Efficacy of Controls Over Drug Seizures*, OIG-11-57, March 2011.
- In September 2011, we reported that the Coast Guard did not accurately capture and bill all indirect costs incurred for the Deepwater Horizon oil spill response effort. The results of the audit found that Coast Guard had adequate internal controls, policies, and procedures to accurately bill direct costs from the Deepwater Horizon oil spills, but the unprecedented size of the spill challenged its existing processes for capturing indirect costs and revealed weaknesses in these processes. The Coast Guard did not have adequate policies, procedures, and internal controls to ensure that indirect costs are verified using Coast Guard official systems of record.<sup>31</sup> *United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill*, OIG-11-115, September 2011.

<sup>29</sup> DHS-OIG, *U.S. Customs and Border Protection's Ground Transportation of Detainees*, (OIG-11-27, January 2011).

<sup>30</sup> DHS-OIG, *CBP's Efficacy of Controls Over Drug Seizures*, (OIG-11-57, March 2011).

<sup>31</sup> DHS OIG, *United States Coast Guard's Internal Controls and Cost Capturing for the Deepwater Horizon Oil Spill*, (OIG-11-115, September 2011).



### ***Anti-Deficiency Act Violations***

The Department continues to have challenges with complying with the *Anti-Deficiency Act* (ADA). As of September 30, 2011, the Department reported six instances of potential ADA violations in various stages of review within the Department and its components.

Management at the Coast Guard continues to work toward resolving four potential ADA violations, one of which was identified during FY 2011. Those potential ADAs relate to (1) funds may have been used in advance of an approved apportionment from OMB, (2) funds used for construction and improvement projects, (3) funds that were inappropriately used for modifications to fixed price contract, and (4) the improper execution of the obligation and disbursement of funds for the lease of passenger vehicles.

### **Financial Statements Audit**

The following six items present the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2010. Each item is divided into two categories: (1) Military – Coast Guard, and (2) Civilian – all other DHS components. These six items represent the six material weaknesses identified during the independent audit of the FY 2010 DHS consolidated balance sheet and statement of custodial activity. Five of the six weaknesses continued to exist throughout FY 2011 and were again noted in the FY 2011 Independent Auditors' Report. In FY 2011, the Fund Balance with Treasury material weakness was downgraded to a significant deficiency. Further, DHS made some progress in two of the material weaknesses, and accordingly, those conditions were narrowed in scope. Specifically, DHS corrected the weakness conditions related to financial management, but not the deficiencies related to financial reporting; hence, financial management and reporting was reduced to financial reporting. Additionally, the auditors noted improvement in internal controls over Actuarial Liabilities, primarily because Coast Guard was able to assert to over \$40 billion of actuarial liabilities. Coast Guard continues to have significant challenges in Environmental and Other Liabilities, which resulted in a material weakness for the Department during FY 2011. For a complete description of the internal control weaknesses identified in the FY 2010 audit, see OIG-11-09.<sup>32</sup> To determine the status, we compared the material weaknesses reported by the independent auditor in FY 2010 with those identified in FY 2011.<sup>33</sup>

Based on the consolidated result of the six financial management areas included in the report, DHS has made measurable progress overall in financial management.

<sup>32</sup> DHS-OIG, *Independent Auditors' Report on DHS' FY 2010 Financial Statements and Internal Control over Financial Reporting*, (OIG-11-09, November 2010).

<sup>33</sup> DHS-OIG, *Independent Auditors' Report on DHS' FY 2011 Financial Statements and Internal Control Over Financial Reporting*, (OIG-12-07, November 2011).





### **Financial Reporting**

Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period.

- **Military:**

In previous years, the independent auditors noted that the Coast Guard had several internal control deficiencies that led to a material weakness in financial reporting. To address the material weakness conditions, the Coast Guard developed its *Financial Strategy for Transformation and Audit Readiness*, which is a comprehensive plan to identify and correct conditions that are causing control deficiencies. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2010 included: (1) lack of sufficient financial management personnel to identify and address control weaknesses; and (2) lack of effective policies, procedures, and controls surrounding the financial reporting process.

The Coast Guard has made progress in remediating the numerous internal control weaknesses identified by the independent auditor during FY 2010 in financial reporting. The Coast Guard implemented new policies and procedures, and automated tools to improve internal controls and the reliability of its financial statements. This effort has allowed the Coast Guard to assert to the auditability of all balance sheet accounts except property, plant and equipment and environmental liabilities. However, the Coast Guard does not have properly designed, implemented, and effective policies, procedures, processes, and controls surrounding its financial reporting process. Further, the FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2012. Consequently, components of the financial reporting deficiencies reported in the past remain uncorrected at September 30, 2011.

- **Civilian:**

In FY 2010, the independent auditors identified department-wide control weaknesses that have a pervasive effect on the effectiveness of internal controls over consolidated financial reporting. The auditors also found financial reporting internal control deficiencies at FEMA and TSA. Taken together, these deficiencies contributed to a departmental material weakness.

During FY 2011, the Department made progress overall in addressing the department-wide control weaknesses over consolidated financial reporting. The independent auditors noted that during FY 2011, FEMA corrected control deficiencies that contributed to the overall material weakness. Although TSA continued to make progress by hiring property accounting personnel and completing reconciliation of its balance sheet accounts, it has not fully developed its financial reporting process with sufficient policies, procedures, and internal controls to ensure reliability of certain significant financial statement balances. Further, in FY 2011, control deficiencies at USCIS



contributed to the Department's material weakness in financial reporting. The auditors noted that in FY 2011, the Department implemented a change in accounting treatment of certain user fees collected by USCIS. The change resulted in the correction of an error in the presentation of user fees as reported in previous years, and identification of a control weakness in the financial reporting process. The auditors also noted that USCIS did not have sufficient policies and procedures or documentation supporting the process used to develop adjustments to deferred revenue. These combined internal control deficiencies contributed to the Department's financial reporting material weakness in FY 2011.

### **Information Technology Controls and Financial Systems Functionality**

IT general and application controls are essential for achieving effective and reliable reporting of financial and performance data.

- Military:

A number of the Coast Guard's challenges in financial reporting are due to the lack of an effective general ledger system. The Coast Guard currently uses multiple systems that do not comply with the requirements of the *Federal Financial Management Improvement Act*.

In previous years the independent auditors noted that one of the most significant IT issues at the Coast Guard that could affect the reliability of the financial statements related to the development, implementation, and tracking of IT scripts, and the design and implementation of configuration management policies and procedures.

During FY 2011, Coast Guard focused on improving documentation with the script change control process and implemented the final module of the script change management tool initiated in FY 2010. While the independent auditors noted that some previously identified control deficiencies were remediated, other deficiencies continued to exist. Coast Guard's core financial system configuration management process and financial system functionality remained a challenge to Coast Guard's ability to assert to all financial sheet balances during FY 2011. The auditors noted that the IT security access and configuration management controls were not operating effectively, and continued to present risks to DHS financial data confidentiality, integrity, and availability. Financial system functionality is inhibiting the Coast Guard's ability to implement and maintain internal controls supporting financial system data processing and reporting.

The independent auditors also reported that financial data in the general ledger might be compromised by automated and manual changes that are not adequately controlled. The changes are implemented through the use of an IT scripting process, which was instituted as a solution to address functionality



and data quality issues. However, the controls over the script process were not properly designed or implemented effectively.

Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls necessary to support accurate and reliable financial data. For example, existing limitations impair Coast Guard's ability to maintain adequate posting logic transaction codes to ensure that transactions are recorded in accordance with U.S. generally accepted accounting principles.

- Civilian:

During FY 2010, the independent auditor identified IT control weaknesses in five areas that continued to present risks to the confidentiality, integrity, and availability of DHS' financial data: (1) access controls, (2) configuration management, (3) security management, (4) contingency planning, and (5) segregation of duties. Additionally, the independent auditors noted that in some cases financial system functionality inhibited DHS' ability to implement and maintain or install internal controls. These combined internal control deficiencies contributed to the Department's financial management and reporting material weakness in FY 2010.

For FY 2011, DHS has made limited progress overall in correcting the IT general and applications control weaknesses identified in the FY 2010 Independent Auditors' Report. During FY 2011, DHS and its components corrected approximately 31% of the IT control weakness conditions that the auditors had identified in prior years. Coast Guard, FEMA, Federal Law Enforcement Training Center (FLETC), and ICE made the most progress in remediating the IT control weaknesses. Although conditions improved at Coast Guard, FEMA, FLETC, and ICE, conditions at CBP deteriorated during the year. The majority of new control deficiencies the independent auditors identified during the year were at CBP.

The auditors noted that at the end of FY 2011, over 135 IT control weakness conditions existed, of which more than 65% are repeat from last year. Approximately 25% of the repeat findings were for IT deficiencies that management represented were corrected during FY 2011.

The auditors noted that many of the financial systems in use at DHS components have been inherited from the legacy agencies and have not been substantially updated since DHS' inception. As a result, ongoing financial system functionality limitations are contributing to the Department's challenges in addressing systemic internal control weaknesses and strengthening the overall control environment.

The FY 2011 Independent Auditors' Report noted that the IT control weaknesses remained for the five areas and continued to present risks to the



confidentiality, integrity, and availability of DHS' financial data: (1) access controls, (2) configuration management, (3) security management, (4) contingency planning, and (5) segregation of duties.

### **Property, Plant, and Equipment**

DHS capital assets and supplies consist of items such as property, plant, and equipment, operating materials; and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.

- Military:

The Coast Guard maintains approximately 49% of the Department's PP&E, including a large fleet of boats and vessels.

For FY 2010, the independent auditors noted that the Coast Guard had difficulty establishing its opening PP&E balances primarily because of poorly designed policies, procedures, and processes implemented, combined with ineffective internal controls. PP&E was not properly tracked or accounted for many years preceding the Coast Guard's transfer to DHS in 2003.

Furthermore, the fixed asset module of the Coast Guard's Core Accounting System (CAS) was not being updated timely for effective tracking and reporting of PP&E on an ongoing basis. As a result, the Coast Guard was unable to accurately account for its PP&E, and provide necessary information to DHS' Office of Financial Management for consolidated financial statement purposes.

In FY 2011, the Coast Guard continued to execute remediation efforts to address PP&E process and control deficiencies, specifically those deficiencies associated with vessels, small boats, aircraft, and select construction in process projects. Remediation efforts are scheduled to occur over a multi-year timeframe beyond FY 2011. Consequently, the Coast Guard has made only limited progress in this area during FY 2011.

- Civilian:

During FY 2010, CBP and TSA contributed to a departmental material weakness in PP&E. The deficiencies at TSA were more severe than at CBP.

Although TSA made some progress in remediating control deficiencies during FY 2011, including having auditable beginning internal use software balance, it was unable to fully address all of the conditions that existed in FY 2010.

Consequently, the overall severity of its internal control weakness conditions remained throughout FY 2011. Likewise, although CBP demonstrated some progress in remediating control deficiencies during FY 2011, the auditors identified control deficiencies similar to those noted in the prior year. Further,



internal control deficiencies were identified in the Office of Management that contributed to the overall DHS material weakness.

### **Environmental and Other Liabilities**

Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including environmental, accounts payable, legal, and accrued payroll and benefits liabilities.

- Military:

The Coast Guard's environmental liabilities consist of environmental remediation, clean up, and decommissioning, and represent approximately \$973 million or 93% of total DHS environmental liabilities. Environmental liabilities are categorized as relating to shore facilities and vessels. Shore facilities include any facilities or property other than ships (e.g. buildings, fuel tanks, lighthouses, small arms firing ranges, etc).

The independent auditors noted that during FY 2011, the Coast Guard continued to implement a multi-year remediation plan to address process and control deficiencies related to environmental liabilities. As a result, the Coast Guard made limited progress in implementing policies and procedures. However, most of the control weakness conditions reported in the FY 2010 Independent Auditors' Report remained throughout FY 2011.

- Civilian:

No control deficiencies related to Environmental and Other Liabilities were identified at the civilian components in FY 2011.

### **Budgetary Accounting**

Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.

- Military:

The Coast Guard has over 80 Treasury Account Fund Symbol (TAFS) covering a broad spectrum of budget authority, including annual, multi-year, and no-year appropriations; and several revolving, special, and trust funds. Each TAFS with separate budgetary accounts must be maintained in accordance with OMB and Treasury guidance.

Many of the conditions that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2010 remained throughout FY 2011. For example, the Coast Guard has not fully implemented policies, procedures, and internal controls over its process for validation and verification of undelivered order balances.



- Civilian:

For FY 2010, internal control weaknesses at CBP and FEMA contributed to a material weakness in budgetary accounting for the Department.

During FY 2011, the Department demonstrated moderate progress in correcting the budgetary accounting material weakness. The independent auditors noted that corrective actions CBP implemented during FY 2010 continued to be effective throughout FY 2011. Additionally, during FY 2011 FEMA continued to improve its processes and internal control over the obligation and monitoring process. However, some control deficiencies remained at FEMA. The control deficiencies at FEMA, combined with those at Coast Guard resulted in an overall material weakness in the area for the Department.

#### **Fund Balance with Treasury**

Fund Balance with Treasury (FBWT) represents accounts held at the Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency's FBWT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of various U.S. Government financial reports, and providing a more accurate measurement of budget resources.

- Military:

FBWT at the Coast Guard represents approximately 11% of total DHS FBWT. During FY 2010, the independent auditors reported a material weakness in internal control over FBWT at the Coast Guard. During FY 2011, the Coast Guard corrected several significant control deficiencies around FBWT. As a result, Coast Guard was able to assert to the completeness, existence, and accuracy of FBWT.

However, the Coast Guard continues to have FBWT control deficiencies. For example, Coast Guard does not have a process in place to provide transaction-level supporting documentation for all reconciling items. Consequently, some of the weakness conditions that were reported in FY 2010 remain throughout FY 2011. The auditors consider the remaining weaknesses to be less severe, but still important enough to require management's attention.

- Civilian:

No control deficiencies related to FBWT were identified at the civilian components in FY 2011. Corrective actions implemented in previous years continued to be effective throughout FY 2010 and FY 2011.



## INFRASTRUCTURE PROTECTION

The need to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, and minimize incident consequences complicates protection efforts for all critical infrastructure and key resources and remains a great challenge for DHS.

### Risk Assessment Efforts in the Dams Sector

Dams and related structures are especially important because one catastrophic failure at some locations could affect populations exceeding 100,000 and have economic consequences surpassing \$10 billion. We reviewed the Department's risk assessments effort in the Dams Sector<sup>34</sup> to determine whether the Office of Infrastructure Protection has taken steps to assess risk at the most critical dam assets, and followed up to ensure that recommendations were implemented. We found the Department lacks assurance that risk assessments were conducted and security risks associated with critical dam assets were identified and mitigated. The Department did not: (1) review all critical dam asset risk assessments conducted by other agencies, (2) conduct security reviews for 55% of the critical dam assets, or (3) ensure that corrective actions were completed to mitigate risk when security gaps were identified.

DHS was unable to complete these tasks because it does not have the authority to ensure that security partners participate in risk management activities or that dam owners undergo departmental assessments and implement corrective action. The National Infrastructure Protection Plan prescribes a partnership approach between government and the private sector to voluntarily manage risk. Underlying legislation does not give the Department the necessary authority to ensure that security partners participate in risk management activities, or that dam owners undergo departmental assessments and implement corrective action. DHS could not always obtain cooperation from its security partners and dam owners and did not always collaborate successfully. This collaborative approach can be successful only if security partners and dam owners work together to perform risk management. The Assistant Secretary, Office of Infrastructure Protection, agreed with our recommendation to determine the appropriateness of a legislative proposal to establish regulatory authority for the critical Dams Sector assets similar to the Chemical Sector. Specifically, DHS personnel need authority to review risk assessments, conduct inspections when assessments are deficient, and make recommendations for corrective actions.

## BORDER SECURITY

Securing the Nation's borders from the illegal entry of aliens, contraband, terrorists and weapons of mass destruction, while welcoming all legitimate travelers and trade, continues to be a major challenge. DHS apprehends hundreds of thousands of people and seizes volumes of illicit cargo entering the country each year. DHS is responsible for securing the 7,000 miles of international borders that the United States shares with Canada and Mexico.

<sup>34</sup> DHS-OIG, *DHS Risk Assessment Efforts in the Dams Sector*, (OIG-11-110, September 2011).



### **Western Hemisphere Travel Initiative**

To address the challenge of facilitating the entrance of legitimate travelers while securing the Nation from illegal entry of aliens and terrorists, DHS and Department of State implemented the Western Hemisphere Travel Initiative (WHTI). WHTI requires citizens of the United States, Canada, Bermuda, and Mexico arriving at air, land and sea ports of entry to present passports or other approved documents to enter the United States. CBP is not prepared to fully enforce the new document requirement at land ports of entry. CBP has acquired and deployed substantial technological tools to aid in inspecting travelers arriving at land ports of entry. However, CBP has not analyzed the impact that a substantial increase in secondary inspection workload will have on secondary inspection staffing and infrastructure during full enforcement. The reported WHTI compliance rates during the initial eight-month informed compliance period indicate noncompliant travelers arriving at the agency's 39 busiest land ports may increase the secondary inspection workloads at these ports by an average of 73% if all noncompliant travelers required secondary inspections. Also, the agency has not finalized the operating procedures its officers will use to verify the identity and citizenship of noncompliant travelers.<sup>35</sup>

CBP's implementation of the WHTI document requirements have improved the agency's ability to validate the identity and citizenship of compliant air passengers, allowing officers to spend more time inspecting travelers without passports. However, there is inadequate assurance that CBP officers "verified" the identity and citizenship of all individuals who failed to provide a passport or other WHTI-compliant documentation. CBP officers did not always document the basis for their decisions to admit air passengers who were noncompliant with the new document requirements. Also, CBP officers did not always follow the agency's policy for referring all noncompliant passengers to a secondary inspection area for a more thorough review.<sup>36</sup>

### **Information Sharing on Foreign Nationals: Overseas Screening**

DHS has implemented several programs to screen foreign nationals while they are still overseas. These programs rely on biographical, biometric, and documentary information in the Department's and other federal data systems. In our FY 2011 report, *Information Sharing on Foreign Nationals: Overseas Screening (Redacted)*,<sup>37</sup> we evaluated whether levels of cooperation, resources, and technology were adequate for Department officers to assess the risks posed by foreign nationals who seek to enter the United States. We also reviewed plans to consolidate and improve information in the Department's data systems. The Department has made progress in evaluating admissibility of foreign nationals before they travel to the United States. The level of cooperation among components that conduct overseas screening is high. Headquarters support offices have long-term plans to streamline

<sup>35</sup> DHS-OIG, *Customs and Border Protection's Implementation of the Western Hemisphere Travel Initiative at Land Ports of Entry*, (OIG-11-16, November 2010).

<sup>36</sup> DHS-OIG, *Customs and Border Protection Needs To Improve Its Inspection Procedures for the Western Hemisphere Travel Initiative* (OIG-11-43, February 2011).

<sup>37</sup> DHS-OIG, *Information Sharing On Foreign Nationals: Overseas Screening (Redacted)*, (OIG-11-68, April 2011).





access to information in the Department's data systems, and improve screening and data analysis capabilities. However, DHS initiatives face serious resource and technological challenges. Information is fragmented among more than 17 data systems, and officers must conduct labor intensive, system-by-system checks to verify or eliminate each possible match to terrorist watch lists and other derogatory information.

CBP's National Targeting Center is challenged by insufficient staff and difficult working conditions. Effective small-scale screening and interdiction programs need sufficient resources to meet operational needs and congressional mandates. We made 18 recommendations to standardize the technology used to share information in Departmental data systems, enable federal officers to obtain and use the most current and complete data available, and improve information sharing procedures. Departmental components concurred with 17 of the 18 recommendations. However, for five recommendations with which components concurred, including three that would increase productivity for thousands of DHS employees, components said that they would need to request additional resources in the next federal budget cycle to implement the recommendations.

## TRANSPORTATION SECURITY

TSA is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. The Nation's economy depends upon secure, yet efficient transportation security measures. Although TSA is making progress, it continues to face challenges with strengthening security for aviation, mass transit and other modes of transportation.

### Passenger and Baggage Screening

TSA's screening of persons and property continues to be a vital element of the overall aviation security system. The *Aviation and Transportation Security Act*<sup>38</sup> requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our covert testing of carry-on baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not cleared for loading onto a passenger aircraft.<sup>39</sup> The same report identified needed improvements for TSA's Advanced Imaging Technology.

### Airport Badging Process Oversight

TSA's responsibilities include ensuring that employees working in secured airport areas are properly vetted and badged. The agency relies on designated airport operator employees to perform the badging application process. We reported that individuals who pose a threat may obtain airport badges and gain access to secured airport areas.<sup>40</sup> We analyzed vetting

<sup>38</sup> Public Law 107-71, November 19, 2001.

<sup>39</sup> DHS-OIG, *Evaluation of Newly Deployed and Enhanced Technology and Practices at the Passenger Screening Checkpoint (Unclassified Summary)* (OIG-10-75, March 2010).

<sup>40</sup> DHS-OIG, *TSA's Oversight of the Airport Badging Process Needs Improvement (Redacted)* (OIG-11-95, July 2011).



data from airport badging offices and identified badge holder records with omissions or inaccuracies pertaining to security threat assessment status, birthdates, and birthplaces.

These problems exist because TSA has designed and implemented only limited oversight of the application process. Specifically, the agency did not (1) ensure that airport operators have quality assurance procedures for the badging application process; (2) ensure that airport operators provide training and tools to designated badge office employees; and (3) require its Transportation Security Inspectors to verify the airport data during their reviews.

### **Passenger Air Cargo Security**

Approximately 7.6 million pounds of cargo are transported on passenger planes each day. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably “known” either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. Through covert testing, we identified vulnerabilities in the cargo screening procedures employed by air carriers and cargo screening facilities to detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.<sup>41</sup> Although TSA has taken steps to address air cargo security vulnerabilities, our undercover audit demonstrated that the agency does not have assurance that cargo screening methods always detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.

### **Training**

Transportation Security Officers screen passengers, carry-on baggage, and checked baggage to prevent prohibited objects from being transported on aircraft. TSA can improve its management of the training program for the screening workforce.<sup>42</sup> The agency needs to develop and document standard processes to (1) use officer test results to evaluate training program results; (2) assign on-the-job training responsibilities; and (3) evaluate workforce and training needs to ensure that officers have the tools and time necessary to complete training requirements.

TSA did not establish a lead office to organize and coordinate Transportation Security Officer training until 2006. The agency issued a management directive designating the Operational and Technical Training Division responsible for the overall management of the analysis, design, development, and implementation of Transportation Security Officer training programs. However, the division did not assume an active leadership role until 2009 due to its need to maintain current training levels and respond to emerging threats. Without a documented process for updating training based on screener performance data and changes in technology or equipment, the TSA may be missing opportunities to enhance its officers’ skills and abilities.

---

<sup>41</sup> DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft*. (OIG-10-119, September 2010).

<sup>42</sup> DHS-OIG, *Transportation Security Administration’s Management of Its Screening Workforce Training Program Can Be Improved* (OIG-11-05, October 2010).



### **Rail and Mass Transit**

Passenger rail stations are attractive terrorist targets because of the large number of people in a concentrated area. Amtrak provides passenger rail service for about 27 million passengers every year, using approximately 22,000 miles of rail in 46 states and the District of Columbia. We identified that grant recipients, such as Amtrak, transit agencies, and state and local authorities, coordinate risk mitigation projects at high-risk rail stations. However, Amtrak is not always using grant funds to implement mitigation strategies at the highest risk rail stations, in terms of casualties and economic impact.<sup>43</sup> Amtrak has not mitigated critical vulnerabilities reported in risk assessments. These vulnerabilities remain because TSA (1) did not require Amtrak to develop a corrective action plan addressing its highest ranked vulnerabilities; (2) approved Amtrak investment justifications for lower risk vulnerabilities; and (3) did not document roles and responsibilities for the grant award process.

The Transportation Sector Network Management, Mass Transit and Passenger Rail Division, needs to work closely with Amtrak to establish a corrective action plan that ensures decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by previous risk assessments. The Transportation Sector Network Management, Mass Transit and Passenger Rail Division needs to create and report internal procedures that describe how the agency will carry out its roles and responsibilities in the grant award process for ensuring that Amtrak and other grant recipients address the highest priority security vulnerabilities.

## **TRADE OPERATIONS AND SECURITY**

CBP is charged with the dual mission of securing the Nation's borders, while facilitating legitimate trade and travel. While CBP continues to take action in this area, challenges remain with strengthening internal controls over revenue and protecting our Nation from security threats.

### **Customs Revenue**

Customs revenue remains the second largest source of revenue for the U.S. government. CBP collected an estimated \$32 billion in duties, fees, and taxes (revenue) in FY 2010, an increase of 9.5% over FY 2009. In the current economic environment, it is imperative CBP ensure that participating importers comply with federal trade requirements and that government revenues are protected. In 2010 and 2011, OIG conducted revenue audits of the Importer Self Assessment program<sup>44</sup> and the Single Transaction Bonds process<sup>45</sup> and found significant issues remain with oversight of these programs. The Importer Self Assessment program was initiated in 2002 as a voluntary approach to trade compliance. It is based on the

<sup>43</sup> DHS-OIG, *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations (Redacted)* (OIG-11-93, June 2011).

<sup>44</sup> DHS-OIG, *Customs and Border Protection's Importer Self-Assessment Program*, (OIG-10-113, August 2010).

<sup>45</sup> DHS-OIG, *Information Technology Management Letter for the Federal Emergency Management Agency Component for the FY 2009 DHS Integrated Audit*, (OIG-10-92, May 2010).



premise that importers with strong internal controls achieve the highest level of compliance with federal trade laws and regulations and require less enforcement review and oversight. Our most recent review highlighted several areas where improvement can be made, including establishing and enforcing policies and procedures to document management controls and assessing risks to trade compliance.

Further, we noted that CBP needs to improve internal controls over the Single Transaction Bonds process which protects CBP from revenue loss when importers fail to fulfill their financial obligations. In 2011, the OIG conducted an audit of CBP's Single Transaction Bond program and found that from FY 2007 through FY 2010, CBP lost \$46.3 million in revenue because of inaccurate, incomplete, or missing bonds. We recommended that CBP develop a risk based approach that includes identification, assessment, and mitigation of the risk of revenue loss associated with the single transaction bonding process.

### **Cargo Security**

Ensuring that only legitimate cargo is allowed entry into the United States while facilitating the free flow of trade remains a challenge. Based on our FY 2010 audits, *CBP's Cargo Targeting and Examinations*<sup>46</sup> and *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*,<sup>47</sup> we concluded that targeting and examination of high risk shipments continues to be a challenge for CBP. For example, CBP needs to update its guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats and conduct a risk assessment to determine which pathways pose the highest risk.

The Free and Secure Trade (FAST) program is a commercial clearance program for known low-risk shipments entering the United States from Canada and Mexico. FAST allows for expedited processing of entities that have completed background checks and fulfill certain eligibility requirements. Improvements are needed in CBP's initial enrollment process for carriers to ensure that only low-risk carriers are allowed to participate in the FAST program. Highway carriers that did not meet all Custom-Trade Partnership against Terrorism's minimum security requirements have been certified to receive FAST program benefits. Also, the CBP Vetting Center and Trade Partnership against Terrorism supply chain security specialists did not always follow established procedures when determining the initial eligibility of highway carriers.<sup>48</sup>

Developing and maintaining a multi-layered risk based approach to trade security is a significant challenge. Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* requires DHS to screen all cargo destined for the U.S. that is loaded on or after July 1, 2012. Over the past two years, CBP and DHS have raised concerns to Congress about the feasibility of 100% screening and have advocated for continuing to use a

<sup>46</sup> DHS-OIG, *Cargo Targeting and Examinations*. (OIG-10-34, January 2010).

<sup>47</sup> DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*. (OIG-10-01, October 2009).

<sup>48</sup> DHS-OIG, *Improvements Needed in the Process to Certify Carriers for the Free and Secure Trade Program* (OIG-11-25, March 2011).



risk-based approach to meet the intent of mitigating high risk cargo. Regardless of whether DHS formally adopts 100% screening or continues to use its risk-based approach to trade security, DHS must ensure that it has adequate resources, infrastructure, and processes. DHS must also be able to reach agreement with the international community to resolve issues concerning corresponding resources, oversight, costs, timing, and enforcement considerations, as well as a process to resolve disagreements as they arise.



**Appendix A**  
**Report Distribution**

---

**Department of Homeland Security**

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

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate



#### ADDITIONAL INFORMATION AND COPIES

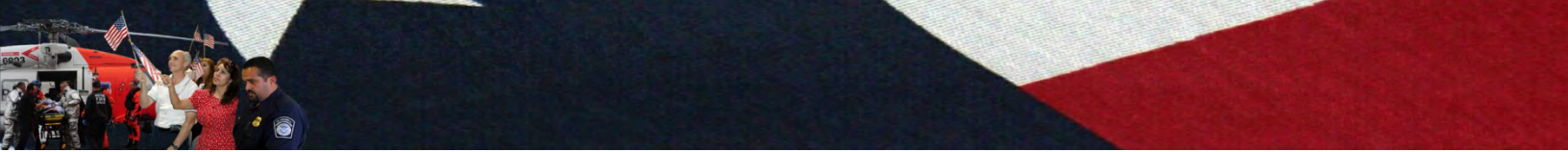
To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, e-mail your request to our OIG Office of Public Affairs at [DHS-OIG.OfficePublicAffairs@dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@dhs.gov), or visit our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

#### OIG HOTLINE

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

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

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



## Management's Response

*The Reports Consolidation Act of 2000* (P.L. 106-531) requires that, annually, the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) prepare a statement summarizing the major management challenges facing the Department and an assessment of the Department's progress in addressing those challenges. For Fiscal Year (FY) 2011, the OIG has identified the Department's major challenges in nine broad areas:

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

DHS carries out multiple complex and highly diverse missions. While the Department continually strives to improve the efficiency and effectiveness of its programs and operations, as progress is achieved, new management challenges arise.

Overcoming major management challenges requires long-term strategies for ensuring stable operations, sustained management attention, and resources. This section of the report details the Department's efforts to address each of the aforementioned challenges and the plans it has in place to overcome specific issues highlighted by the OIG.

### ***Challenge #1: Acquisition Management***

An effective acquisition management infrastructure is essential to support the Department's mission. Effective acquisition management requires having the people, policies, and systems in place to ensure taxpayer assets are effectively and efficiently utilized. This is accomplished by having a combination of people who are experts in various disciplines, including program management, policy, operations, contracting, engineering, information technology, logistics, business and financial management, cost analysis, and testing and evaluation. Recognizing this, DHS established a core of acquisition experts at the Department to perform the appropriate governance, as well as coaching, guidance, and support to help execute programs well on a day-to-day basis. To lead this effort and enhance the Department's ability to effectively provide capability to users in support of DHS goals and objectives, the Acquisition Program Management Division (APMD) was established within the Office of the Chief Procurement Officer (OCPO) in 2007 to lead DHS in matters relating to acquisition.

According to the OIG, the magnitude of the number, dollar value, and complexity of the Department's acquisition activities keeps acquisition management among its challenges. The OIG also points out that DHS continues to make progress in this area. We agree with both assessments and continue to work to improve our acquisition management infrastructure for providing oversight





of DHS's many complex and large-dollar procurements. The OIG identified the following challenges that need to be addressed: Organizational Alignment and Leadership; Policies and Processes; Acquisition Workforce; and Knowledge Management and Information Systems.

### **Sub-Challenge: Organizational Alignment and Leadership**

DHS agrees with the OIG's assessment that in FY 2011 the Department improved the acquisition program's organizational alignment and maintained strong executive leadership, but has room for further improvement. Specifically, there are several accomplishments we would like to highlight. For example, DHS acquisition management was reorganized to reflect a layered approach, with the Component chief acquisition executives and the heads of contracting activities reporting informally to the Under Secretary for Management (USM) and OCPO, respectively. In addition, in response to a U.S. Government Accountability Office (GAO) report, DHS has taken action to implement its Integrated Strategy for High Risk Management. Specifically, DHS has:

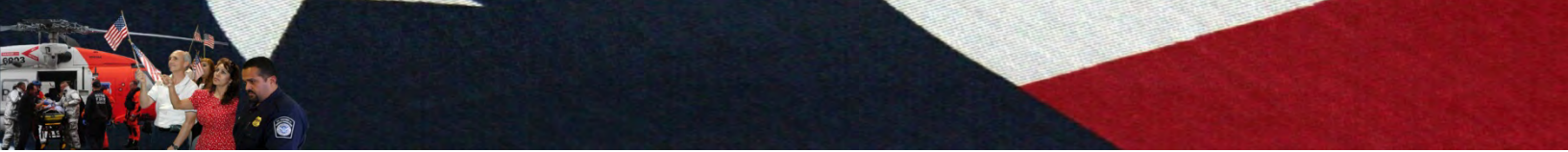
- Established the Program Accountability and Risk Management Office, reporting directly to the USM, combining the Acquisition Program Management Division and the Cost Analysis Division under one executive director;
- Completed a workforce study, the results of which have been used to augment acquisition staff for programs and Components;
- Completed a requirements definition for a decision support tool to improve business intelligence on programs (including tracking the efficacy of required actions resulting from oversight activities); and
- Begun chartering work for the implementation of the Integrated Investment Life Cycle Model (IILCM).

These actions have already established an improved acquisition management infrastructure, including much of what is needed to address GAO's concerns regarding workforce needs. DHS plans to complete implementation of IILCM as well as the first phases of the decision support tool deployment in FY 2012 in order to fully address GAO's and OIG's concerns regarding this management challenge.

### **Sub-Challenge: Policies and Processes**

DHS continues to develop and strengthen its acquisition management policies and processes. According to the OIG, the Department needs to provide detailed guidance and improve oversight and internal controls in some areas, such as the logistics process used to facilitate strategic sourcing of detection equipment. In response, the DHS Strategic Sourcing Program Office conducted a business case analysis to determine the feasibility of procuring detection equipment under a strategic sourcing vehicle(s). The business case concludes that strategic sourcing for detection equipment can potentially eliminate duplication and reduce costs by leveraging purchase volume.

On September 8, 2011, the USM established an Executive Steering Committee (ESC) and a Commodity Working Group (CWG) for detection equipment. The purpose of this initiative is to develop a coordinated approach and apply strategic sourcing principles to the acquisition and management of detection equipment.



Moving forward, the CWG will be responsible for developing a coordinated approach to acquiring and managing detection equipment as it implements a strategic sourcing solution and completes all necessary tasks (i.e., identify requirements, perform market research, and develop sourcing strategy). The ESC will be responsible for approving the final requirements, ensuring the CWG has adequate resources, and resolving any key issues encountered by the CWG.

A DHS-wide detection equipment contract will provide a vehicle for efficient acquisition and improved commodity management. Further, leveraging buying power for detection equipment will reduce costs for DHS and its Components. DHS anticipates a strategically sourced contract vehicle to be awarded in FY 2013.

### **Sub-Challenge: Acquisition Workforce**

DHS continues to make progress in recruiting and retaining a workforce capable of managing a complex acquisition program, as noted by the OIG, and will continue to evaluate workforce needs and make adjustments as appropriate to address this challenge. According to GAO, the U.S. Coast Guard reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent and filled 832 of its 951 acquisition positions as of November 2010. Following participation in a DHS-wide pilot, the U.S. Coast Guard was awarded a contract with Dayton Aerospace, Inc. to provide a Sustainment Acquisition Composite Model (S/ACOM) for project acquisition workforce staffing requirements. The model projects current and future year (5-year) requirements in accordance with the DHS Future Years Homeland Security Program and provides a functional breakout for all major system acquisition projects.

S/ACOM helped the U.S. Coast Guard identify and close a 100 full-time position (FTP) resource gap within its major systems acquisition workforce. Using direct/expedited hire authority for civilian recruitment and the current process for military personnel assignments, the U.S. Coast Guard has sufficient authority to reduce the 14-percent vacancy rate. The current staffing and acquisition certification level for U.S. Coast Guard major systems acquisitions is sufficient to successfully execute the programs as contained in the President's Budget Request for FY 2012. In addition, this request contains 17 new FTPs to strengthen oversight and meet the highest acquisition priorities in systems engineering, life-cycle logistics, test & evaluation, and business financial management. The U.S. Coast Guard will continue to use S/ACOM in their workforce planning efforts to project future requirements and to determine if current acquisition staffing is sufficient.

In addition, to help address a challenge identified by the OIG, FEMA recently revised its policy to allow disaster assistance employees performing contracting functions to be classified as General Schedule (GS)-1102, Contract Specialists. This will greatly improve FEMA's ability to attract and recruit experienced contracting officers with higher contracting authority to work at disaster sites. The change will also decrease turnover rates and allow for smooth contract execution.

### **Sub-Challenge: Knowledge Management and Information Systems**

DHS agrees with the OIG that the Department has made progress in deploying an enterprise acquisition information system and tracking key acquisition data. This progress is highlighted by reports from the Department's acquisition reporting system of record (nPRS), dated October 3, 2011, showing 13 of 17 programs having approved Acquisition Program Baselines and 2 more in final routing at the Department level. In addition, Components use this system to enter and update



acquisition documentation (i.e., cost, budget, performance, and schedule data). The system shows 15 of 17 programs have key acquisition documentation from Components, while the remaining 2 programs had the documentation prepared but not yet entered. These improvements were the result of a concentrated effort by APMD/Program Accountability and Risk Management in FY 2011 to ensure critical thinking for this program had been documented.

## ***Challenge #2: Information Technology Management***

DHS continues to work to enhance the Department's information management, and DHS Components have made progress in addressing challenges with these systems identified by the OIG and in providing greater assurance that DHS-held information is protected. The Chief Information Officer (CIO) will continue to provide oversight of IT systems consolidation efforts, including Enterprise Wireless Infrastructure (EWI) security, the OneNet Project, and the DHS Data Center.

### **Sub-Challenge: IT and Cybersecurity**

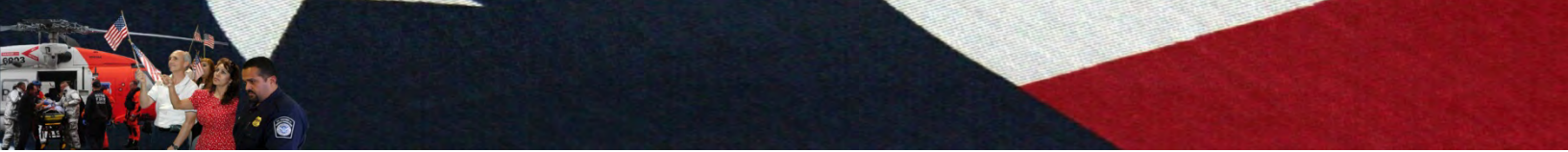
DHS agrees with the OIG that the Department has continued to improve and strengthen its security program but challenges still remain to further strengthen IT security. In January 2011, the Chief Information Security Officer (CISO) issued and implemented the *IT Security Continuous Monitoring Strategy: An Enterprise View v1.0* to meet OMB and National Institute of Standards and Technology (NIST) guidance.

U.S. Customs and Border Protection (CBP) has made considerable progress in strengthening EWI security to address a recent OIG recommendation that it needs to strengthen enterprise wireless infrastructure security by remediating its open Plan of Action and Milestones (POA&Ms). Specifically, CBP published policy and implemented guidance in 2009 for developing and implementing the CBP wireless security program. In July 2010, CBP certified and accredited EWI in accordance with processes outlined by NIST. The certification process for EWI included a review of all required documentation, such as a system security plan, risk assessment, and a system test and evaluation plan. In addition, CBP performed an independent security test and evaluation, and established wireless security configurations to protect wireless networks and devices against security vulnerabilities. Also, CBP included wireless security awareness in its annual security awareness and rules of behavior training.

CBP is addressing its open POA&Ms. To date, CBP reviewed and re-baselined the master POA&M list and schedule with the Information Systems Security Manager, to remediate which POA&Ms can be closed and to open new ones to reflect actions that are still needed to minimize potential security risks. Depending on funding approval timelines, CBP will commence with risk mitigation activities, procurement, and staffing actions.

In addition, CBP has enabled the wireless intrusion detection system but is not currently monitoring the system. CBP has a transition plan in place to monitor the system and has created a resource requirements request to obtain the necessary funding.

CBP has also set up vulnerability scans for all EWI Wireless Controllers. These scans will be conducted by CBP's wireless Information Systems Security Officer. CBP is developing a schedule



to ensure that vulnerability scans are conducted on a regular and recurring basis by December 2011.

In early February 2011, the U.S. Citizenship and Immigration Services (USCIS) Office of Security and Integrity (OSI) initiated a Risk Management Special Review to identify current risk management efforts across USCIS, gauge their effectiveness, and determine steps to be taken in order to coordinate and enhance enterprise risk management at USCIS. A charter and work plan were prepared, and OSI formed the Enterprise Risk Management Task Force. Staff members from OSI met with DHS risk management officials, attended risk management training, created a database for the project, and started a pilot risk management program within OSI. At the successful conclusion of the pilot, OSI will form a USCIS-wide task force to explore implementation of the program throughout USCIS.

Other accomplishments include appointment of a Senior Risk Executive to oversee the development of the USCIS Risk Management Office and to represent USCIS within the DHS Risk Management Office, and the completion of drafts currently under review by the Enterprise Risk Management Task Force, including:

- Management Directive that establishes authorities, responsibilities, and procedures;
- Process flow chart that outlines risk identification, mitigation, and information lines of communication; and
- White paper that outlines a general approach to establishing a risk management office and the steps necessary to establish an effective risk management process within USCIS.

In addition, USCIS is working with the Office of Transformation Coordination to establish requirements to enhance the Electronic Immigration System's (ELIS's) ability to address insider threats. DHS officials are actively engaged on the appropriate project teams to ensure additional internal risk mitigation strategies are addressed in ELIS. These requirements are currently planned for inclusion in the Release B of ELIS, which is scheduled to begin development late FY 2012.

The National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (NPPD/IP) works closely with the DHS Data Center to ensure its personnel receive protected critical infrastructure information (PCII) training. The PCII Program is an information-protection program that enhances information sharing between the private sector and the government. In addition, PCII is used by DHS and other federal, state, and local analysts to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures. All DHS Data Center personnel with access to NPPD systems that house PCII data have completed PCII training.

The DHS Data Center is responsible for ensuring the appropriate implementation of many of the security and system configuration controls associated with NPPD systems. In June 2011, the DHS CIO released an initial version of the Enterprise Common Controls, Data Center Two, Service Level Two guidance document, which is intended to supplement previous service agreements and clearly articulate which security and configuration controls are the responsibility of the DHS Data Center and how they should be implemented.



DHS, NPPD, and NPPD/IP information system security management personnel have reviewed current system security standards and documentation to achieve continued authority to operate until April 2014. In addition, when application configuration concerns are identified, they are addressed through business processes and/or software patch updates.

The National Cyber Security Division (NCSD) is the DHS entity with lead responsibility for implementing or coordinating, as appropriate, the National Strategy to Secure Cyberspace, National Infrastructure Protection Plan cybersecurity activities, and the Comprehensive National Cybersecurity Initiative. NCSD is developing a draft strategic plan that will include “performance measures that are aligned with its mission, as outlined in the Quadrennial Homeland Security and Bottom-Up reviews.” NCSD’s strategic plan is progressing through the approval process and includes a plan for developing implementation schedules for each goal within the strategic plan.

In addition, NCSD reports its performance on a quarterly basis against the measures it developed. At the same time, NCSD continuously assesses its current suite of measures and measure gaps, and then develops new measures to close identified gaps. Lastly, the Office of Cybersecurity and Communications is implementing corrective actions to address gaps identified by the OIG to ensure cybersecurity and communications programs are appropriately aligned and their overall performance is adequately assessed.

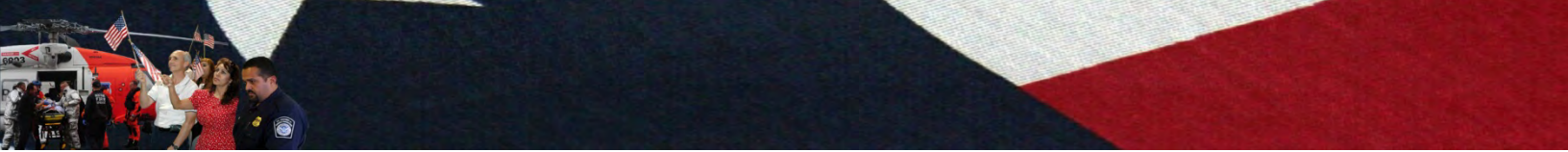
### **Sub-Challenge: IT Management**

DHS and its Components are working to address the OIG’s recommendations to overcome challenges in upgrading their respective IT infrastructures, both locally and enterprise-wide. DHS agrees with the OIG’s findings that the Department has made progress toward consolidating the existing Components’ infrastructures into OneNet, the Department’s wide area network (WAN) initiative.

CBP continues to assess various infrastructure upgrades and is preparing a project charter that will include the business priorities provided by the different CBP operational environments when service is disrupted. In addition, CBP is developing a network infrastructure operations and maintenance effort to: ensure end-to-end network connectivity and high rates of network availability; reduce single points of failure within the CBP infrastructure; establish a continuous technology refresh lifecycle for key hardware network and software network components; and forecast technology advances and alignments to CBP strategic objectives and the lines of business of the CBP key stakeholders.

To date, CBP has completed several IT initiatives that will ensure availability of the CBP infrastructure, which include: network (WAN/local area network) infrastructure upgrades at prioritized CBP sites; WAN optimization, which allows network traffic on the data circuit to increase the overall available circuit bandwidth and network performance; upgraded cabling; End-2-End monitoring platform for greater proactive monitoring of the CBP network; and mobile communications.

Several IT projects and activities are planned and/or underway that will address availability and connectivity of the network across CBP including its various operational environments. The projects are near term (0 to 2 years), midterm (2 to 5 years), or long term (5 to 10 years). The results of all projects will, at some level, contribute to high rates of network availability. All



projects depend on funding approval and will be prioritized on the basis of budget approvals and constraints.

### **Sub-Challenge: Privacy**

DHS agrees with the OIG that USCIS has demonstrated an organizational commitment to privacy compliance by establishing its Privacy Office, appointing a privacy officer, and making progress in implementing a privacy program that complies with privacy laws, but that the Department can do more to improve the protection of personally identifiable information (PII) and the overall culture of privacy.

The USCIS Office of Privacy has been hosting job-specific, advanced, or specialized privacy training courses. The Office of Privacy has hosted instructor-led privacy awareness training for all USCIS Headquarters employees and contractors on a monthly basis through the end of FY 2011 and is providing similar training at USCIS Regional, District, and Field offices. Further, the Office of Information Technology has incorporated privacy awareness information into the USCIS Computer Security Awareness Training and the USCIS IT Rules of Behavior. Both awareness mechanisms stipulate that all personnel must be able to identify PII and know the proper PII handling guidelines in accordance with the USCIS Office of Privacy's policies and procedures.

The USCIS Office of Privacy conducted Privacy Awareness Week in April 2011 to enhance the culture of privacy at the agency and increase employee awareness of privacy issues. It is also evaluating a series of videos addressing various aspects of privacy and expects to begin launching the videos in late November 2011.

In addition, OSI developed the USCIS Physical Security Inspection Workbook to assess security countermeasures and ensure consistent security standards and equipment are employed across USCIS. OSI completed three inspections at USCIS Headquarters facilities and piloted this workbook at seven locations in the field in FY 2011. In addition, OSI has partnered with Service Center Operations to conduct reviews of the four service centers to address any gaps in security systems and procedures that impact the protection of privacy information. OSI is evaluating the comments and results from these facility inspections and expects to finalize the workbook by the end of December 2012.

The Electronic Security Systems Nationwide Deployment Project has provided USCIS with measurable metrics to help determine whether a facility has adequate and functional security countermeasures (e.g., physical access control system, closed circuit television and intrusion detection systems). Further, in FY 2011, OSI made upgrades and improvements to these systems at both Headquarters and several regional facilities.

By the end of March 2012, the USCIS Privacy Office plans to incorporate a training page on the Office of Privacy's Intranet Web site. The training page will include links to privacy policy and guidance, training materials and presentations, Privacy-BLAST (newsletter), and upcoming training offerings and events.

The USCIS Privacy Office is finalizing a general privacy awareness training course targeted to all USCIS personnel (federal and contractor), which is expected to launch by November 30, 2011. It



also is developing specialized privacy awareness training course targeted to program or system managers and expects to have a beta version by December 2011.

To address issues regarding technical safeguards, the USCIS Office of Information Technology (OIT) has issued Public Key Infrastructure (PKI) certificates to 7,400 USCIS employees. OIT plans to continue to issue PKI certificates to all employees, ensure thumb drives are trackable property, issue a Management Directive on audit and accountability, and enhance the audit and monitoring capability of USCIS case management systems.

### ***Challenge #3: Emergency Management***

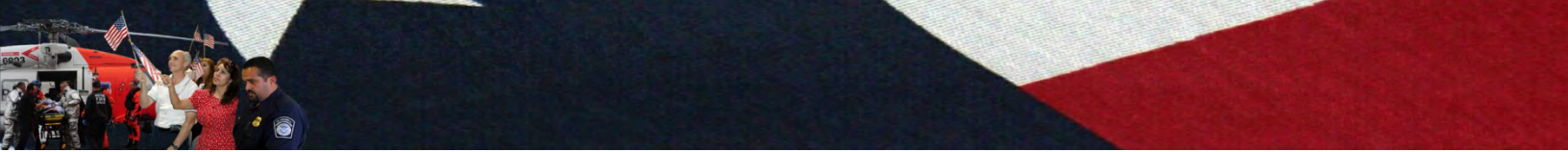
DHS agrees with the OIG that the Federal Emergency Management Agency (FEMA) has made great strides in improving its disaster preparedness and recovery. FEMA continues to work to improve, particularly in the areas identified by OIG as challenges. Specifically, DHS is working to make improvements in the emergency support function; implement and evaluate mass care and emergency standard operating procedures, tools, and initiatives; and provide debris removal expertise and guidance.

#### **Sub-Challenge: Emergency Support Function**

OIG stated that although FEMA generally fulfilled its roles and responsibilities under the Emergency Support Functions, the agency can improve its coordination with stakeholders and its operational readiness. FEMA is currently engaged in working-group activities with stakeholders to address this challenge. In October 2010, FEMA's Office of Response and Recovery launched an effort to reinvigorate the Emergency Support Function Leadership Group (ESFLG), the senior-level entity that coordinates responsibilities, resolves operational and preparedness issues, and provides planning guidance and oversight for interagency response and recovery activities. The goal of this effort—and the mission of the ESFLG—is to improve the effectiveness of coordinated federal response and recovery activities by engaging interagency leadership through a forum that fosters the exchange of information, planning, and decision-making.

ESFLG membership includes senior officials who can speak authoritatively on behalf of their respective organizations, including representatives from each of the 15 emergency support functions (ESFs). ESFLG meetings now serve as a vehicle to address issues that directly affect the roles and responsibilities of the ESFs as described in the National Response Framework and its annexes. Also in 2010, the revived ESFLG group managed FEMA's Whole Community planning effort—a worst-case, catastrophic disaster scenario affecting 7 million people and 25,000 square miles. Through its working group structure, the ESFLG identified 13 core capabilities and supporting objectives required for a rapid and effective response. The working groups then developed courses of action to close capability deltas in support of each capability. These capabilities were also tested through the participation of ESF members during National Level Exercise 2011: New Madrid Earthquake.

Building on the ESFLG's Whole Community efforts and in response to Presidential Policy Directive #8 (PPD-8), FEMA is leading the development of a Federal Interagency All-Hazards Response Plan, to include scenario-specific annexes that integrate prior earthquake, hurricane, and catastrophic planning efforts. Employing the Whole Community framework and the ESFLG



throughout PPD-8 efforts, FEMA seeks to integrate non-traditional response strategies required for catastrophic disasters. The final plan will comprehensively address coordinated federal support to regional, state, tribal, and local entities for all-hazard responses.

### **Sub-Challenge: Mass Care and Emergency Assistance**

FEMA is working to address OIG recommendations to implement and evaluate mass care and emergency standard operating procedures, tools, and initiatives by increasing the use of these items at exercises. For example, Mass Care activities were exercised at the National Level Exercise 2011. As part of the scenario, Mass Care services were coordinated and provided to 4 million people and 1.5 million pets in seven affected states. Mass Care task forces were deployed to support the survivors and affected states and individual assistance/technical assistance contractors were activated and mobilized to support survivors. All Mass Care tools, including contractors, agreements with other agencies and organizations, and other Mass Care partners were coordinated and used.

In addition, states are beginning to use some of the Mass Care tools. For example, in 2010, the Multi Agency Feeding Template and Task Force documents were used in Florida, and the National Mass Evacuation Tracking System was used in Maryland; in 2011, the Household Pets Task Force was used in Maine, and the interface of the Web-enabled Emergency Operations Centers was tested in Arkansas as part of the National Level Exercise 11.

FEMA and the American Red Cross are also working together to complete the interface of the two National Shelter System databases. Both agencies are working on an agreement and protocol that will facilitate the exchange. A software modification that will allow for both programs to exchange data has been completed.

### **Sub-Challenge: Debris Removal Operations**

DHS agrees with the OIG that FEMA's public assistance program has, in general, been a successful effort; vast amounts of debris have been removed and disposed of, allowing communities to proceed toward recovery unencumbered. FEMA is working to address its recommendations to improve planning, contracting, and oversight of debris operations to increase the cost-effectiveness of these operations.

While FEMA provides support for debris removal, including through reimbursements, state and local jurisdictions are ultimately responsible for debris removal.

FEMA agrees with the OIG on the benefits of the Public Assistance Pilot Program, specifically with regard to the initiative to provide an increased federal cost share for applicants with debris management plans. The authority provided by Congress to implement the pilot ended on December 31, 2008. After the pilot, FEMA assessed the pilot program and submitted a report to Congress. On the basis of those findings, FEMA is developing regulatory action to permanently implement the initiatives of the pilot.





## ***Challenge #4: Grants Management***

FEMA awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. FEMA is continuously working to enhance its grant management to include risk management principles and performance measures in order to determine how the preparedness grants have improved preparedness capabilities across the Nation.

### **Sub-Challenge: Disaster Grants Management**

FEMA's progress includes implementing a long-term approach to enhance financial monitoring within the regions. This approach implements risk management principles to direct scarce monitoring resources to grantees and programs with the most need. As part of a multi-year process, FEMA has refined criteria for deciding which grants to monitor, standardized Regional Financial monitoring activities, and expanded ongoing oversight activities to ensure early identification of issues. This approach builds on the established monitoring approach and will drive FEMA toward continuously advancing its grants management capability.

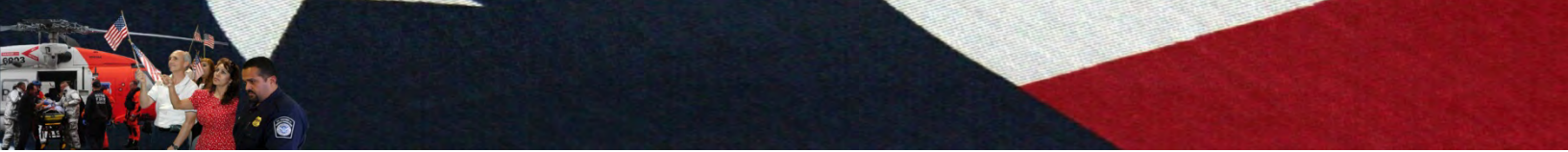
### **Sub-Challenge: Preparedness Grants Management**

FEMA has undertaken two initiatives to establish performance measures for the Preparedness Grant Programs. The Grant Programs Directorate is developing both internal and external management and administrative performance measures to track how well the grants are managed. In addition, the National Preparedness Division is building upon the performance metrics established in the Homeland Security Grant Program (HSGP) and Emergency Management Performance Grant and is creating metrics for the remaining preparedness grant programs. When finalized and combined, these two efforts to develop performance measures will allow FEMA to better manage and analyze the preparedness grant programs. Ultimately, these measures will help to determine how the preparedness grants have improved preparedness capabilities across the Nation.

FEMA continues to work with Congress, DHS Headquarters, and state grant administrators to consolidate grant programs in which activities are allowable under multiple grants. In the FY 2010 HSGP's Program Guidance, a fifth program, Operation Stone Garden, was added into the cluster of programs comprising HSGP. This was done to help streamline the application and award process. In FY 2011, the Buffer Zone Protection Program and the Interoperable Emergency Communication Program were no longer funded. Activities previously allowable under those programs are now eligible under the HSGP and Urban Area Security Initiative Program. Moving forward, FEMA will continue to address redundancies and identify opportunities to streamline grant programs where possible.

## ***Challenge #5: Financial Management***

DHS is dedicated to demonstrating good stewardship of taxpayer dollars. In January 2011, Secretary Napolitano committed to the goal of receiving a qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity in FY 2011. This level of confidence and support from our Secretary spoke volumes to all levels of financial management



throughout the Department and strongly reinforced all of our efforts to improve financial management at DHS.

From FY 2006–2011, DHS has reduced the number of audit qualifications from 10 to 1, Department-wide material weaknesses in internal controls over financial reporting from 10 to 5, and the number of Component conditions contributing to material weaknesses from 25 to 7. Although five material weaknesses remain, in most cases, the Department lessened the severity of the conditions, and corrected its material weakness condition in Actuarial Liabilities.

In FY 2011, the Department obtained a qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity. This means that for the first time since FY 2003, we can report to the public that most of the line items on the Department balance sheet are materially correct. We still face challenges, but we made significant progress in strengthening internal controls and implementing corrective actions within several key financial management areas. In FY 2011, the Department:

- Developed a more-robust risk management process, meeting with Components frequently to mitigate high-risk areas and to prevent new material weaknesses. We also developed a new technical accounting issues resolution process, wherein Components can communicate issues and work with the Department to determine the best path forward.
- Addressed financial management and business process challenges and shared best practices and lessons learned by identifying subject matter experts in critical risk areas and leveraging their expertise through cross-Component working groups. In addition, DHS updated its “Component Requirements Guide,” which contains approximately 40 standard financial reporting processes and provides guidance for implementing controls and reporting financial data.
- Analyzed the skill sets of essential financial management personnel and developed a plan to improve core competencies in key financial management areas. Implemented a new training program that in FY 2012 will offer courses to the financial management community in subjects ranging from appropriations law and federal accounting fundamentals to budget formulation/execution and the U.S. Standard General Ledger.
- Worked closely with Components to plan responses to IT notices of findings and recommendations, with a focus on FEMA and U.S. Coast Guard scripting issues. Because of a strong FY 2011 IT remediation process, we have reduced the severity of some areas of material weakness.
- Continued to refine and update the Financial Management Policy Manual to provide all DHS employees with standard processes to follow for budgetary policy, financial reporting, financial assistance, and travel and bank card management.

The gains made in financial management at DHS over the past few years are due to the hard work of dedicated employees at the DHS Office of the Chief Financial Officer and Components across the Department. We have put in place policies, processes, and structures to help ensure consistent operations for each of our financial accounting centers and financial management offices within DHS Components. Improvements made by the Components include corrective actions that increased the Department’s auditable balance sheet balances to approximately 90 percent in FY 2011.



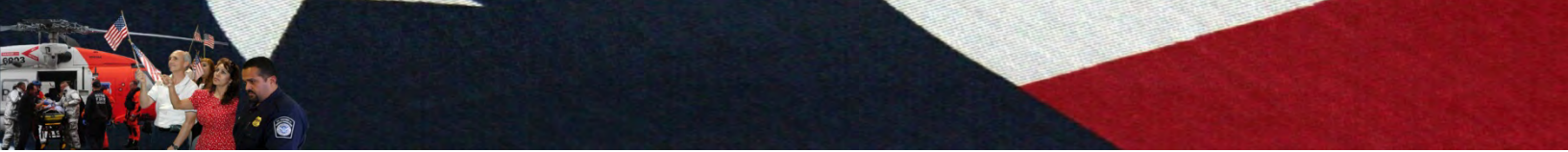
- Showing great commitment from senior leadership, the Commandant of the U.S. Coast Guard issued a memo to the U.S. Coast Guard community stressing the importance of implementing corrective actions in order to achieve success with the audit in FY 2011. By executing corrective action plans, implementing new processes, and monitoring risk throughout the fiscal year, the U.S. Coast Guard has been able to reach major milestones, making it possible for the Department to attain a balance sheet opinion in FY 2011.
- In FY 2007, the U.S. Coast Guard had disclaimer conditions on all balances. Since then, the U.S. Coast Guard has reduced its disclaimer conditions each year. This year, the U.S. Coast Guard asserted to all balance sheet items but Property, Plant, and Equipment and the associated impact on environmental liabilities and cumulative results of operations, representing a total of \$57.5 billion, or more than 80 percent of its balance sheet.
- Most significantly, the U.S. Coast Guard corrected a longstanding entity level control deficiency. This success is due to the Commandant's leadership in setting strong tone at the top and to delegating responsibility for internal control from senior management to all financial management staff levels and across business lines.
- In FY 2011, the Department's Financial Reporting material weakness was narrowed in scope because the U.S. Coast Guard implemented processes and procedures to support its financial statement balances. The U.S. Coast Guard also reduced the scope of its Financial Systems material weakness through corrective actions to improve computer scripts that impacted the accuracy of financial statements and consolidated the scope of its Environmental and Other Liabilities material weakness through elimination of another liability condition related to more than \$40 billion in medical retirement benefits.
- FLETC corrected its control deficiency in IT Controls and System Functionality; FEMA corrected its control deficiency in Financial Reporting; and CBP corrected control deficiencies in Budgetary Accounting and Entity-Level Controls. ICE reduced the severity of its control deficiency in IT Controls and System Functionality.

These successes have positioned DHS to be able to expand the audit to all of the financial statements in FY 2012. By taking a deeper dive into the financial statements, we will identify additional areas for corrective action, taking us further down the road toward a clean opinion on all financial statements.

While we have made progress, we recognize that significant internal control challenges remain. The Department's Deputy Chief Financial Officer will remain actively engaged with senior management and staff at each Component, overseeing corrective actions to ensure continued progress across the Department. The Department has several initiatives under way and planned to remediate internal control challenges.

### **Sub-Challenge: Managerial Cost Accounting**

The Department is determining best way to use and deploy managerial cost accounting (MCA) across the enterprise. We have chartered a cross-Component working group to assist Components in costing methodologies and developing a methodology to approximate full cost, as required by SFFAS No. 4, Managerial Cost Accounting. This group is studying the extent to which DHS is currently using MCA, with the goal of identifying best practices and defining Component requirements for implementation and reporting.



DHS is working to develop a consistent approach across Components for determining the full costs of program and missions at the individual program/mission activity level. Our goal is to be able to accumulate and consolidate these costs to align directly with the major goals and outputs described in the DHS strategic and performance plans (QHSR goals), and eventually enable Statement of Net Cost to be presented by major program/strategic goal in compliance with OMB Circular A-136.

In addition, DHS will continue to develop its strategy for deploying MCA Department-wide. This strategy will take some time to execute because full implementation of SFFAS No. 4 is highly dependent on financial systems. The Department is modernizing its core financial systems, implementing a common accounting structure, and developing data standards and business intelligence tools to collect and crosswalk cost data at program/project/activity level across Department Components.

DHS will ensure Mission Action Plans at key Components include long-term corrective actions and milestones related to the compliance with SFFAS No. 4 and the ability to report full costs at individual program/mission activity level that align directly with the Department's major programs/strategic goals.

### **Sub-Challenge: Antideficiency Act**

In FY 2011, the Department continued to implement its plan to improve compliance with the *Antideficiency Act* (ADA). This multi-year plan includes policy reviews, Department-wide training, and internal control test work to prevent ADA violations.

- In FY 2010, we completed a crosswalk of Component administrative control of funds policies to the Department-wide policy and initiated revisions to strengthen Department-wide funds controls.
- In FY 2011, we made significant progress ensuring appropriate controls are in place to prevent violations. As part of A-123 testing, the Department assessed Component-level internal controls over the Budget Resource Monitoring process to ensure controls are in place to prevent future ADA violations.
- In FY 2011, we offered several introductory and refresher courses in appropriations law, and we developed an online course scheduled for launch through Department and Component learning systems in the first quarter of FY 2012.

### **Sub-Challenge: Financial Statements Audit**

We recognize that maturing our Department is a collective effort, and we continue to implement initiatives to strengthen and mature the Department across many areas. The Department is preparing to move beyond the Balance Sheet to the other financial statements and to prepare for the Internal Controls Over Financial Reporting audit. We are working with Components to develop risk registers for the statements of budgetary resources, net cost, and custodial activity. We will continue to meet regularly with Components through the Financial Management Working Group, issue-specific working groups, and regular risk-management and audit status meetings to assess their progress executing corrective action plans.

In support of our goal of continued progress toward a clean audit opinion, the Department will:



- Continue targeted risk assessments to identify and remediate weaknesses in accounting and financial reporting.
- Partner with Components to design and implement corrective actions to prepare all financial statements for audit, to remediate weaknesses, and to ensure continued progress in FY 2012 and beyond.
- Expand pilot efforts to have the independent auditor use management’s internal control over financial reporting work, which will build additional audit efficiencies.

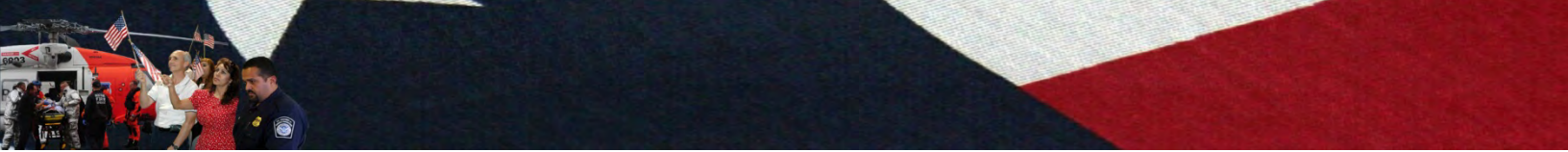
Modernize core financial management systems; establish standard, key business processes and internal controls; and implement a standard line of accounting across financial systems to ensure DHS sustains its audit progress. Progress that relies on manual processes may not be sustainable without such system improvements and standard processes.

### ***Challenge #6: Infrastructure Protection***

DHS works closely with federal partners and the private sector to deter threats, mitigate vulnerabilities, and minimize incident consequences for all Critical Infrastructure and Key Resources (CIKR). The OIG states that the need to coordinate with and rely on federal partners and the private sector presents a challenge for the Department but also an opportunity for DHS to engage people across the country in the protection and resilience of the nation’s infrastructure. DHS continues to support the voluntary framework developed in response to Homeland Security Presidential Directive 7, and the support of voluntary stakeholders has helped the Department with its achievements thus far. Although challenges remain, DHS continues to make significant progress to protect the nation’s CIKR. For example, NPPD/IP launched a strategic effort called the Critical Infrastructure Risk Management Enhancement Initiative, which will strengthen critical infrastructure protection and resilience across all sectors and regions. Its goal is to ensure that National Infrastructure Protection Plan critical infrastructure protection and resilience activities achieve outcomes that are developed on the basis of the most pressing risks and our effectiveness in managing those risks.

#### **Sub-Challenge: Risk Assessment Efforts in the Dam Sector**

DHS has identified, consistent with the National Infrastructure Protection Plan, the Nation’s most critical systems within the Dams Sector and has developed a risk assessment tool that combines all three functions of risk: threat, vulnerability, and consequence. While DHS does not have regulatory authority over the Dams Sector, it does provide public and private sector partners with education and training opportunities that offer guidance on protective measures and crisis management in addition to conducting vulnerability assessments that identify potential security improvements. Specifically, NPPD/IP collaborates with federal, state, local, and private sector partners on many initiatives and provides a wealth of information such as a cybersecurity roadmap to secure control systems; guidelines and training on security awareness, protective measures, and crisis management; an exercise program to enhance regional disaster resilience (Dams Sector Exercise Series); and vulnerability assessment products that identify potential areas for improvement and suggest protective measures that could be implemented on a voluntary basis. In addition, NPPD is working with stakeholders from industry and government to determine whether a legislative proposal should be made to address any critical gaps, addressing an OIG recommendation.



## ***Challenge #7: Border Security***

In March 2009, the Obama Administration launched the Southwest Border Initiative to bring focus and intensity to Southwest Border security, coupled with a reinvigorated, smart, and effective approach to enforcing immigration laws in the interior of our country. DHS is now more than two years into this strategy, and based on previous benchmarks set by Congress, it is clear that this approach is working.

Under the initiative, CBP has increased the number of Border Patrol agents deployed to the Southwest Border to more than 18,000, which is more than twice the number stationed in the region in 2004. In addition, DHS has doubled personnel assigned to Border Enforcement Security Task Forces, which work to dismantle criminal organizations along the border. The number of ICE intelligence analysts along the border focused on cartel violence has also increased. In all, a quarter of ICE's personnel are now in the region, the most ever. In addition, the number of border liaison officers assigned to work with their Mexican counterparts has tripled, and CBP is now screening all southbound rail traffic and a random number of other vehicles for illegal weapons and cash that are helping fuel the cartel violence in Mexico.

### **Sub-Challenge: Western Hemisphere Travel Initiative**

In 2009, DHS implemented the Western Hemisphere Travel Initiative (WHTI), a program that strengthens border security for land and sea travel to the United States, while facilitating legitimate travel and trade by requiring that U.S., Mexican, and Canadian citizens present a passport or other secure travel document<sup>1</sup> that denotes identity and citizenship when crossing the border. Prior to the implementation of WHTI, there was no documentary requirement for U.S. or Canadian citizens to enter the United States from within the Western Hemisphere; travelers could present any of numerous documents or simply make an oral declaration without presenting any documentation. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases. Today, due to WHTI, the national query rate is over 97 percent.

To support WHTI, DHS has worked with U.S. governors and Canadian government officials to develop state and provincial Enhanced Driver's Licenses (EDLs) that denote identity and citizenship for frequent border crossers, and with the Department of State to develop a wallet-sized U.S. Passport Card. Both documents, as well as others developed for WHTI, can be electronically verified with the issuing agency at the port of entry. CBP and Canada Border Services Agency also worked to expand enrollment in the NEXUS trusted traveler program. The United States has deployed Radio Frequency Identification technology readers at ports that cover 99 percent of inbound vehicle traffic at the Northern Border and allow the documents to be read as the traveler is approaching the inspection booth.

CBP is also working with tribes across the country on the development of Enhanced Tribal Cards (ETCs). To date, CBP has signed Memoranda of Agreement for the development of ETCs with the Kootenai Tribe of Idaho, the Pascua Yaqui of Arizona, the Tohono O'odham of Arizona, the Seneca Nation of New York, the Coquille of Idaho, and the Hydaburg of Alaska.

---

<sup>1</sup> WHTI-compliant documents include passports, U.S. passport cards, military identification cards, trusted traveler cards, Enhanced Driver's Licenses, and Enhanced Tribal Cards.



### **Sub-Challenge: Information Sharing on Foreign Nationals: Overseas Screening**

To enable officers and analysts to use a single sign-on for DHS systems used for screening foreign nationals, the DHS CIO developed the Identity, Credential, and Access Management Segment Architecture (version 1.0, March 31, 2010) and Information Sharing Segment Architecture (version 2.1, May 15, 2009), which identifies the requirement for single sign-on across multiple internal and external systems, including screening systems.

Additional resources are being developed to establish a portal on the secure Homeland Security Information Network (HSIN) through which authorized DHS users can log on to DHS Web-based databases to access information on foreign nationals. The DHS OCIO Information Sharing and Exchange Division is working with the Office of Operations (OPS) and I&A to build this functionality into the HSIN 3.0 rollout, scheduled for initial operating capability in the third quarter of FY 2012. Until then, OCIO is also working with OPS HSIN and I&A to put in place an interim capability.

In response to staffing issues identified by OIG, CBP National Targeting Center-Passenger (NTC-P) has identified the need for 55–75 new permanent CBP officer FTP and new, permanent managerial, support, and administrative FTP to support the additional staff. The 55–75 new positions are needed to adequately staff new or enhanced targeting programs, including pre-departure screening, Advanced Targeting Team initiatives, outbound targeting, Visa re-vetting, and expanded Immigration Advisory Program operations. The officers would be spread across three shifts, to cover a 24-hour period. The allocation of officers to specific shifts and targeting programs is continually evaluated. The President's FY 2012 budget request includes funding for multiple enhancements to the NTC-P, including for the hiring of additional staff. As of September 30, 2011, 179 officers are on full-time or temporary duty. A full complement of staff should be achieved by FY 2013.

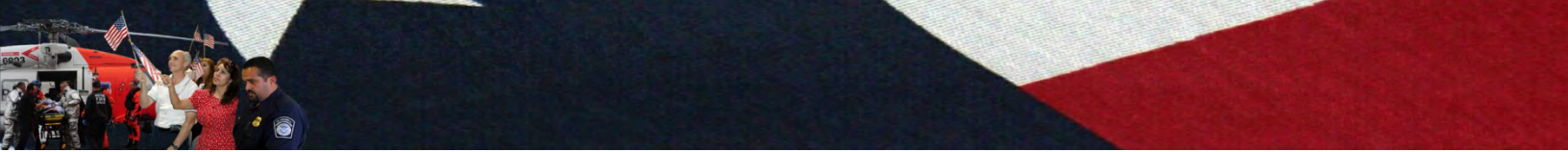
The NTC-P has implemented a variety of changes to promote staff retention, including: improvements to the hiring process and postings of vacancy announcements; implementation of employee recognition and communications initiatives; establishment of permanent shifts with rotating long weekends; establishment of a permanent training team; periodic rotations through multiple programs; and participation in the Student Career Experience Program, which provides student interns with a paid work experience that may make them eligible for permanent employment upon graduation from their academic institution.

### ***Challenge #8: Transportation Security***

According to the OIG, TSA is making progress in meeting the challenges of transportation security. However, it remains a challenge for TSA to establish effective security strategies while facilitating the legitimate flow of passengers and cargo.

### **Sub-Challenge: Passenger and Baggage Screening**

TSA appreciates the OIG's work to identify opportunities to further enhance TSA's checkpoint program. TSA continuously enhances its screening technologies and procedures to address evolving threats to our Nation's transportation systems. The best defense against threats to our



transportation systems remains a risk-based, layered security approach that uses a range of measures, both seen and unseen. After analyzing the latest intelligence and studying available technologies and other processes, TSA determined that Advanced Imaging Technology (AIT) is the most effective method to detect metallic and non-metallic threat items concealed on passengers. In addition, TSA is in the process of upgrading its AIT units with Automatic Target Recognition. This will enhance AIT units' detection capability by increasing the throughput and corresponding percentage of passengers screened by this technology while also further enhancing the privacy protections in place for AIT screening.

TSA has initiated the deployment of the Advanced Technology (AT)-2 units, which will be used to screen passengers' carry-on items. The AT-2 systems are equipped with algorithms that are intended to assist the operator with automatic detection of prohibited items and threats. This platform also provides TSA a baseline of performance, upon which future enhancements can be accomplished. Finally, TSA is procuring Credential Authentication Technology (CAT)/Boarding Pass Scanning Systems (BPSS), which Transportation Security Officers (TSOs) will use to validate and verify passengers' identification and boarding passes, increasing security at the checkpoints. CAT/BPSS will automatically verify both passenger identification documents and boarding passes, which will help facilitate identity-based screening while making the process more effective and efficient.

CAT/BPSS will eventually replace the current manual "lights and loupes" used by security officers to verify document authenticity. TSA anticipates the new technology will enhance security and increase efficiency by automatically verifying passenger identification and boarding passes. It will be incorporated into TSA's passenger prescreening pilot that is slated to begin at four airports this fall. This aligns with TSA's latest efforts to enhance the passenger screening experience by moving toward a more risk-based, intelligence-driven counter-terrorism agency.

TSA began testing travel document authentication technology at its Transportation Security Integration Facility in July 2011. Earlier versions of this technology were tested at Ronald Reagan Washington National (DCA) and Baltimore/Washington International Thurgood Marshall (BWI) airports in 2009.

As with all technologies, TSA will continue to push industry to higher performance requirements in an effort to increase detection and accuracy while also improving screening operations efficiency. TSA is already conducting work in a number of areas included in the OIG's recommendations. In addition, TSA is formulating plans to implement the other recommendations in the report.

### **Sub-Challenge: Airport Badging Oversight**

TSA is responsible for implementing a process to ensure employees working in secured airport areas are properly vetted and badged, and must oversee the designated airport-operator employees who perform the badging application process. TSA ensures that airport operators have quality assurance procedures for the badging application process by implementing the requirements in Sections III–V of Security Directive 1542-04-08G, *Security Threat Assessment and Reporting Requirements Related to Individuals with Airport-Issued Identification Media*, dated May 28, 2009. TSA also ensures that airport operators provide training and tools to designated badge office employees by implementing the requirements in Attachment B, Section II of Security Directive 1542-04-08G. Transportation Security Inspectors are required to verify the airport data





during their inspections as required in the Domestic Airport Inspection, Prompt Section 14: Security Directive 1542-04-08 Series. This is, at a minimum, a yearly inspection requirement.

### **Sub-Challenge: Passenger Air Cargo Security**

Prior to 9/11, no federal security requirements existed for cargo screening. Now, 100 percent of all cargo transported on passenger aircraft that depart U.S. airports is screened commensurate with screening of passenger checked baggage. This was accomplished largely through the Certified Cargo Screening Program, which permits entities that have undergone rigorous inspection and certification processes throughout the air cargo supply chain to screen cargo.

In December 2010, TSA implemented requirements for 100 percent screening of high-risk cargo on international flights bound for the United States. Following this, Secretary Napolitano and TSA Administrator Pistole solicited feedback from passenger carriers on their ability to screen 100 percent of all air cargo on international inbound passenger aircraft. The Department evaluated formal industry comment to this proposal and continues to finalize its strategy and timeline for implementing the 100 percent international inbound cargo screening requirement. As part of this effort, TSA will work with industry to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process, which certifies foreign aviation security programs that are commensurate with TSA standards.

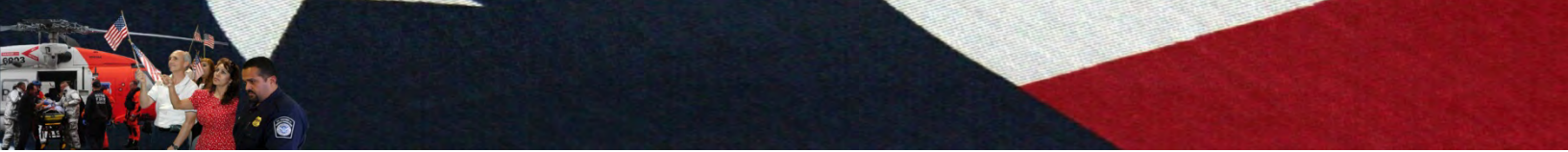
In addition, In January 2011, Secretary Napolitano announced a new partnership with the World Customs Organization (WCO) to enlist other nations, international bodies, and the private sector in increasing the security of the global supply chain—outlining a series of new initiatives to make the system stronger, smarter, and more resilient.

As part of the effort to strengthen the global supply chain, ICE, in coordination with the WCO, launched Operation Global Shield in 2010, a multilateral law enforcement effort aimed at combating the illicit cross-border diversion and trafficking of precursor chemicals for making improvised explosive devices (IED) by monitoring their cross-border movements. In March 2011, the WCO voted to make Project Global Shield a permanent program.

In addition, the Customs Trade Partnership Against Terrorism (C-TPAT), a voluntary public-private sector partnership program, strengthens cargo security throughout the international supply chain by working closely with importers, carriers, consolidators, licensed customs brokers, and manufacturers. The C-TPAT program—launched in November 2001 with seven participating companies—evaluates trusted shippers through security checks and on-site evaluations. As of October 2011, C-TPAT has 10,189 certified partners worldwide and has conducted 18,872 on-site validations of manufacturing and logistics facilities in 97 countries, representing some of the highest risk areas of the world.

### **Sub-Challenge: Training**

TSA's Operational and Technical (OTT) Training Division, within the Office of Security Operations, provided information on several activities already under way that address the challenge the OIG highlighted regarding training of TSA's screening workforce. OTT has established an integration process team (IPT) to review and analyze current documented and undocumented OTT business practices and processes. OTT currently uses events or inputs, such as Aviation Security



Assessment Program test results, internal [TSA] and external [OIG and GAO] covert test results, new threat and/or intelligence/threat information, and changes to procedures as catalysts to update existing or design new training materials. The deliverable from this IPT is a document that includes regulated and repeatable milestone-driven processes and procedures to ensure currency, effectiveness, and efficiency of training curriculum.

TSA's efforts to formalize the On-the-Job Training Instructor (OJTI) program are enhancing the level of training of the screening workforce. DHS OIG was provided an update stating that OTT conducted an OJTI Operational Tryout (OTO) at Seattle airport (SEA) to pilot a structured training curriculum for the TSOs who will serve as OJTIs. This included mandatory courses on mentoring and providing effective feedback. On the basis of initial feedback during the OTO in SEA, changes were made to the curriculum, a second OTO was conducted, and the new model was highly successful. Expansion of the program is beginning in the first quarter of FY 2012.

The DHS OIG also recommended that TSA determine if modifications to its allocation of training computers in the field are adequate. TSA completed an initial review of the current allocation of training computers and must continue that review because it is clear that simply establishing a TSO-to-training computer ratio for all airports would not be an appropriate solution. Office/training space, training room locations, and maximum number of officers that can be removed from the operations for training at any given time all must be factored in to ensure each airport has an appropriate training computer allocation.

OTT will continue its work to finalize the documentation that will capture OTT business practices and processes to ensure the currency, effectiveness, and efficiency of the training curriculum. National rollout of the formalized training program for OJT instructors will be conducted throughout FY 2012.

The review of training-computer allocations will continue throughout FY 2012, and adjustments may be made to individual airport inventories if they have a demonstrated need and can accommodate the additional equipment.

TSA believes that progress has been and continues to be made as TSA continues to build its training portfolio, with the desired outcome of improving performance and developing its workforce.

In FY 2012, OTT anticipates having documents that describe the processes used to identify needs for updating training materials and/or to develop new materials on the basis of information from various sources. TSA will continue to define changes needed to support a training program that is both comprehensive and adapts to address evolving threats.

### **Sub-Challenge: Rail and Mass Transit**

The final report for OIG-11-93, "DHS Grants Used for Mitigating Risks to Amtrak Rail Stations," was issued in June 2011. The 90-day response was submitted in September 2011. The language cited in the Management Challenges report does not reflect the recommendations from OIG-11-93. TSA is addressing the recommendations from the OIG-11-93 report, as follows and as previously submitted to the OIG.



*OIG-11-93 Recommendation 1—Require the Transportation Sector Network Management, Mass Transit and Passenger Rail Division, to work closely with Amtrak to establish a corrective action plan that ensures decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by previous risk assessments. The plan should include:*

- *Preliminary strategies and designs specifying the identification and commitment of all interested parties, to be presented during the grant application process to facilitate prompt mitigation efforts,*
- *Details on the amount of funding needed to address the most critical vulnerabilities, and*
- *Milestones for the timely approval of mitigation projects.*

TSA, in coordination with FEMA, is actively coordinating with Amtrak to address all items. TSA has completed a Baseline Assessment for Security Enhancement (BASE) review for the Northeast Corridor, and the preliminary results are being compiled and analyzed. Amtrak and DHS met on September 12, 2011, to discuss several items, including how the FY 2011 Amtrak grant funds can be used to address items from the BASE results and how corrective action plans will be developed for security projects that are currently either partially funded or not funded.

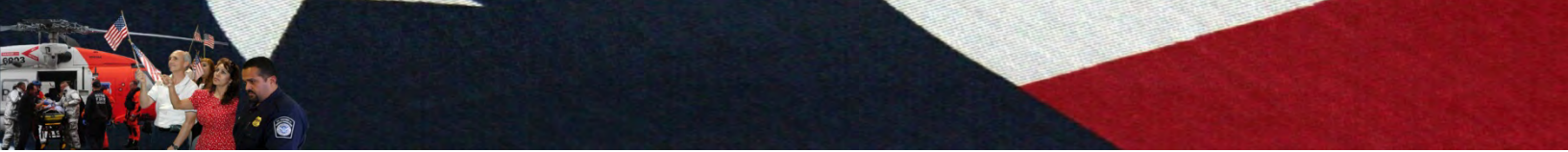
Actions planned to address Recommendation 1 within the next year:

- Members of the Mass Transit and Passenger Rail Security Division (MTPRS) will work with TSA/Office of Security Operations, Compliance, through the Northeast Regional Security Inspectors, to complete the second regional BASE assessment for Amtrak.
- Although a formal security plan cannot be finalized before the security plan regulation is issued, TSA will continue to work with Amtrak in the interim to develop action plans and security projects that address vulnerabilities identified through other completed assessments and plans.

Actions planned to address Recommendation 1 within the next 2–3 years:

- Members of MTPRS will work with TSA/Office of Security Operations, Compliance, through the Northeast Regional Security Inspectors, to complete the third and final regional BASE assessment per year, completing the 3-year system-wide assessment.
- The system-wide BASE assessment will be used with the foundation Amtrak already built through its prioritization “quilt.” The quilt summarizes in spreadsheet format the results of Amtrak’s system-wide risk assessments; provides a snapshot of critical assets identified in the risk assessments; and includes the status of on-going mitigation projects, including relevant funding sources. The quilt is a living document and is updated as necessary with current information. This quilt will set the baseline to inform a comprehensive security plan that will include strategies, designs, and cost-mitigation efforts.
- TSA will develop and include, as part of its internal procedures (per Recommendation 2), performance metrics to ensure the timely approval of Amtrak security projects.

*OIG-11-93 Recommendation 2—Ensure the Transportation Sector Network Management, Mass Transit and Passenger Rail Division, creates and reports internal procedures that describe how the agency will carry out its roles and responsibilities in the grant award process for ensuring that Amtrak and other grant recipients address the highest-priority security vulnerabilities.*



FEMA and TSA have set forth how each agency will carry out its roles and responsibilities in the grants award process in a memorandum of agreement that was signed by both agency Administrators in March 2011. An updated memorandum of understanding was also signed June 30, 2011, between TSA, FEMA, and the U.S. Department of Transportation/Federal Railroad Administration regarding how Amtrak funding would be administered and identifying, at a high level, each agency's role in the award process.

Actions planned to address Recommendation 2 within the next year:

- TSA will develop its own internal processes document, which it will share with FEMA, to document how TSA will internally carry out its roles and responsibilities.
- The internal processes will be validated during the FY 2012 grants cycle.

Actions planned to address Recommendation 2 within the next 2–3 years:

- TSA will review the documented processes as performed during the FY 2012 grants cycle and make updates and improvements based on lessons learned.
- Any updates to the internal processes will be shared with FEMA.

TSA is actively working on issuing a security plan regulation, which would cover Amtrak, as required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. 110-53). Once complete, this regulation will serve as the basis for DHS's coordination with Amtrak in developing DHS's system-wide security plan. A formal security plan cannot be finalized with Amtrak until such time. As stated in Recommendation 1, future-year appropriations to implement the "fund[ing of] Amtrak rail station remediation projects" is uncertain.

### ***Challenge #9: Trade Operations and Security***

CBP has made progress on the challenges identified by the OIG regarding completion of assessments of risk and the need for standard procedures and guidance for Importer Self Assessment (ISA) program participants.

#### **Sub-Challenge: CBP Revenue**

CBP provided a risk matrix and risk analysis for the ISA program. The risk matrix provided guidance for the assessment of risk based on the likelihood of occurrence and impact of the risk, if it occurred. The risk analysis identified 10 risk factors, the probability of occurrence and severity of the risk, and mitigating controls. This risk analysis demonstrates that CBP analyzed the individual risks to trade compliance associated with policies for accepting importers into the ISA program and identified appropriate mitigating activities for each risk. Further, CBP identified the source of the mitigating activities, such as the ISA Handbook, ISA SOP, etc. OIG has indicated that CBP's corrective action satisfied the intent of the recommendation, which was closed on July 18, 2011.

CBP provided support that it has removed ISA program oversight responsibilities from port account managers and assigned those importer accounts to national account managers. OIG has indicated that CBP's corrective action satisfied this recommendation, which was closed on November 18, 2010.



ISA SOP #2011-001 requires that national account managers review the information in the importer's annual notification letters including the findings from the periodic testing. In addition, ISA SOP #2011-001 requires the national account managers to complete an ISA account risk summary, which includes the evaluation of risk associated with importer self-testing results and actions taken. OIG has indicated that CBP's corrective action satisfied the intent of the recommendation, which was closed on July 18, 2011.

CBP decided that in lieu of updating the National Account Manager Guidebook, it will implement Account Management's SOP for ISA Accounts. The purpose of the SOP is to provide guidance and instruction to national account managers on assessing and reviewing ISA applicants and to promote uniform oversight of ISA program participants. The SOP addresses the challenges of the ISA program from an account management perspective and will be the authoritative document that national account managers follow for ISA account management purposes. The SOP has been reviewed by CBP stakeholders and is awaiting final approval. Once CBP obtains final approval, the SOP will be disseminated for implementation.

In addition to Account Management's SOP for ISA Accounts, additional formal procedural guidance is provided in ISA SOP #2011-001 issued by the Partnership Programs Branch to ensure consistent and effective implementation of the program.

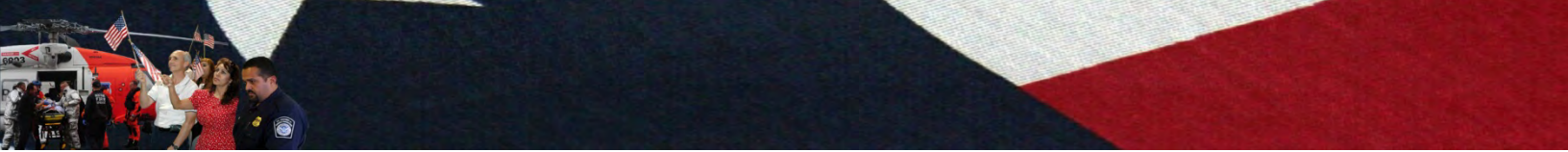
To address the OIG recommendation, CBP has incorporated the requirement for bond automation into the Automated Commercial Environment Cargo Release Concept of Operations (ConOps). The ConOps is currently under senior leadership review. CBP is confirming the high-level requirements. The deployment date of Single Transaction Bonds will not be available until CBP completes the acquisitions and procures a development contract. The acquisition date is estimated to occur in the second quarter of FY 2012. The estimated completion date is March 31, 2012.

### **Sub-Challenge: Cargo Security**

CBP updated the Anti-Terrorism Contraband Enforcement Team National Directive to address terrorism threats and outline minimum procedures for CBP officers to follow when performing anti-terrorism examinations, including specific procedures for inspecting for chemical, biological, nuclear, and radioactive threats. The directive is awaiting final approval.

As mentioned earlier, the C-TPAT, a voluntary public-private sector partnership program, strengthens cargo security throughout the international supply chain by working closely with importers, carriers, consolidators, licensed customs brokers, and manufacturers. The C-TPAT program—launched in November 2001 with seven participating companies—evaluates trusted shippers through security checks and on-site evaluations. As of October 2011, C-TPAT has 10,189 certified partners worldwide and has conducted 18,872 on-site validations of manufacturing and logistics facilities in 97 countries, representing some of the highest risk areas of the world.

To address an OIG recommendation, C-TPAT has updated the Web-based partner security profile to include additional security questions and has conducted refresher training for supply chain security specialists (SCSSs) regarding review of the security profile and vetting procedures; the latter was done in conjunction with the CBP Vetting Center. The program conducts quarterly random management reviews of newly certified security profiles for highway carriers to ensure the accuracy and consistency of the decisions made by the SCSS.



CBP is participating in DHS initiatives focused on biological and chemical threats to the United States and is working to update and develop new rule indicators in the inbound cargo CBP Automated Targeting System (ATS-N) to target high-risk shipments. To supplement its expertise and experience in these areas, CBP will draw on the knowledge of DHS bio-terror subject-matter experts as well as the knowledge of members of the intelligence community. Through participation in these initiatives and through the use of their recommendations, CBP will be well-positioned to identify pathways that pose the highest risk of biological and chemical weapons entering the country. This will support the acquisition and deployment of biological and chemical detection equipment and will ensure that the appropriate guidance and training is provided to CBP personnel. This thoroughly coordinated initiative and its accomplishments are described below.

In 2010, CBP personnel from the Office of Field Operations (OFO), Agriculture Programs and Trade Liaison (APTL) and the Office of Intelligence and Investigative Liaison (OIIL) held a series of meetings with subject-matter experts from the Biodefense Knowledge Center (BKC), Lawrence Livermore National Laboratory (LLNL), to discuss the determination of risk, conduct studies, and create intelligence requirements for the identification and interdiction of possible biological and chemical terrorist material by the biodefense community.

OFO and OIIL briefed BKC personnel on the Automated Targeting System in relation to targeting high-risk cargo shipments, including the use of rules and weight sets for identifying high-risk cargo. OIIL also provided a review of current ATS rules used to identify cargo with the highest risk for possible biological or chemical terrorist material.

After receiving analysis from subject-matter experts, BKC reviewed current ATS rules for the cargo shipment threat area and provided OIIL with recommendations for the enhancement of the lists utilized for targeting. BKC also developed lists pertaining to known scientists and facilities for possible application in ATS targeting rules.

Three rules summits were held throughout 2010. These summits led to the creation of preliminary rule concepts for targeting high-risk biological and chemical threats in the inbound cargo stream and the development of a number of rule modifications, including the creation of several new rules bundles, blocking of common pathogen description acronyms to eliminate false matches of manifest descriptions, marks and numbers, and updating of facility lists.

APTL is currently in a testing period for the ABTC2 Weight Set to target inbound cargo. After testing is completed, OIIL and TASPO will complete an analysis of rule firings during the test period for APTL review and approval. OIIL will support APTL development of an SOP and field training plan for national deployment of the ABTC2 Weight Set.

Additional planned efforts include OFO designing a pilot rollout of the Weight Set and creating the policy for targeting shipments for biological and chemical threats and evaluate the Weight Set prior to national deployment. OIIL will continue to support OFO via ATS rules and Weight Set work for the nationwide implementation of the Ag/Bio Weight Set. The estimated completion date is December 31, 2011.



## Concluding Comment

The Department concurs with the OIG's assessment that

...the Department has made progress in coalescing into an effective organization, as well as addressing its key mission areas to secure our nation's borders, increase our readiness and resiliency in the face of a terrorist threat or a natural disaster, and implement increased levels of security in our transportation systems and trade operations.

We appreciate the perspectives offered by the OIG in its management challenges report and will use them to assist the Department in developing our future plans for addressing these important areas.



## Acronym List





## Acronyms

ADA – Anti-Deficiency Act	CRCL – Civil Rights and Civil Liberties
ADMP – Active Duty Military Payroll	CSRS – Civil Service Retirement System
AFG – Assistance to Firefighters Grants	C-TPAT - Customs Trade Partnership Against Terrorism
AFR – Annual Financial Report	CWG – Commodity Working Group
AIT – Advanced Imaging Technology	CY – Current Year
APMD – Acquisition Program Management Division	DADLP – Disaster Assistance Direct Loan Program
APTL – Agriculture Programs and Trade Liaison	DC – District of Columbia
ARRA – American Recovery and Reinvestment Act	DHS – U.S. Department of Homeland Security
AT – Advanced Technology	DHS FAA – Department of Homeland Security Financial Accountability Act
ATA – American Trucking Association	DIEMS – Date of Initial Entry into Military Service
BKC – Biodefense Knowledge Center	DNDO – Domestic Nuclear Detection Office
BP – British Petroleum	DOC – Department of Commerce
BPD – Bureau of Public Debt	DOD – Department of Defense
BPSS – Boarding Pass Scanning Systems	DOL – Department of Labor
BUR – Bottom-Up Review	DRO – Detention and Removal Operations
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance	EDL – Enhanced Driver’s License
CAT – Credential Authentication Technology	EDS – Explosive Detection System
CBP – U.S. Customs and Border Protection	EFSP – Emergency Food and Shelter Program
CBRN – Chemical, Biological, Radiological, and Nuclear	ELIS – Electronic Immigration System
CDL – Community Disaster Loan	EMI – Emergency Management Institute
CDP – Center for Domestic Preparedness	ER – Efficiency Review
CFO – Chief Financial Officer	ESC – Executive Steering Committee
CFR – Code of Federal Regulations	ESF – Emergency Support Functions
CIKR – Critical Infrastructure and Key Resources	ESFLG – Emergency Support Function Leadership Group
CIO – Chief Information Officer	ETC – Enhanced Tribal Card
CIRT – Controlled Impact Rescue Tool	ETD – Explosive Trace Detection
CISO – Chief Information Security Officer	EWI – Enterprise Wireless Infrastructure
COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985	FAR – Federal Acquisition Regulation
COTR – Contract Officer’s Technical Representative	FBI – Federal Bureau of Investigation
COTS – Commercial Off-the-Shelf	FBwT – Fund Balance with Treasury
	FCRA – Federal Credit Reform Act of 1990
	FECA – Federal Employees Compensation Act



- FEMA – Federal Emergency Management Agency
- FERS – Federal Employees Retirement System
- FFMIA – Federal Financial Management Improvement Act of 1996
- FISMA – Federal Information Security Management Act
- FLETC – Federal Law Enforcement Training Center
- FMFIA – Federal Managers’ Financial Integrity Act
- FOSC – Federal On-scene Coordinators
- FPS – Federal Protective Service
- FTP – Full-time Position
- FY – Fiscal Year
- GAAP – Generally Accepted Accounting Principles
- GAO – Government Accountability Office
- GCCF – Gulf Coast Claims Facility
- GETS – Government Emergency Telecommunications Service
- GSA – General Services Administration
- GSP – Generalized System of Preferences
- HSA – Homeland Security Act of 2002
- HSGP – Homeland Security Grant Program
- HSIN – Homeland Security Information Network
- HSPD – Homeland Security Presidential Directive
- HS-STEM – Homeland Security Science, Technology, Engineering, and Mathematics
- ICCB – Internal Control Coordination Board
- ICE – U.S. Immigration and Customs Enforcement
- IDI – Injured Domestic Industries
- IED – Improvised Explosive Device
- IEFA – Immigration Examination Fee Account
- IHP – Individuals and Household Programs
- IILCM – Integrated Investment Life Cycle Model
- INA – Immigration Nationality Act
- IP – Improper Payment
- IPERA – Improper Payments Elimination and Recovery Act
- IPIA – Improper Payments Information Act of 2002
- ISA – Importer Self Assessment
- ISO – Immigration Services Officer
- IT – Information Technology
- LLNL – Lawrence Livermore National Laboratory
- LOI – Letters of Intent
- MCA – Managerial Cost Accounting
- MCO – Mission Critical Occupation
- MD&A – Management’s Discussion and Analysis
- MERHCF – Medicare-Eligible Retiree Health Care Fund
- MGMT – Management Directorate
- MHS – Military Health System
- MOA – Memorandum of Agreement
- MRS – Military Retirement System
- MTS – Metric Tracking System
- ND – Non-Disaster
- NFIP – National Flood Insurance Program
- NIST – National Institute of Standards and Technology
- NPFC – National Pollution Funds Center
- NPPD – National Protection and Programs Directorate
- nPRS – Next-Generation Period Reporting System
- NSA – National Security Agency
- NTAS – National Terrorism Advisory System
- NTC-P – National Targeting Center-Passenger
- OCAO – Office of the Chief Administrative Officer
- OCFO – Office of the Chief Financial Officer
- OCIO – Office of the Chief Information Officer
- OCPO – Office of the Chief Procurement Officer



- OFO – Office of Field Operations
- OHA – Office of Health Affairs
- OIG – Office of Inspector General
- OIIL – Office of Intelligence and Investigative Liaison
- OJT – On-the-Job Training
- OJTI – On-the-Job Training Instructor
- OMB – Office of Management and Budget
- OM&S – Operating Materials and Supplies
- OPA – Oil Pollution Act of 1990
- OPEB – Other Post Retirement Benefits
- OPM – Office of Personnel Management
- OPS – Office of Operations
- ORB – Other Retirement Benefits
- OSI – Office of Security and Integrity
- OSLTF – Oil Spill Liability Trust Fund
- OTO – Operational Tryout
- OTT – Operational and Technical Training Division
- PA – Public Assistance
- PA&E – Program Analysis and Evaluation
- PCS – Permanent-Change-of-Station
- PII – Personally Identifiable Information
- PM – Program Manager
- POA&M – Plan of Action and Milestones
- PPD – Presidential Policy Directive
- PP&E – Property, Plant, and Equipment
- Pub. L. – Public Law
- PY – Prior Year
- QHSR – Quadrennial Homeland Security Review
- Recovery Act – The American Recovery and Reinvestment Act of 2009
- RSSI – Required Supplementary Stewardship Information
- S/ACOM – Sustainment Acquisition Composite Model
- SAT – Senior Assessment Team
- SBI<sup>net</sup> – Secure Border Initiative Network
- SBR – Statement of Budgetary Resources
- SCDL – Special Community Disaster Loan
- SCSS – Supply Chain Security Specialists
- SFFAS – Statement of Federal Financial Accounting Standards
- SFRBTF – Sport Fish Restoration Boating Trust Fund
- SMC – Senior Management Council
- S&T – Science and Technology Directorate
- TAFS – Treasury Account Fund Symbol
- TASC – Transformation and Systems Consolidation
- TCM – Trade Compliance Measurement
- TSA – Transportation Security Administration
- TSGP – Transit Security Grants Program
- TSO – Transportation Security Officers
- U.S. – United States
- U.S.C. – United States Code
- US-CERT - United States Computer Emergency Readiness Team
- USCG – U.S. Coast Guard
- USCIS – U. S. Citizenship and Immigration Services
- USM – Under Secretary for Management
- USSS – U.S. Secret Service
- VA – Veterans Affairs
- IBE – Validation Instrument for Business Enterprises
- WAN – Wide Area Network
- WHTI – Western Hemisphere Travel Initiative
- WYO – Write Your Own





Homeland  
Security



Homeland  
Security