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.

Entry Summary of Trade Compliance Measurement
($ in millions)

	FY 2012	FY 2011
Estimated Revenue Gap	$484.0	$342.0
Preliminary Revenue Gap of all collectable revenue for year (%)	1.21%	.91%
Estimated Over-Collection	$65	$64
Estimated Under-Collection	$549	$406
Overall Trade Compliance Rate (%)	96.47%	96.71%

The preliminary overall compliance rate for FY 2012 is 96.47 percent. The final overall trade compliance rate and estimated revenue gap for FY 2012 will be issued in February 2013.

Schedule of Spending

The Schedule of Spending (SOS) presents an overview of how departments or agencies are spending money. The SOS presents total budgetary resources, gross outlays, and fiscal year-to-date total obligations for the reporting entity on a combined basis. The data used to populate this schedule is the same underlying data used to populate the Statement of Budgetary Resources (SBR). This is the first fiscal year the Department is presenting the SOS, thus the presentation does not include prior year information.

What Money is Available to Spend. This section presents resources that were available to spend as reported in the SBR. "Total Resources" refers to "Total Budgetary Resources" as described in the SBR. "Amounts not Agreed to be Spent" represent apportioned resources and resources exempt from apportionment not obligated at year end. "Amounts not Available to Spend" are not apportioned by Congress; therefore, are unavailable for obligation. Total "Amounts Agreed to be Spent" refers to obligations incurred in all sections.

How was the Money Spent. This section presents services or items that were purchased. The major categories presented represent the Department's Components or sub-agencies. Those Components that have a material impact on the SBR are presented separately. Other Components are summarized into Directorates and Other Components, which includes DNDO, FLETC, I&A and OPS, MGMT, OHA, OIG, NPPD, S&T, USCIS, and USSS. The items in this section align to OMB Budget Object Class definitions found in OMB Circular No. A-11; however, the amounts reported here reflect outlays (not obligations) by budget object class reconciled to total obligations incurred. "Amounts Remaining to be Spent" represent the fiscal year change in the obligated balances plus any recoveries of prior year obligations, adjusted for transfers of unpaid obligations. A negative balance on this line can occur when payments against both current and prior years' obligations exceed current year obligations. This is expected in years of declining budgetary resources.

The Department encourages public feedback on the presentation of this schedule.

Department of Homeland Security
Schedule of Spending
For the Year Ended September 30, 2012
(In Millions)

	2012
What Money is Available to Spend?	
Total Resources	**$ 79,503**
Less Amount Available but Not Agreed to be Spent	8,552
Less Amount Not Available to be Spent	3,778
TOTAL AMOUNT AGREED TO BE SPENT	**67,173**
How was the Money Spent?	
U.S. Customs and Border Protection	
Personnel Compensation and Benefits	9,428
Contractual Services and Supplies	3,140
Acquisition of Assets	1,325
Grants, Fixed Charges, and Other Spending	2,224
Total Spending	**16,117**

U.S. Coast Guard	
Personnel Compensation and Benefits	5,213
Contractual Services and Supplies	4,767
Acquisition of Assets	878
Grants, Fixed Charges, and Other Spending	188
Total Spending	**11,046**
Federal Emergency Management Agency	
Personnel Compensation and Benefits	1,083
Contractual Services and Supplies	2,904
Acquisition of Assets	587
Grants, Fixed Charges, and Other Spending	11,394
Total Spending	**15,968**
U.S. Immigration and Customs Enforcement	
Personnel Compensation and Benefits	2,868
Contractual Services and Supplies	3,235
Acquisition of Assets	129
Grants, Fixed Charges, and Other Spending	17
Total Spending	**6,249**
Transportation Security Administration	
Personnel Compensation and Benefits	4,661
Contractual Services and Supplies	2,394
Acquisition of Assets	369
Grants, Fixed Charges, and Other Spending	111
Total Spending	**7,535**
Directorates and Other Components	
Personnel Compensation and Benefits	3,760
Contractual Services and Supplies	6,675
Acquisition of Assets	567
Grants, Fixed Charges, and Other Spending	167
Total Spending	**11,169**
Department Totals	
Personnel Compensation and Benefits	27,013
Contractual Services and Supplies	23,115
Acquisition of Assets	3,855
Grants, Fixed Charges, and Other Spending	14,101
Total Spending	**68,084**
Total Spending for the Department	**68,084**
Amounts Remaining to be Spent	**(911)**
TOTAL AMOUNT AGREED TO BE SPENT	**$ 67,173**

Summary of Financial Statement Audit and Management Assurances

Table 1 and Table 2 below provide a summary of the financial statement audit results and management assurances for FY 2012.

Table 1. FY 2012 Summary of the Financial Statement Integrated Audit Results

Audit Opinion	**QUALIFIED**				
Restatement	**YES**				
Material Weakness	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
Financial Reporting	1				1
IT Controls & System Functionality	1				1
Property, Plant & Equipment	1				1
Environmental & Other Liabilities	1				1
Budgetary Accounting	1				1
Total Material Weaknesses	**5**	**0**	**0**	**0**	**5**

In FY 2012, 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 prior year. For example, Fund Balance with Treasury at U.S. Coast Guard was resolved; Financial Reporting at USCIS was resolved; Property Plant and Equipment at TSA and MGMT was resolved; and IT Controls and System Functionality and Budgetary Accounting was reduced in severity at U.S. Coast Guard.

In FY 2012, the Department is providing reasonable assurance on internal controls over financial reporting, with the exception of four material weaknesses identified in Table 2. Management has performed its evaluation, and the assurance is provided based upon the cumulative assessment work performed on Entity Level Controls, Environmental Liabilities, Fund Balance with Treasury, Human Resources and Payroll Management, Payment Management, Insurance Management, and Revenue and Receivables. DHS management has remediation work to continue in FY 2013; however, no additional material weaknesses were identified as a result of the work performed in these business process areas. The following Table provides those areas where material weaknesses were identified and remediation work continues.

DHS reported one less material weakness at the Department level than reported by the independent auditor. The difference between the audit results and management's conclusion is due to reporting requirement timing differences. The differing conclusion is the independent audit reports on a U.S. Coast Guard Environmental Liability material weakness that existed during FY 2012. Management's conclusion considers the effectiveness of controls as of September 30, 2012. The U.S. Coast Guard implemented procedures during FY 2012, which reduced the severity of the material weakness as of September 30, 2012 for management's assurance.

Table 2. FY 2012 Effectiveness of Internal Control Over Financial Reporting

EFFECTIVENESS OF INTERNAL CONTROL OVER FINANCIAL REPORTING (FMFIA SECTION 2)					
Statement of Assurance	QUALIFIED				
Material Weakness	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
Financial Reporting	1				1
IT Controls & System Functionality	1				1
Property, Plant & Equipment	1				1
Environmental & Other Liabilities	1		ü		0
Budgetary Accounting	1				1
Total Material Weaknesses	**5**	**0**	**(1)**	**0**	**4**
EFFECTIVENESS OF INTERNAL CONTROL OVER OPERATIONS (FMFIA SECTION 2)					
Statement of Assurance	QUALIFIED				
Material Weakness	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
Financial Assistance Awards Policy & Oversight	1				1
Acquisition Management	1				1
Funds Control	1				1
Entity Level Controls	1		ü		0
Total Material Weaknesses	**4**	**0**	**(1)**	**0**	**3**
CONFORMANCE WITH FINANCIAL MANAGEMENT SYSTEMS REQUIREMENTS (FMFIA SECTION 4)					
Statement of Assurance	SYSTEMS DO NOT CONFORM WITH FINANCIAL SYSTEM REQUIREMENTS				
Non-Conformances	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
Federal Financial Management Systems Requirements, including Financial Systems Security & Integrate Financial Management Systems	1				1
Noncompliance with the U.S. Standard General Ledger	1				1
Federal Accounting Standards	1				1
Total Non-Conformances	**3**	**0**	**0**	**0**	**3**
Compliance with Federal Financial Management Improvement Act (FFMIA)		**DHS**		**Auditor**	
Overall System Compliance		**No**		**No**	
1. System Requirements		**No**			
2. Accounting Standards		**No**			
3. USSGL at Transaction Level		**No**			

Effectiveness of Internal Control Over Financial Reporting

Pursuant to the *Department of Homeland Security Financial Accountability Act* (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 an opinion on all financial statements. Since FY 2005 DHS reduced audit qualifications from 10 to 1, and material weaknesses by half. For the seventh consecutive year, we

have made tremendous progress strengthening Department-wide internal controls over financial reporting, as evidenced by the following FY 2012 achievements:

- The U.S. Coast Guard corrective actions significantly reduced risk related to financial scripts and Fund Balance with Treasury reconciliations resulting in reducing the severity of IT Controls and System Functionality and fully remediating weaknesses related to Fund Balance with Treasury. In addition, U.S. Coast Guard implemented the Audit Command Language as a mitigating control and reduced the severity of weaknesses related to Budgetary Accounting. Most significantly, the U.S. Coast Guard corrected the audit qualification related to Environmental Liabilities by developing a new methodology.
- 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 material weakness correction at the U.S. Coast Guard and continued risk reductions of system security vulnerabilities at FEMA, ICE, and USCIS.
- TSA's corrective actions fully remediated a longstanding material weakness in Property, Plant, and Equipment by developing sustainable processes, policies, and procedures for effective internal controls related to Internal Use Software and reconciliation of property balances.
- USCIS executed corrective actions and fully remediated weaknesses related to Financial Reporting by updating processes and related procedures over the recording of deferred revenue.

Significant internal control challenges remain in the areas of Financial Reporting; IT Controls and System Functionality; Property, Plant, and Equipment; and Budgetary Accounting. To support the remediation effort, the Department's Chief Financial Officer conducts weekly risk management meetings with applicable Components, 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 2012 Internal Control Over Financial Reporting Corrective Actions

Material Weakness	Component	Year Identified	Target Correction Date
	USCG, ICE, and TSA	FY 2003	FY 2013
Financial Reporting	DHS has not established an effective financial reporting process due to the lack of integrated financial processes and systems. U.S. Coast Guard materially contributes, while ICE and TSA significantly contribute to the Department's overall material weakness.		
Corrective Actions	The DHS OCFO will continue to support U.S. Coast Guard, ICE, and TSA in implementing corrective actions to establish effective financial reporting control activities.		

Material Weakness	Component	Year Identified	Target Correction Date
	USCG, FEMA, CBP, ICE, and USCIS	FY 2003	FY 2013
IT Controls and System Functionality	The Department's Independent Public Auditor has identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to inherited control deficiencies surrounding general computer and application controls. FEMA materially contributes, while U.S. Coast Guard, CBP, ICE, and USCIS significantly contribute to the Department's overall material weakness. The *Federal Information Security Management Act* mandates that federal agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance. In addition, the Department's financial systems do not conform to the *Federal Financial Management Improvement Act*.		
Corrective Actions	The DHS OCFO and OCIO will support the U.S. Coast Guard, FEMA, CBP, ICE, and USCIS design and implementation of 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, CBP, and ICE	FY 2003	FY 2013
Property, Plant, and Equipment	The controls and related processes surrounding U.S. Coast Guard 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 ICE which contribute to the overall material weakness.		
Corrective Actions	U.S. Coast Guard will implement policies and procedures to support completeness, existence, and valuation assertions for PP&E. The DHS OCFO will continue efforts to support U.S. Coast Guard and other Components in 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, FEMA, ICE, MGMT, and FLETC	FY 2004	FY 2012
Budgetary Accounting	The Department identified weaknesses in the Budgetary Resource Management process such as the lack of fully implemented policies and procedures, ineffective monitoring controls, and lack of effective verification and validation of obligations. The U.S. Coast Guard, FEMA, ICE, MGMT, and FLETC contribute to the overall Department level material weakness.		
Corrective Actions	The DHS OCFO will continue to support U.S. Coast Guard, FEMA, ICE, MGMT, I&A/Ops, and FLETC in implementing corrective actions to establish effective financial reporting control activities.		

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 seventh consecutive year, we have made tremendous progress in strengthening Department-wide internal controls over operations, as evidenced by the following FY 2012 achievements:

- The Office of the Chief Financial Officer (OCFO) improved stewardship of Federal assistance funding across DHS. The OCFO published eleven policies in FY 2012 to guide Components' and Awardees' actions; began work on a Financial Assistance Oversight Review Guide which will support adherence to DHS policy and government-wide standards; improved identification and tracking of Office of the Inspector General and DHS Management actions taken to resolve and close annual Awardee audit findings; and submitted to the Under Secretary for Management a Directive and Instructions to define the financial assistance line of business.
- The OCFO implemented corrective action plans for all programs with estimated improper error amounts above $10 million. This work led to a reduction in estimated improper payments for DHS high-risk programs. In addition, the OCFO completed independent reviews for all high-risk IPERA programs and ARRA spending; attained a 94 percent cumulative recoupment/resolution rate for high-dollar overpayments identified in the Secretary's quarterly reports to the DHS OIG, OMB, and the public; and developed and began implementation of a DHS *Do Not Pay* Implementation Plan.
- The DHS OCFO conducted a risk-based compliance assessment over Component Fleet and Travel cards and the use of travel vouchers, in relation to Federal and Departmental guidance. The Department established a baseline measure of controls currently in place and developed a corrective action plan for deficiencies identified during this process. Internal progress review briefings were held for each card program which allowed Senior Component Accountable Officials to brief the Department's Chief Financial Officer, Chief Procurement Officer, and Chief Readiness Support Officer on best practices, performance metrics, and common challenges.
- The Under Secretary for Management established the Program Accountability and Risk Management Office (PARM) in FY 2011 to govern program investment oversight. PARM's mission is to reduce the risk that programs will exceed their budget and schedule or fail to meet mission requirements. For example, by obtaining life cycle cost estimates in FY 2012 for developing programs, PARM reduced the DHS risk of program cost overruns. Estimates are targeted at programs outside of the operations and maintenance phase where life cycle cost estimates are the most valuable.
- DHS made significant improvements to the acquisition workforce by improving the balance of program management staff to the rest of the acquisition workforce and by balancing the number and expertise of DHS employees with appropriate use of contractors. DHS was lauded in FY 2012 by the GAO for its documented improvements in this area.

- The Chief Readiness Support Officer created and actively promoted a new Internal Control Program Webpage which was actively updated throughout the Fiscal Year.
- The Office of the Chief Readiness Support Officer achieved substantial remediation of OIG findings relating to Control Over Firearms. The underlying work included development of a Component monthly sensitive assets loss, damage, destruction report and quarterly scorecard; review of all Component policies and procedures; implementation of an Equipment Control Class sensitive assets methodology; publication of a revised DHS Firearm Asset Policy; and conducting an analysis of firearms losses from FY 2006 to FY 2008 versus FY 2009 to FY 2011.
- The Office of the Chief Information Officer implemented the usage of HSPD-12 Smartcards for logical access to the DHS Headquarters Network for all DHS Headquarters Federal and contract staff users in the National Capitol Region; increased the level of Information Technology program and portfolio governance across the Department by establishing 3 Portfolio Governance Boards and 17 Executive Steering Committees; implemented a process to continuously review and evaluate the health of all IT programs on the Major Acquisition Oversight List; completed the implementation of TechStat at the Component level; and chartered six Primary Function Executive Steering Committees to oversee investments delivering similar capabilities.
- The Office of the Chief Human Capital Officer (OCHCO) conducted an in-depth assessment of operational service delivery effectiveness, and implemented corrective actions, including functional and geographic realignments of staff, to improve service delivery. The OCHCO ensured alignment of DHS workforce planning processes to new government-wide practices; updated the DHS Workforce Planning Guide; and established a skills gap assessment strategy to pilot with selected DHS mission critical occupations.
- The Chief Security Officer (CSO) reinvigorated the influence and scope of the CSO Council; addressed internal control challenges by re-directing security support resources across Components as needed; worked with the CSO Council to introduce the Security Professional Education Development (Sped) Program; and leveraged a Congressional inquiry concerning the security clearance suspension process and EEO complaints into a Department-wide review.

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

Table 4. FY 2011 Internal Control Over Operations Corrective Actions

Material Weakness	Component	Year Identified	Target Correction Date
	DHS and FEMA	FY 2008	FY 2014
Financial Assistance Awards Policy and Oversight	Significant progress has been made on conditions affecting stewardship of Federal assistance funding across DHS listed in last year's report. Eleven policies were published in FY 2012, and twenty-seven policies will be published in FY 2013 to guide Components' and Awardees' actions. Standard templates were developed through DHS-wide working groups, and a Financial Assistance Oversight Review Guide is in development to ensure adherence to DHS policy and government-wide standards. Progress has been made in identifying and tracking Office of the Inspector General and DHS Management actions taken to resolve and close annual Awardee audit findings. Headquarters offices are working with Components to assist in timely notification and closeout of OMB Circular A-133 audit requirements. Through the Deputy Secretary's initiative to *Improve the Health of DHS Financial Assistance* a Directive and Instruction have been submitted for USM approval to define the financial assistance line of business, including the business models, areas of high risk, gaps in key controls, and clear lines of responsibility.		
Corrective Actions	Publish the twenty-seven policies described above, support all policies through training, and continue efforts to further establish and improve the Line of Business.		

Material Weakness	Component	Year Identified	Target Correction Date
	DHS	FY 2008	FY 2013
Acquisition Management	During FY 2012 significant progress was made to reduce the severity of this challenge, but work remains, and sustainment needs to be achieved. DHS financial and procurement systems are not integrated which leaves our processes vulnerable. However, progress has been made to mitigate these vulnerabilities. DHS established the Program Accountability and Risk Management Office (PARM) to govern oversight while the Chief Procurement Officer is responsible for procurement oversight. This restructuring ensures proper oversight for the function as well as program accountability.		
Corrective Actions	Continue oversight policy development and remediation efforts. Improve training for cost estimation, understanding regulation and acquisition documentation. Improve Acquisition workforce through training and targeted recruiting. Improve communications with the government vendor community.		

Material Weakness	Component	Year Identified	Target Correction Date
	USCG, ICE, and USSS	FY 2006	FY 2013
Funds Control	U.S. Coast Guard repeated the prior year Anti-Deficiency Act (ADA) controls material weakness. ICE made progress against prior-year conditions by developing an Administrative Control of Funds Directive; however, additional work is needed to implement the Directive across ICE program offices. Finally, USSS has not completely implemented funds control policies and procedures to address prior-year ADA violations reported by GAO.		
Corrective Actions	U.S. Coast Guard is developing enterprise-wide policies and procedures for assessing ADA risks, testing effectiveness of controls, and monitoring to fully implement DHS policy. ICE plans to conduct verification and validation procedures to ensure their Administrative Control of Funds Directive is effectively implemented. USSS will update their policies and procedures for the Monthly Execution Report to fully reflect implemented process improvements. The DHS OCFO will validate and verify this work.		

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 2012 include: the reduction in estimated improper payments for high risk programs, the completion of full independent reviews of the components, the creation of the Do Not Pay Implementation Plan; 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 2012, DHS conducted risk assessments on 55 DHS programs, totaling nearly $18 billion in FY 2011 disbursements. We completed risk assessments for all programs unless total disbursements were less than $10 million or testing was required based on prior year results. We assessed all payment types except for federal Intra-governmental 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.

Improper payment estimates in this section are based on statistical estimates for FY 2011 payments. These estimates are then projected for FY 2012 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.
- Contract Payment Management – Identification of contract management weaknesses identified in previous payment testing. Discrepancies between Contracting Officer Representatives (COR) reviewing and approving invoices with CORs listed in contract. Contractors reviewing and approving invoices on behalf of the COR. Lack of familiarity with goods and services listed on invoices. Time available to review invoices prior to payment. Sufficiency of supporting documentation to support invoice amount prior to payment. Completeness of contract file in order to verify agreed upon amounts for goods and/or services.

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 2012 Risk Assessments and Prior Year Payment Sample Testing

Component	Program Name	FY 2012 Disbursements (Based on FY 2011 Actual Data) ($ Millions)
CBP	Border Security Fencing	$197
	Custodial – Refund & Drawback	$1,343
FEMA[1]	Disaster Relief Program – Individuals and Households Program (IHP)	$880
	Disaster Relief Program – Vendor Payments	$494
	Insurance – National Flood Insurance Program (NFIP)	$794
	Grants – Public Assistance Programs (PA)	$2,990
	Grants – Homeland Security Grant Program (HSGP)	$1,472
	Grants – Assistance to Firefighters Grants (AFG)	$471
	Grants – Emergency Food and Shelter Program (EFSP)	$45
	Grants – Transit Security Grants Program (TSGP)	$196
ICE	Enforcement and Removal Operations (ERO)	$1,570
NPPD	Federal Protective Service (FPS)	$733
Total Disbursements		**$11,185**

Note 1: All FEMA disbursement totals are national figures. Selected States and Territories were tested for the State-Administered programs HSGP, PA, TSGP. See Table 2 for a listing of states and territories tested for these programs in FY 2012.

II. Statistical Sampling

For FY 2012 reporting, a stratified sampling design was used to test payments based on FY 2011 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 2012 Payment Population (Based on FY 2011 Actual Data) ($ millions)	FY 2012 Sample Size (Based on FY 2011 Actual Data) ($ millions)	FY 2012 Est. Error Amount (Based on FY 2011 Actual Data) ($ millions)	FY 2012 Est. Error Percentage (Based on FY 2011 Actual Data) (%)
CBP	Border Security Fencing	$197	$146	$0	0.03%
	Refund & Drawback	$1,343	$141	$0	0.01%
FEMA	Disaster Relief Program – Individuals and Households Program (IHP)	$880	$3	$3	0.29%
	Disaster Relief Program – Vendor Payments	$494	$155	$15	3.09%
	Insurance – National Flood Insurance Program (NFIP)	$794	$34	$6	0.75%
	Grants – Public Assistance Programs (PA)[1]	$701	$328	$0	0.06%
	Grants – Homeland Security Grant Program (HSGP)[2]	$555	$128	$1	1.05%
	Grants – Assistance to Firefighters Grants (AFG)	$471	$78	$8	1.60%
	Grants – Transit Security Grants Program (TSGP)[3]	$44	$25	$1	4.63%
	Grants – Emergency Food and Shelter Program (EFSP)	$45	$14	$1	2.51%
ICE	Enforcement and Removal Operations (ERO)	$1,570	$389	$133	8.47%
NPPD	Federal Protective Service	$733	$172	$10	1.37%
DHS	**All Programs[4]**	**$7,827**	**$1,613**	**$178**	**2.27%[5]**
DHS	**High Risk Programs[6]**	**$2,797**	**$716**	**$158**	**5.65%**

Note 1. Note 1: Sample testing of the Public Assistance Program was done in two stages covering eight States (CA, FL, HI, MS, MT, ND, SD, and TN) and American Samoa. These States and Territory paid out $701 million out of a national total of $2,990 million. The totals in the table are the stage two payment populations for the States and Territory tested in FY 2012. See Table 18 Improper Payment Reduction Outlook for the national estimated error rate and amount.

Note 2. Sample testing of the Homeland Security Grant Program was done in two stages covering 15 States (AK, AR, CA, CT, DE, GA, MA, MD, ME, MS, NH, OR, SD, TX, and UT), America Samoa, Guam, Puerto Rico, and U.S. Virgin Islands. These States and Territories paid out $555 million out of a national total of $1,472 million. The totals in the table are the stage two payment populations for the States and Territories tested. See Table 18 Improper Payment Reduction Outlook for the national estimated error rate and amount.

Note 3. Sample testing of the Transit Security Grant Program was done in two stages covering eleven States (FL, HI, KS, MA, MN, MO, OR, PA, VA, TX, and WA). These States paid out $44 million out of a national total of $196 million. The totals in the table are the stage two payment populations for the nine States. See Table 18 Improper Payment Reduction Outlook for the national estimated error rate and amount.

Note 4. Program total of $7,827 in this table differs from $11,185 total in Table 18 Improper Payment Reduction Outlook. For State-Administered grant programs, the table above lists the population totals for the States tested, while Table 18 Improper Payment Reduction Outlook lists the national payment populations.
Note 5. Percentage figures based on cumulative totals.
Note 6. Totals for programs with estimated error amounts of $10 million or greater as listed in this table.

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 six programs due to national estimated error amounts above $10 million:

1. FEMA's Assistance to Firefighters Grants;
2. FEMA's Disaster Relief Program - Vendor Payments;
3. FEMA's Emergency Food and Shelter Program;
4. FEMA's National Flood Insurance Program;
5. ICE's Enforcement and Removal Operations Program; and,
6. NPPD's Federal Protective Service Program.

Also provided is an update to corrective actions listed in the FY 2011 Annual Financial Report for FEMA's Public Assistance 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.

Status of Prior Year Corrective Action Plans for FEMA High-Risk Programs

Table 7. Assistance to Firefighters Grant Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect Information on Application		
1. Failure to Provide Accurate Information on Application	1. Update AFG Program Guidance and tutorials to instruct potential applicants to register in the National Fire Incident Reporting System and provide required information in support of their grant application.	Completed June 2012
	2. Perform additional grantee outreach and direct applicants to include their Fire Department Identification Number as part of their grant application.	Completed June 2012
Category of Error: Purchase Outside Allowable Timeframe		
1. Purchase Made Outside the Period of Performance	1. Conduct semi-annual grantee outreach and include language in the correspondence reminding grantees to monitor their disbursement progress as it relates to their respective grant's period of performance.	Completed June 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.	Funding required
Category of Error: Unallowable Use of Excess Funds		
1. Use of Excess Funds without Supporting Amendment or to Purchase Ineligible Goods and/or Services	1. Require each applicant to complete the *AFG Grant Management Tutorial* that is currently available on the AFG Program website.	Completed June 2012
Category of Error: Insufficient Documentation		
1. Failure to Submit Supporting Documentation	1. Develop grantee documentation organization and retention guidance and offer associated record keeping training.	March 2013
	2. Develop a plan that outlines procedures for conducting annual audits of grantee supporting documentation.	March 2013

Table 8. Disaster Relief Fund Vendor Payments Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Policies to Prevent Improper Payments		
1. Acquisition manual needs to be strengthened	1. Update acquisition manual to include a chapter on procurement roles and responsibilities for contract payments. Specific points to include: contracting officer delegations; invoice requirements including reviews against regulations, contract terms and conditions; requirements for adequate supporting documentation; procedures for establishing billing rates; and a description of billing mechanisms required for different contract types.	March 2013
	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 2013
2. COTR manual needs to be strengthened	1. Add a chapter on how to review invoices for approval.	March 2013
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 2013
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.	March 2013
Category of Error: Non-Contract Payments		
1. Standard operating procedures needed	1. Develop a process and standard operating procedures for authorizing and paying non-contract payments such as lease payments and bills of lading.	March 2013
Category of Error: Acceptance and Receiving		
1. Reports and contract file maintenance needs improvement	1. Develop a standard inspection, acceptance, and receiving report for contracting officer's technical representatives and complete training on its proper completion and use.	March 2013
	2. Implement an electronic contract file maintenance system.	September 2013

Table 9. Emergency Food and Shelter Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Supporting Documentation		
1. Missing Proof of Purchase	1. Develop guidance around the supporting documentation checklist to state that unless the checklist is completely satisfied, the documentation will not be accepted by EFSP.	Completed 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.	Completed March 2012
3. Missing LRO Documentation: o Missing required certification documents, o 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.	Completed 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.	Completed March 2012
	2. Provide grantees with technical assistance on maintaining adequate documentation for transactions using EFSP funds.	Completed December 2011
Category of Error: Purchase Outside Allowable Timeframe		
1. Purchase Made Outside the Period of Performance	1. Require local boards to conduct outreach activities with LROs throughout the period of performance.	Completed 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 2013
Category of Error: Spending Condition Non-compliance		
1. Spending Condition Errors	1. Develop a mandatory on-line training course to be taken and passed by all local boards and LROs awarded funding.	Funding required
2. Incorrect Rent, Mortgage or Utility Payment: o Current Payments Made Too Early o 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.	Completed March 2012

Table 10. National Flood Insurance Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect Estimate / Worksheet Calculation Errors		
1. Insurance coverage incorrectly applied by adjusters. Claim estimates included items not covered under Flood insurance policy.	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences. 2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	Completed May 2012
Category of Error: Payment Processing Errors		
1. Incorrect Application of Salvage	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences 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.	Completed May 2012
Category of Error: Insufficient Damage Documentation		
1. Lack of supporting documentation for adjuster estimates on lump-sum items. Increased Cost Compliance claims not supported with required claim documentation.	1. Training: Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences. 2. Process Improvement: Increase the frequency of claims operation reviews until satisfactory progress has been made by insurers and flood vendors.	Completed May 2012

Table 11. Public Assistance (PA) Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect Entity Paid		
1. Incorrect Federal Information Processing Standards Number	1. Improve grantee project worksheet (PW) development procedures by incorporating a quality check after the initial PW is completed to confirm all information within the PW is relevant and correct prior to submitting the final version into the system of record.	Completed October 2011
Category of Error: Unmet Work Completion Deadline		
1. Failure to Complete Work During Period of Performance	1. Increase grantee documentation review guidance and create and conduct Public Assistance payment processing training.	Completed March 2012
Category of Error: Scope Discrepancy between Project Worksheet Scope of Work (SOW) and Supporting Documentation		
1. Discrepancies Found between PW SOW and Supporting Documentation	1. Require FEMA project specialists and Public Assistance coordinators to take training courses on proper PW data entry and development, project writing skills, and audit review requirements.	Completed October 2011
	2. Develop reference guides and/or checklists for costs documentation reviews to improve consistency of scope reviews.	Completed 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.	Completed October 2011
Category of Error: Calculation Error between Force Account Summary Sheet and Closeout PW		
1. Mathematical Calculation Error	1. Develop guidance for grantees to eliminate use of rounding in payment calculations to improve accuracy of disbursements of grant funds to sub-grantees.	March 2013
Category of Error: Direct Administrative Costs Not Supported in Closeout PW		
1. Direct Administrative Costs Not Included in Closeout PW	1. Improve guidance and outreach to grantees on payment calculations, quality control, and overall accuracy of information when closing out a PW.	Completed October 2011

Corrective Action Plans for FY12 FEMA High-Risk Program

Table 12. Planned Disaster Relief Fund Vendor Payments Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Policies to Prevent Improper Payments		
1. FEMA COR manual needs to be updated for revised DHS COR policy	1. Update FEMA COR manual to be consistent with DHS COR policy regarding the following: o Clarify who has the authority to approve cost reimbursable and T&M payments (DHS COR manual section 7.14); o Clarify impact of DCAA-DHS MOU requiring 1st invoices be routed through DCAA on cost reimbursable contracts.	March 2013
2. 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 2013
3. 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.	March 2013
Category of Error: Non-Contract Payments		
1. Standard operating procedures needed	1. Develop a process and standard operating procedures for authorizing and paying non-contract payments such as lease payments and bills of lading.	March 2013
Category of Error: Acceptance and Receiving		
1. Reports and contract file maintenance needs improvement	1. Develop a standard inspection, acceptance, and receiving report for contracting officer's technical representatives and complete training on its proper completion and use.	January 2013
	2. Implement an electronic contract file maintenance system.	September 2013

Table 13. Planned Transit Security Grants Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Supporting Documentation		
1. Missing Invoices and Missing Proof of Payment	1. Enhance T*SGP Guidance* related to grant financial management guidelines, standardized minimum reporting requirements, and financial recordkeeping to reduce gaps in the Grantee and Sub-Grantee invoice and/or other expenditure documentation.	March 2013
	2. Require Grantees and Sub-Grantees to comply with document retention requirements past the required three-year grant period.	March 2013
	3. Conduct training for TSGP program and financial officers to include compliance with standardized financial management practices, responding to documentation requests, and document retention	March 2013
Category of Error: Unallowable Costs		
1. Grantee paid overtime to employees beyond standard grant allowable timeframe of six months.	1. Enhance *HSGP Guidance* related to grant financial management guidelines, standardized minimum reporting requirements, and financial recordkeeping to reduce gaps in the Grantee and Sub-Grantee invoice and/or other expenditure documentation.	March 2013
	2. Include language in the Sub-Grantee contracts to specify allowable cost activities in all of the cost categories for the respective award year.	March 2013
	3. Require that Grantees provide allowable cost rationale and documentation to support decision making.	March 2013

Corrective Action Plan for ICE High-Risk Program

Table 14. Completed ERO Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Missing Documentation		
1. Insufficient documentation to support and/or validate financial transactions	1. Provide payment documentation requirements and instructions to the program offices. Instructions to detail the following: (1) invoices that do not contain all invoice backup documentation must be rejected by the receiving and acceptance official, (2) compliance required with record retention guidelines according to National Archives and Records Administration, and (3) the need for program offices to maintain and have readily available all service agreements and memoranda of understanding.	May 2012
	2. Automate FY 2012 IPERA documentation collection by establishing a central SharePoint collaboration site.	March 2012
Category of Error: Invalid / Improper Invoice		
1. Vendor payments delayed or made incorrectly due to inadequate information	1. Conduct refresher training for payment technicians on elements of a proper invoice and ensure that improper invoices are rejected upon receipt.	May 2012
Category of Error: Contract Quality		
1. Improper processing of contracts and obligations; not in compliance with the Federal Acquisition Regulation	1. Implement new receipt and acceptance requirements.	September 2012
Category of Error: Payment Quality and Accuracy		
1. Improper processing of vendor payments and disbursements	1. Conduct refresher training for contracting officer, contracting officer's representatives (COR), and/or program manager to ensure review of invoices to contracted pricing, invoice alignment to correct obligations, and accurate and complete supporting documentation.	May 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.	May 2012

Table 15. Planned ERO Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Identify and Correct Known Errors in ICE Detention Agreements		
1. Payments may be made inaccurately due to amount, vendor, and/or without appropriate supporting documentation	1. Establish a tracking report for identified vendor and pricing errors.	November 2012
	2. Modify detention agreements to correct known vendor errors.	December 2012
	3. Modify detention agreements to correct known pricing errors.	February 2013
	4. Identify FY 2012 invoice documentation for detention agreements currently located at ERO Offices and upload to centralized system of record for retention.	April 2013
Category of Error: Updates Needed to Marshal Service Agreements (MSA) used for ICE Detainees		
1. Payment may be made for ineligible items	1. Review MSAs to ensure ICE is included within the scope of the agreement and, when necessary, notify Procurement of need to add ICE to scope.	December 2012
	2. MSAs modified to include ICE in scope and updated agreement stored in system of record.	February 2013
Category of Error: More Robust Invoice Review and Approval Needed		
1. Payment may be made inaccurately due to amount, vendor, and/or without appropriate supporting documentation	1. Issue interim guidance regarding invoice review and approval to Contracting Officer Representatives (COR).	November 2012
	2. Conduct training sessions for CORs on interim guidance.	December 2012
	3. Develop invoice review checklist and reference guide. Conduct training sessions, as appropriate.	March 2013
	4. Issue final guidance.	March 2013
	5. Update checklist and reference guide. Conduct training sessions for CORs and accounting technicians on final guidance.	April 2013
Category of Error: Inaccurate Contracting Officer Representative Designations		
1. Payment may be made inaccurately due to not being received by a duly authorized official	1. Review existing detention agreements for missing of inaccurate COR designation.	February 2013
	2. Update detention agreement to reflect designated COR.	March 2013

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Poor Obligating and Receiving and Acceptance Procedures		
1. Payments may be made inaccurately due to amount, vendor, not received by duly authorized official, obligation not recorded properly, and/or without appropriate supporting documentation	1. Update procedures for obligating detention agreements.	February 2013
	2. Review, and if necessary, update guidance on completing requisitions for detention agreements to include coordination with Procurement to align contract requirements.	March 2013
	3. Update procedures regarding detention agreements receiving and acceptance. Provide guidance and instruction to CORs.	March 2013
Category of Error: Review and Update Marshal Service Agreements (MSA) used for ICE Detainees		
1. Payment may be made for ineligible items	1. Review MSAs to ensure ICE is included within the scope of the agreement and, when necessary, notify Procurement of need to add ICE to scope.	December 2012
	2. MSAs modified to include ICE in scope and updated agreement stored in system of record.	February 2013
Category of Error: Enhancements Needed to Documentation Retention, Obligation, and Receiving/Acceptance Procedures for Telecommunications Orders		
1. Payment may be made inaccurately without appropriate supporting documentation	1. Issue updated guidance on telecommunication order processing and recording.	March 2013
	2. Update guidance for obligating telecommunications orders and for receiving and acceptance.	May 2013
Category of Error: Contract Quality		
1. Improper processing of contracts and obligations; not in compliance with the Federal Acquisition Regulation	1. Establish and provide "Subject to Availability of Funds" guidance regarding notification to vendor for funds availability, receipt of invoice, and payment of interest.	May 2013

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 16. Completed Federal Protective Service Program Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Contract Oversight		
1. Contractor approving payment of invoices on behalf of the COTR	1. Remove contractors from the process of paying invoices, including terminating contractor access to Webview. Coordinate all Webview access requests through NPPD.	November 2011
2. 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.	March 2012
	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.	June 2012

Table 17. Planned Federal Protective Service Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Contract Oversight		
1. Contractor approving payment of invoices on behalf of the COR	1. Provide CORs with support to review and approve payments within Webview.	March 2013
	2. Issuance of updated Invoicing Policy (POP 603R1). POP 603R1 will provide additional support to CORs by requiring COs to approve all invoices submitted for payment. This will reduce the administrative responsibilities currently placed on the CORs. Per DHS Acquisition policy, the contacting officer may delegate certain authorities to the CORs such as reviewing invoices of any contract type; however approving authority may only be delegated to CORs for Firm Fixed Price type contracts. Most of FPS's contracts are other than Firm Fixed Price.	March 2013
3. Contract Administration Weakness	1. Continue to implement the recommendations of the IPERA Contract Administration Improvement Team and monitor progress/quality improvements	September 2013
	2. Issuance of updated Invoicing Policy (POP 603R1). POP 603R1 will address identified contract administration weaknesses, align FPS processes with the HSAM, and adopt the "best practices" of OPO and NPPD.	March 2013

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 18 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 18. 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 2010 Actual Data)			(Based on FY 2011 Actual Data)			Based on FY 2012 Actual and Estimated Data)			(Based on 2013 Estimated Data)			(Based on 2014 Estimated Data)		
Border Security Fencing (CBP)[3]	$336	0.01%	$0	$197	0.03%	$0	$173	0.01%	$0	$159	0.01%	$0	$157	0.01%	$0
Refund & Drawback (CBP)	$1,198	0.28%	$3	$1,343	0.01%	$0	$1,949	0.01%	$0	$1,300	0.01%	$0	$1,300	0.01%	$0
IHP (FEMA)	$679	0.31%	$2	$880	0.29%	$3	$880	0.29%	$3	$1,022	0.29%	$3	$1,227	0.29%	$4
Disaster Relief Program Vendor Payments (FEMA)	$582	2.87%	$17	$494	3.09%	$15	$494	2.50%	$12	$791	2.00%	$16	$949	1.50%	$14
NFIP (FEMA)	$1,085	1.21%	$13	$794	0.75%	$6	$863	0.75%	$6	$1,036	0.75%	$8	$1,243	0.75%	$9
PA (FEMA)[1]	$3,532	0.32%	$11	$2,990	0.31%	$9	$2,990	0.30%	$9	$3,588	0.25%	$9	$4,306	0.20%	$9
HSGP (FEMA)[1]	$1,516	0.34%	$5	$1,472	1.00%	$15	$1,472	1.00%	$15	$1,766	1.00%	$18	$2,120	0.50%	$11
AFG (FEMA)	$385	5.09%	$20	$471	1.60%	$8	$421	1.50%	$6	$505	1.50%	$8	$606	1.50%	$9
TSGP (FEMA)[1]	$109	0.68%	$1	$196	1.77%	$3	$196	1.50%	$3	$235	1.50%	$4	$282	1.50%	$4
EFSP (FEMA)	$201	7.64%	$15	$45	2.51%	$1	$100	2.00%	$2	$120	1.50%	$2	$144	1.50%	$2
ERO (ICE)	$1,332	8.12%	$108	$1,570	8.47%	$133	$1,652	8.12%	$134	$1,652	5.70%	$94	$1,668	2.28%	$38
FPS (NPPD)	$811	3.27%	$27	$733	1.37%	$10	$900	1.00%	$9	$900	0.50%	$5	$900	0.50%	$5
All Programs[2]	**$11,766**	**1.89%**	**$222**	**$11,185**	**1.82%**	**$203**	**$12,090**	**1.65%**	**$200**	**$13,075**	**1.26%**	**$165**	**$14,901**	**0.70%**	**$104**

Note1: FEMA has three State-Administered Programs—HSGP, PA, and TSGP—that are tested on a three-year cycle. To calculate the national error rate for FY 2011 actual data, error rates from States tested in FY 2011 and FY 2012 were applied to the FY 2011 State payment populations. A weighted average of these tested States was applied as the estimated error rate for States which will be tested in FY 2013. Beginning in FY 2013, a weighted average estimate will no longer be required as all States will have been tested and consequently have a known estimated error rate. These estimated error rates will be updated during the second three-year cycle of improper payment testing. 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.

Note 2: Two programs tested in FY 2011 were not tested in FY 2012 as: (1) the underlying payments were payroll, (2) the estimated error amounts for these programs were under $10 million, and (3) the estimated error rates were 0.13% or less. These two programs are TSA's Aviation Security Payroll and

USCG's Active Duty Military Payroll. In dropping these programs from the Improper Payment Reduction Outlook Table, the Totals for All Programs for PY will differ from the All Program CY totals published in the FY 2011 Annual Financial Report.

Note 3: The prior year outlays figure for CBP's Border Security Fencing Program were increased from the $251 million figure listed in the FY 2011 DHS Annual Financial Report to correct for $85 million in payments which were misidentified by CBP as adjustments. Full details are listed in the DHS Office of Inspector General Report, *Department of Homeland Security's Compliance with the Improper Payments Elimination and Recovery Act of 2010* (OIG-12-48).

Overpayments and Underpayments Details

The table that follows provides overpayment and underpayment breakouts for the Department's high-risk programs. The table shows that over 99 percent of the Department's estimated improper payments are due to overpayments.

Table 19. Overpayment and Underpayment Detail on DHS Sample Test Results

		FY 2012 Gross Total (Based on FY 2011 Actual Data)		FY 2012 Overpayment Total (Based on FY 2011 Actual Data)		FY 2012 Underpayment Total (Based on FY 2011 Actual Data)	
Component	**Program**	**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	0.03%	$0	0.02%	$0	0.01%
	Refund & Drawback (CBP)	$0	0.01%	$0	0.01%	$0	0.00%
FEMA	IHP (FEMA)	$3	0.29%	$3	0.29%	$0	0.00%
	Disaster Relief Fund Vendor Payments (FEMA)	$15	3.09%	$15	3.07%	$0	0.02%
	NFIP (FEMA)	$6	0.75%	$6	0.75%	$0	0.00%
	PA (FEMA)[1]	$9	0.31%	$9	0.30%	$0	0.01%
	HSGP (FEMA)[1]	$15	1.00%	$15	1.00%	$0	0.00%
	AFG (FEMA)	$8	1.60%	$8	1.60%	$0	0.00%
	TSGP (FEMA)[1]	$3	1.77%	$3	1.77%	$0	0.00%
	EFSP (FEMA)	$1	2.51%	$1	2.51%	$0	0.00%
ICE	ERO (ICE)	$133	8.47%	$132	8.42%	$1	0.05%
NPPD	FPS (NPPD)	$10	1.37%	$10	1.37%	$0	0.00%
DHS	**All Programs[2]**	**$203**		**$202**		**$1**	

Note 1: Figures for FEMA's State-Administered Programs (HSGP, PA and TSGP) are based on the National error estimates listed in Table 14.
Note 2: TSA and USCG were removed from the sample test results for FY12 as described in Note 2 to Table 18.

V. Recapture of Improper Payments

DHS completed recovery audit activities for FY 2011 disbursements and continued collection activities for errors identified in prior-year recovery audits. Work was completed at CBP and ICE (and its cross-serviced Components). Recovery activity is underway, but not completed, at FEMA and the U.S. Coast Guard (and its cross-serviced Components). In late FY 2012, FEMA implemented a more rigorous approach to recovery auditing. As a result, FEMA's recovery audit activities are taking longer and are expected to produce improved results. The additional services related to the alternative approach were not available from the recovery audit vendor until late in the fiscal year. The objective of this alternative activity is to determine if the expanded scope produces a more cost-beneficial result for FEMA and the Department.

The U.S. Coast Guard followed up on its telecommunications payments targeted recovery audit activities performed in FY 2011. An in-depth review of claims submitted to telecommunications vendors performed in early FY 2012 revealed that additional scrutiny was necessary to present fully supportable and recoverable claims. As a result, the U.S. Coast Guard rescinded the initial claims, collaboratively worked with the recovery audit vendor to provide the necessary claim information, and re-established updated claims to the telecommunications vendors. The recovery audit vendor

has begun, but not yet completed, recovery audit work over FY 2010 and FY 2011 general payments for the U.S. Coast Guard and its cross-serviced Components.

The U.S. Secret Service entered FY 2012 intending to complete a recovery audit over FY 2010 and FY 2011 payments (stated in the FY 2011 Annual Financial Report). After full consideration of the security restrictions, which necessitate that all recovery audit work be performed on-site, the relatively small size of the U.S. Secret Service, and vendor feedback; the U.S. Secret Service performed a cost analysis and determined that a general recovery audit would not be cost effective at this time. FLETC also updated their cost analysis and determined that a general recovery audit would not be cost effective at this time.

As reported in the FY 2011 Annual Financial Report, the U.S. Coast Guard hired a recovery audit vendor in FY 2011 to perform a targeted, in-depth examination of telecommunications invoices. This examination of 14,000 telecommunications invoices from FY 2005 through FY 2010 initially identified errors totaling $4,144,859, of which $64,460 was recovered, and $4,080,399 underwent collection. All of these improper payments were overpayments. In FY 2012, these claims were re-examined and rescinded after some of the initial claims were challenged by the telecommunications providers. Upon further examination, and support, the U.S. Coast Guard re-established $1,495,732 in claims. An additional claim of $118,457 is pending, and $9,045 in third−party overcharges was recovered.

The low recoupment rate of these payment errors reflects: (1) the fact that this was the U.S. Coast Guard's initial 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 need for due diligence in the validation of the correctness of potential claims.

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.

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

Immediate benefits from this targeted recovery audit activity included the cancelling 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 no longer 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, information technology,

procurement, financial management, and legal has been assembled to rectify known billing issues, and to develop a corrective action plan to improve systemic process and payment errors ensuring the 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 continuous training will be provided to the designated account representatives who order telecommunications services. In addition, telecommunications contracts will be modified as appropriate to include language eliminating the use of third−party billings.

In Table 20, which follows, current year (CY) equals FY 2011 disbursements for all Components except DNDO, TSA, and U.S. Coast Guard where CY equates to FY 2010 and FY 2011 disbursements. Prior year (PY) represents FY 2005–FY 2009 for DNDO, TSA, and U.S. Coast Guard; FY 2004–FY 2010 for CBP, ICE, MGMT, NPPD, OHA, S&T, and USCIS; and FY 2009–FY 2010 for FEMA.

Table 20. Payment Recapture Audit Reporting

Comp.	Type of Payment (contract, grant, benefit, loan, or other)	Amount Subject to Review for CY Reporting ($ millions)	Actual Amount Reviewed and Reported (CY) ($ millions)	Amount Identified for Recovery (CY) ($000)	Amount Recovered (CY) ($000)	% of Amount Recovered out of Amount Identified (CY)	Amount Outstanding (CY) ($000)	% of Amount Outstanding out of Amount Identified (CY)	Amount Determined Not to be Collectable (CY) ($000)	% of Amount Determined Not to be Collectable out of Amount Identified (CY)	Amounts Identified for Recovery (PYs) ($000)	Amounts Recovered (PYs) ($000)[1]	Cumulative Amounts Identified for Recovery (CY + PYs) ($000)	Cumulative Amounts Recovered (CY + PYs) ($000)	Cumulative Amounts Outstanding (CY + PYs) ($000)	Cumulative Amounts Determined Not to be Collectable (CY + PYs) ($000)
CBP	contract	$2,088	$2,088	$13	$8	62%	$5	38%	$0	0%	$250	$246	$263	$254	$5	$2
DNDO[1]	contract	$320	$0	$0	$0	n/a	$0	0%	$0	n/a	$1	$1	$1	$1	$0	$0
FEMA[2]	contract	$1,257	$0	$0	$0	n/a	$0	0%	$0	n/a	$181	$0	$181	$0	$3	$178
ICE	contract	$1,978	$1,978	$1	$1	100%	$0	100%	$0	0%	$1,755	$1,622	$1,756	$1,623	$9	$124
MGMT[3]	contract	$529	$529	$0	$0	n/a	$0	0%	$0	n/a	$210	$210	$210	$210	$0	$0
NPPD[3]	contract	$1,372	$1,372	$2	$2	100%	$0	0%	$0	0%	$216	$216	$216	$216	$0	$0
OHA[3]	contract	$47	$47	$0	$0	n/a	$0	0%	$0	n/a	$0	$0	$0	$0	$0	$0
S&T[3]	contract	$468	$468	$0	$0	n/a	$0	0%	$0	n/a	$55	$55	$55	$55	$0	$0
TSA[1]	contract	$4,424	$0	$0	$0	n/a	$0	0%	$0	n/a	$722	$722	$722	$722	$0	$0
USCG[1]	contract	$5,865	$0	$0	$0	n/a	$0	0%	$0	0%	$4,252	$165	$4,252	$165	$1,630	$2,457
USCIS[3]	contract	$800	$800	$0	$0	n/a	$0	0%	$0	n/a	$904	$892	$904	$892	$3	$9
DHS Totals		**$19,148**	**$7,282**	**$16**	**$11**	**69%**	**$5**	**31%**	**$0**	**0%**	**$8,546**	**$4,129**	**$8,560**	**$4,138**	**$1,650**	**$2,772**

Note 1. DNDO and TSA are cross-serviced by the U.S. Coast Guard. The amount subject to review for CY reporting for DNDO, TSA, and the U.S. Coast Guard cover FY 2010 and FY 2011 disbursements. The individual year total disbursement figures are: for DNDO - $159 million in FY 2011 and $161 million in FY 2010; for TSA - $2,274 million in FY 2011 and $2,150 million in FY 2010; and for the U.S. Coast Guard - $3,045 million in FY 2011 and $2,820 million in FY 2010. Recovery audit activities are underway at all three Components.

Note 2. The recovery audit activities at FEMA are using some new techniques which make it hard to estimate a percent completed. Consequently, the actual amount reviewed and reported CY for FEMA is listed as $0.

Note 3. MGMT, NPPD, OHA, S&T, and USCIS are cross-serviced by ICE.

Note 4. The DHS Totals do not list FLETC and the U.S. Secret Service as these Components completed cost analysis which determined that recovery audit work would not be cost effective at this time.

Table 21. 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
CBP	Contract	$13	$8	62%	100%	100%	100%
ICE	Contract	$1	$1	100%	100%	100%	100%
NPPD	Contract	$2	$2	100%	100%	100%	100%
DHS Totals		**$16**	**$11**	**69%**			

Table 22. 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)
CBP	Contract	$5	$0	$0
DHS Totals		**$5**	**$0**	**$0**

Table 23. 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)
CBP	Contract	$0	$2	$0	$6	$0	$0
ICE	Contract	$0	$0	$0	$1	$0	$0
NPPD	Contract	$0	$0	$0	$2	$0	$0
DHS Totals		**$0**	**$2**	**$0**	**$9**	**$0**	**$0**

The table that follows shows the importance of the Secretary's quarterly high-dollar overpayments reporting. These reports began with January-March 2010 reporting.

Table 24. 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	$7,768	$7,097	$13,818	$13,089	$21,586	$20,186
IPIA High-Risk Program Testing	$0	$0	$1,070	$245	$1,070	$245
Post Payment Reviews	$0	$0	$2,620	$2,582	$2,620	$2,582
DHS Totals	**$7,768**	**$7,097**	**$17,508**	**$15,916**	**$25,276**	**$23,013**

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 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.

Managers are responsible for completing internal control work on payment processing as part of the Department's OMB Circular A-123 effort.

Management's improper payments efforts at all Federal Agencies are subject to an annual compliance review by the Agency's Office of Inspector General. In March 2012, the DHS Office of Inspector General issued *Department of Homeland Security's Compliance with the Improper Payments Elimination and Recovery Act of 2010* (OIG-12-48). This report noted two corrections that need to be included in this report.

The first correction is to Table 17 Payment Recapture Audit Reporting (page 208 of the FY 2011 DHS Annual Financial Report). The amount subject to review for current year reporting and the actual amount reviewed and reported had incorrect payment population figures for ICE and NPPD due to the counting of $813 million of Federal Protective Services' payments under ICE instead of the correct NPPD. The reported payment population for ICE was listed as $2,837 million when $2,024 million was correct. The reported payment population for NPPD was listed as $553 million when $1,366 million was correct. The reporting for this year includes Federal Protective Services' payments under NPPD.

The second correction involved $85 million of payments for CBP's Border Security Fencing Program that CBP mistook as adjustments. These payments were tested after the publication of the FY 2011 DHS Annual Financial Report. A total of four improper payments totaling $16,514 were identified (an error rate consistent with payments tested and reported in the Annual Financial Report). The payment population for FY 2010 payments for CBP's Border Security Fencing Program should therefore have been listed as $336 million rather than $251 million. This correction is noted in Table 14.

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* has been measured between 0.001 percent and 0.005 percent for the period of October 2011 through September 2012, with an annual average of 0.003 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 2011 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.

To ensure compliance with this biennial requirement, each DHS Component is required to compile and furnish individual summaries for each type of user fee by addressing the key points for each user fee, in sufficient detail, to facilitate a review by the OCFO. For FY 2011, six DHS Components were responsible for collecting user fees covering various services provided to the traveling public and trade community. The following is a detailed analysis of the fee collections and costs of the related services:

U.S. Customs and Border Protection (CBP) – CBP is responsible for collecting a variety of user fees related to customs duties, inspections, and immigration. These fees include—

1. Agriculture Quarantine and Inspection
2. Consolidated Omnibus Budget Reconciliation Act of 1985 (COBRA)

3. Immigration Enforcement Fines
4. Immigration
5. Land Border Inspection
6. Electronic System for Travel Authorization
7. Harbor Maintenance
8. Merchandise Processing
9. Puerto Rico Trust Fund
10. Small Airports
11. U.S. Virgin Islands
12. Miscellaneous

During FY 2011, CBP collected approximately $4.5 billion in user fees.

Federal Emergency Management Agency (FEMA) – FEMA is responsible for collecting fees related to the Radiological Emergency Preparedness Program and the National Flood Insurance Fund. During FY 2011, FEMA collected approximately $3.2 billion in user fees.

U.S. Immigration and Customs Enforcement (ICE) – ICE is responsible for collecting a variety of user fees related to immigration. These fees include—

- Immigration Inspection
- Breached Bond Detention Fund
- Student & Exchange Visitors Program
- I-246 Stay of Deportation or Removal

During FY 2011, ICE collected approximately $172.1 million in user fees.

Transportation Security Administration (TSA) – TSA is responsible for collecting a variety of user fees related to the security of the nation's aviation system. These fees include—

- Passenger Civil Aviation Security Service (September 11th Security)
- Aviation Security Infrastructure (Air Carrier)
- Air Cargo Security Requirements (Indirect Air Cargo)
- Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations (GA@DCA)
- Other Security Threat Assessment
- Secure Identification Display Area
- Transportation Worker Identification Credential
- Protection of Sensitive Security Information
- Alien Foreign Student Pilot
- Security Threat Assessments for Hazmat Drivers

During FY 2011, TSA collected approximately $2.3 billion in user fees.

U.S. Coast Guard – U.S. Coast Guard is responsible for collecting a variety of user fees related to maritime safety and security. These fees include—

- Commercial Vessel Documentation
- Recreational Vessel Documentation
- Merchant Mariner Licensing & Documentation
- Commercial Vessel Inspection
- Overseas Vessel Inspection

During FY 2011, U.S. Coast Guard collected approximately $23.5 million in user fees.

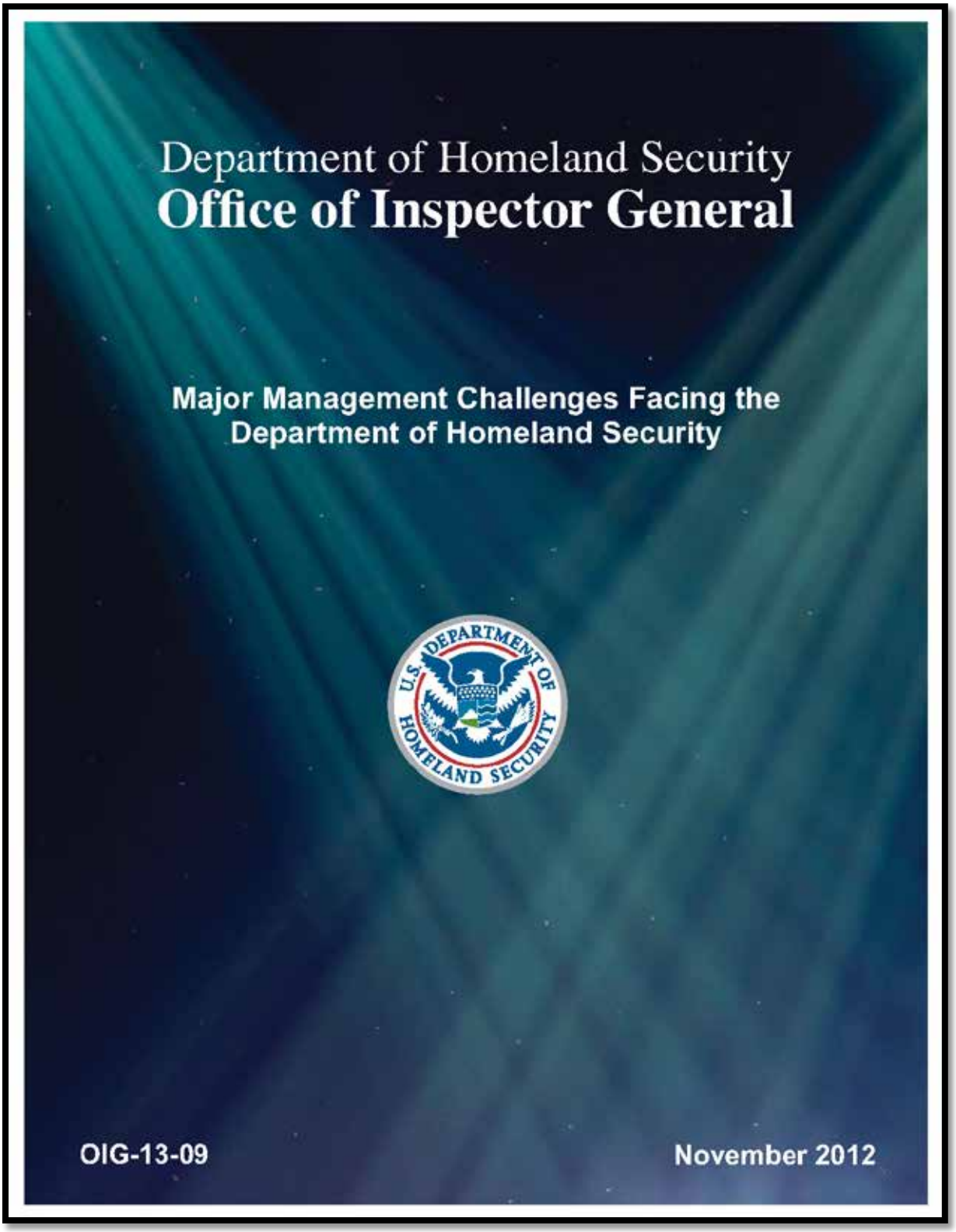
U.S. Citizenship and Immigration Services (USCIS) – USCIS is responsible for collecting a variety of user fees related to the immigration and naturalization process. These fees include—

- Fraud Prevention and Detection
- H-1B Non-Immigrant Petitioner
- Immigration Examinations

During FY 2011, USCIS collected approximately $3.0 billion in user fees.

The OCFO conducted the above DHS user fee assessment based on 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.

Major Management Challenges Facing the Department of Homeland Security



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Major Management Challenges Facing the Department of Homeland Security

The attached report presents our fiscal year 2012 assessment of the major management challenges facing the Department. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually. As stipulated, the report summarizes what the Inspector General considers to be the most serious management and performance challenges facing the agency and briefly assesses the agency's progress in addressing those challenges.

As in previous years, the Department's major challenges are reported in broad areas. For better understanding of how these areas relate to the overall operations of the organization, they have been categorized into two main themes: Mission Areas and Accountability Issues.

Mission Areas

- Intelligence
- Transportation Security
- Border Security
- Infrastructure Protection
- Disaster Preparedness and Response

Accountability Issues

- Acquisition Management
- Financial Management
- IT Management
- Grants Management
- Employee Accountability and Integrity
- Cyber Security

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Mission Areas

Securing the Nation against the entire range of threats that we face in an evolving landscape is a difficult task. The vision and purpose of the Department of Homeland Security (DHS) is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.[1] At its establishment in 2003, the Department faced the challenge of building a cohesive, effective, and efficient Department from 22 disparate agencies, while simultaneously performing the mission for which it was created. As a whole, DHS has made progress in coalescing into a more cohesive organization to address its key mission areas to secure our Nation's borders, increase our readiness, build capacity in the face of a terrorist threat or a natural disaster, and enhance security in our transportation systems and trade operations.

Intelligence

Overview

Intelligence is vital to DHS' framework for securing the Nation. The development, blending, analysis, and sharing of intelligence with appropriate Federal, State, local, tribal, and territorial officials, as well as with private sector partners, must be timely and well coordinated to effectively predict terrorist acts.

Department intelligence programs, projects, activities, and personnel, including the intelligence elements of seven key DHS components, as well as the Office of Intelligence and Analysis (I&A), make up the DHS Intelligence Enterprise. I&A is charged with ensuring that intelligence from the DHS Intelligence Enterprise is analyzed, fused, and coordinated to support the full range of DHS missions and functions, as well as the Department's external partners. The components, most of which predate the creation of the Department, have intelligence elements that provide support tailored to their specialized functions and contribute information and expertise in support of the Department's broader mission set.[2]

[1] http://www.dhs.gov/our-mission

[2] Statement for the Record of Caryn A. Wagner, Under Secretary and Chief Intelligence Officer, Office of Intelligence and Analysis, before the Subcommittee on Counterterrorism and Intelligence House Committee on Homeland Security, "The DHS Intelligence Enterprise - Past, Present, and Future," June 1, 2011.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Challenges

Improving and enhancing support to fusion centers remains a challenge for the Department. To promote greater information sharing and collaboration among Federal, State, and local intelligence and law enforcement entities, State and local authorities established fusion centers throughout the country. A fusion center is a collaboration of two or more agencies to receive, gather, analyze, and disseminate information intending to detect, prevent, investigate, and respond to criminal or terrorist activity. The State and Local Program Office (SLPO), within the Office of Intelligence and Analysis, is responsible for coordinating and ensuring departmental support to the National Network of Fusion Centers.

In our fiscal year (FY) 2012 review, *"DHS' Efforts to Coordinate and Enhance Its Support and Information Sharing with Fusion Centers,"* we assessed: (1) whether the SLPO satisfies the intent of DHS' recommitment to the State, Local, and Regional Fusion Center Initiative; (2) whether planned SLPO efforts will ensure coordinated support of DHS and its components to provide needed information and resources to fusion centers; and (3) if any functional or organizational challenges in DHS hinder its successful support of fusion centers.

Accomplishments

DHS indicated that it has taken significant steps to improve the integration and coordination of intelligence products and processes across the Department. An enhanced analytic plan developed by I&A links data from disparate sources to help identify unattributed cyber intrusions threatening Federal and private sector networks. We determined that since July 2009, the SLPO has increased field support to fusion centers, worked to improve fusion center capabilities, and engaged DHS components. Efforts to develop a department-wide fusion center support strategy are ongoing, but improvements are needed to enhance the I&A's field deployments and DHS component support.[3]

[3] DHS-OIG, *DHS' Efforts to Coordinate and Enhance Its Support and Information Sharing with Fusion Centers* (OIG-12-10, November 2011).

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Transportation Security

Overview

The Transportation Security Administration (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. Airport security includes the use of various technologies to screen passengers and their baggage for weapons, explosives, and other prohibited items, as well as to prevent unauthorized access to secured airport areas. As part of its responsibility, TSA is required to assess and test airport security measures on an ongoing basis to ensure compliance with policies and procedures and prevent security breaches.

Challenges

In spite of TSA's efforts, it continues to face challenges in passenger and baggage screening, airport security, the Secure Flight Program, airport badging, passenger air cargo security, training, as well as in providing oversight for the security of all modes of transportation including rail and mass transit.

Aviation

In regard to passenger and baggage screening, the *Aviation and Transportation Security Act* requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into secured areas of an airport.[4]

In its review of airport security, DHS OIG conducted covert testing of airport access controls as well as passenger and baggage screening.[5] Although test results are classified, access control and checkpoint screening vulnerabilities were identified at the domestic airports tested. Although Transportation Security Officers (TSO) were ultimately responsible for not fully screening checked baggage, our audit identified additional improvements that TSA can make in the evaluation of new or changed procedures, and improvements in supervision of TSOs that could have mitigated the situation.

In FY 2012, a congressional request led to a review of TSA's policies and practices governing its use of full-body x-ray screening equipment (general-use backscatter units)

[4] Public Law 107-71, November 19, 2001.
[5] DHS-OIG, *(U) Covert Testing of Access Controls to Secured Airport Areas* (OIG-12-26, January 2012).

for airport security. Congressman Edward J. Markey was concerned about the safety of the doses of radiation emitted by the units. TSA began deploying general-use backscatter units in March 2010, with 247 units operating in 39 commercial airports around the country at the time of publication of the FY 2012 backscatter unit report. In the United States, an x-ray system is considered compliant with requirements for general-purpose security screening of humans if it complies with standards of the American National Standards Institute.

Independent radiation studies conducted by professional organizations concluded that radiation levels emitted from backscatter units were below the acceptable limits. TSA entered into interagency agreements for additional radiation safety surveys and dosimetry measurement of the dose of radiation emitted by a radiation-generating device monitoring studies to document radiation doses to agency personnel and individuals being screened. All studies concluded that the level of radiation emitted was below acceptable limits.

The Secure Flight Program was implemented in October 2008 in an effort to bolster the TSA security directives established after the terrorist attacks of September 11, 2001. Under this program, TSA receives specific passenger and non-traveler data from the airlines and matches it against the government's watch list. TSA then transmits a boarding pass, with results back to the aircraft operator, so a boarding pass can be issued.

TSA relies on designated airport operator employees to process the badging applications. A July 2011 audit report showed that individuals who pose a threat may obtain airport badges and gain access to secured airport areas.[6] We analyzed vetting data from airport badging offices and identified badge holder records with omissions or inaccuracies in security threat assessment status, birthdates, and birthplaces. These problems existed because TSA did not: (1) ensure that airport operators had quality assurance procedures for the badging application process; (2) ensure that airport operators provided training and tools to designated badge office employees; and (3) require Transportation Security Inspectors to verify the airport data during their reviews.

Through passenger air cargo security, approximately 7.6 million pounds of cargo are transported on passenger planes each day. The Code of Federal Regulations (49 CFR) requires 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 cargo screening procedures employed by

[6] DHS-OIG, *TSA's Oversight of the Airport Badging Process Needs Improvement (Redacted)* (OIG-11-95, July 2011).

air carriers and cargo screening facilities to detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.[7] Although TSA has taken steps to address air cargo security vulnerabilities, the agency did not have assurance that cargo screening methods always detected and prevented explosives from being shipped in air cargo transported on passenger aircraft.

We conducted a review to determine how TSA identifies, reports, tracks and mitigates security breaches at airports nationwide.[8] We determined that TSA does not have guidance for and oversight of the reporting process. This need for guidance resulted in the agency missing opportunities to strengthen airport security. TSA agreed with the recommendations in our report, and as a first step, is developing a standard definition of a security breach. In addition, TSA is also updating its airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels.

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 nearly 27 million passengers every year, using approximately 22,000 miles of rail in 46 states and the District of Columbia. Although grant recipients, such as Amtrak, transit agencies, and State and local authorities, coordinated risk mitigation projects at high-risk rail stations, Amtrak did not always use grant funds to implement mitigation strategies at the highest risk rail stations, in terms of casualties and economic impact.[9] Amtrak did not mitigate 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.

Accomplishments

TSA has taken action as recommended by our audit and inspection work. For instance, the agency began developing detailed utilization reports to ensure that the AIT units deployed are being used efficiently. TSA has also developed more training for TSOs, which should help their performance.

---

[7] DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft* (OIG-10-119, September 2010).
[8] DHS-OIG, *Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports* (OIG-12-80, May 2012).
[9] GAO, *Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened* (GAO-12-837, September 2012).

Since the Secure Flight Program assumed responsibility for passenger prescreening, TSA has provided more consistent passenger prescreening. The program has a defined system and processes to conduct watch list matching. To ensure that aircraft operators follow established procedures, the Secure Flight Program monitors records and uses its discretion to forward issues for compliance investigation. The program also includes privacy safeguards to protect passenger personal data and sensitive watch list records and information. The Secure Flight Program focuses on addressing emerging threats through multiple initiatives.

TSA issued a management directive giving the Operational and Technical Training Division responsibility for overall management of the analysis, design, development, and implementation of TSO training programs.

To identify and track security breaches better, TSA is refining the definition of what constitutes such breaches and implementing a tool to provide more oversight in this area. In addition, TSA is also updating its airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels.

TSA continues to work on improving operations, keeping us informed of the progress made in response to our work.

Border Security

Overview

Securing the Nation's borders from illegal entry of aliens and contraband, including 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 large volumes of illicit cargo entering the country illegally each year. United States Customs and Border Protection (CBP) is responsible for securing the Nation's borders at and between the ports of entry. Within CBP, the mission of the Office of Border Patrol helps secure 8,607 miles of international borders.

Challenges

Although CBP has made progress in securing our borders, it continues to face challenges in the areas of the Free and Secure Trade program (FAST), bonded facilities, unmanned aircraft systems, and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT).

FAST is a commercial clearance program for pre-enrolled commercial truck drivers entering the United States from Canada and Mexico designed to facilitate the free flow

of trade. FAST allows for expedited processing of enrolled trusted travelers, including FAST drivers who fulfill certain eligibility requirements. However, FAST's eligibility processes do not ensure that only eligible drivers remain in the program. CBP is hampered in ensuring that Mexican citizens and residents in the program are low risk because Mexico does not share Southern border FAST information with the United States to assist in vetting and monitoring drivers' eligibility. Although renewal is required every 5 years, ineligible drivers may be actively enrolled in the program, exposing the agency to increased risk of compromised border security.[10]

CBP is responsible for cargo security, including the accountability of the transfer to and storage of cargo at privately owned and operated bonded facilities. Based on audited background checks at 41 bonded facilities at five seaports, CBP did not have effective management controls to ensure that bonded facility employees do not pose a security risk at these facilities. Additionally, CBP neither issued national requirements for background checks on employees of bonded facilities nor ensured that port directors had management controls over background checks at these facilities. As a result, background checks were inconsistent and often ineffective. This may put bonded facilities at greater risk for terrorist exploitation, smuggling, and internal conspiracies. CBP and United States Immigration and Customs Enforcement's (ICE's) Joint Fraud Investigative Strike Teams conducted unannounced investigations of bonded facilities resulting in the detention of more than 350 undocumented workers and workers with outstanding arrest warrants.[11]

Unmanned aircraft systems help secure the Nation's borders from illegal entry of aliens, including terrorists, and contraband, including weapons of mass destruction. These long-endurance, medium-altitude remotely piloted aircrafts provide reconnaissance, surveillance, targeting, and acquisition capabilities. CBP did not adequately plan resources needed to support its current unmanned aircraft inventory. Although CBP developed plans to use the unmanned aircraft's capabilities, its Concept of Operations planning document did not adequately address processes: (1) to ensure that required operational equipment was at each launch and recovery site; (2) for stakeholders to submit unmanned aircraft mission requests; (3) to determine how mission requests were prioritized; and (4) to be reimbursed for missions flown for stakeholders. CBP risks having substantially invested in a program that limits resources and its ability to achieve Office of Air and Marine mission goals.[12]

---

[10] DHS-OIG, *Free and Secure Trade Program-Continued Driver Eligibility* (OIG-12-84, May 2012).
[11] DHS-OIG, *CBP's Management Controls Over Bonded Facilities* (OIG-12-25, January 2012).
12 DHS-OIG, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security* (OIG-12-85, May 2012).

CBP faces challenges in systematically identifying and flagging potential use of fraudulent biographic identities in its US-VISIT system.[13] An analysis of data showed 825,000 instances in which the same fingerprints were associated with different biographic data. These differences ranged from misspelled names and transposed birth dates to completely different names and birth dates. In some cases individuals may have supplied different names and dates of birth at ports of entry; in others individuals may have used different biographic identities at a port of entry after they had applied for a visa under a different name or been identified as a recidivist alien. Inaccurate and inconsistent information reduces the accuracy of US-VISIT data monitoring and impedes the ability to verify that individuals attempting to enter the United States are providing their true names and dates of birth.

Accomplishments

CBP indicated it continues to develop a streamlined and cost-effective process to be used by port offices when conducting background vetting of bonded facility applicants, officers and principals. This process will add significant oversight, tracking and reporting capabilities to the background vetting process and will allow CBP to determine the criminal history of any current or prospective bonded facility applicant. According to CBP officials, US-VISIT has programs to identify individuals who may have overstayed the condition of their visas and manually analyzes entry and exit data to associate fingerprints with biographic information. Stronger oversight of this program will keep better track of individuals entering the United States.

Infrastructure Protection

Overview

Protecting the Nation's critical physical and cyber infrastructure is crucial to the functioning of the American economy and our way of life. Critical infrastructure provides the means and mechanisms by which critical services are delivered to the American people; the avenues that enable people, goods, capital, and information to move across the country. The Department leads the effort, in collaboration with Federal, State, local, regional, and private sector partners, to enhance the protection and resilience of critical infrastructure. Ensuring the security of our critical infrastructure and key resources remains a great challenge.

[13] DHS-OIG, *US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities* (OIG-12-111, August 2012).

Challenges

Catastrophic failures in critical structures such as dams could affect more than 100,000 people and have economic consequences surpassing $10 billion. Yet, the Department could not ensure that risk assessments of dams were conducted or that security risks were identified and mitigated.[14] Specifically, the Department did not review all critical dam risk assessments conducted by other departments and agencies, did not conduct security reviews at 55 percent of critical dams, and did not ensure completion of corrective actions to mitigate risk were completed. Cooperation and collaboration with its security partners is essential to DHS' success in assessing risk and consequently, protecting critical infrastructure such as dams. The *National Infrastructure Protection Plan* prescribes a voluntary partnership between the government and the private sector to manage such risks. The Department does not have the authority to require dam owners to undergo security reviews or implement corrective actions.

DHS' Federal Protective Service (FPS) is responsible for the safety and security of more than 9,000 Federal facilities; the service employs 1,225 Federal staff members and uses 15,000 contracted security guards to carry out its mission. In August 2008, FPS funded a $21 million, 7-year contract to develop and maintain the Risk Assessment and Management Program (RAMP). RAMP was intended to assess and analyze risks to Federal facilities and recommend and track countermeasures, as well as manage post inspections, guard contracts, and guard certification compliance. However, in May 2011, FPS ceased development of RAMP because it was not cost effective and had not met its original goals. In July 2011, the Government Accountability Office (GAO) reported that RAMP's actual costs were more than three times the original $21 million development contract amount, the program was behind schedule, and the system could not be used as intended to complete security assessments or guard inspections. The contract was extended for 1 year to operate and maintain RAMP. Although FPS has stopped its development, the system is still being used to manage its guard force, and it contains historical data that FPS wants to retain and maintain. As of August 2012, FPS had determined its data needs and was working with the RAMP vendor to preserve historical documents and guard-related data.[15] DHS has completed data capture and decommissioned RAMP.

Additionally, according to an August 2012 GAO report, FPS has not effectively led the government facilities sector.[16] It has not obtained data on facilities or coordinated or assessed risk, all of which are key to risk management and safeguarding of critical

[14] DHS-OIG, *DHS Risk Assessment Efforts in the Dams Sector* (OIG-11-110, September 2011).
[15] DHS-OIG, *Federal Protective Service's Exercise of a Contract Option for the Risk Assessment and Management Program* (OIG-12-67, August 2012).
[16] GAO, *Critical Infrastructure: DHS Needs to Refocus its Efforts to Lead the Government Facilities Sector* (GAO-12-852, August 2012).

facilities. Furthermore, FPS has not built effective partnerships across different levels of government, needs a dedicated funding line for its activities in this area, and does not have an action plan for protecting facilities.

Accomplishments

To improve protection of the Dams Sector, DHS is nearing completion of its OIG-recommended assessment of the appropriateness of a legislative proposal to establish regulatory authority for the Dams Sector assets similar to that in the Chemical Sector. At the same time, the Department continues to make strides under the voluntary framework. This includes 100 percent completion of Infrastructure Protection assessments on privately-owned assets included on the FY 2011 Dams Sector critical assets list.

In regard to RAMP, DHS indicated it has minimized FPS costs and saved the government at least $13.2 million by stopping its development and paying the contractor only to operate and maintain the program. FPS also leveraged existing technology to develop the Modified Infrastructure Survey Tool nationwide. During the development, FPS continuously monitored the security posture of Federal facilities by responding to incidents, testing countermeasures, and conducting guard post inspections. Additionally, FPS has taken actions to enhance its coordination with sector-specific agencies for the government facilities sector. These include establishing new relationships with the State, Local, Tribal and Territorial Government Coordinating Council to ensure broader state and local participation in sector coordination procedures.

Disaster and Preparedness Response

Overview

The Federal Emergency Management Agency's (FEMA) task of coordinating emergency support following disasters has become more challenging as the number of events to which it responds has risen each year—from 25 to 70 since 1980. Additionally, FEMA spends an average of $4.3 billion each year in its response efforts. Although the agency has improved its disaster response and recovery, challenges remain.

Challenges

FEMA faces challenges in determining whether to declare events Federal disasters. FEMA uses preliminary disaster assessments to ascertain the impact and magnitude of damage from disasters and the resulting needs of individuals, businesses, the public sector, and the community. These assessments also help to determine whether events become federally declared disasters. In May 2012, we reported that, in deciding whether to declare an event a Federal disaster, FEMA used an outdated indicator that did not accurately measure the ability of State and local governments' to pay for damages.[17] If FEMA had updated the indicator, many recent disasters might not have met the financial conditions for Federal assistance.

In September 2012, GAO also noted that FEMA needed to improve the criteria it used to assess a jurisdiction's ability to recover from disasters.[18] In addition, GAO determined that FEMA had no specific criteria for assessing requests to raise the Federal share for emergency work to 100 percent. Finally, FEMA's administrative costs frequently exceeded its targets.

In evaluating FEMA's disaster recovery in Louisiana, we determined that only 6.3 percent of Katrina-related Public Assistance projects had been closed in the 72 months since the hurricane made landfall.[19] As of July 12, 2011, FEMA had obligated $10.2 billion in Public Assistance grants to support Louisiana's recovery from Hurricane Katrina. However, projects, especially time critical ones such as Debris Clearance and Emergency Work, were years past the closeout deadlines. FEMA, state officials, and subgrantees said the catastrophic damage was the major cause of delay in completing and closing out the Public Assistance projects. According to some officials, delays were also due to issues with the Federal Government's commitment to reimburse Louisiana for 100 percent of all Public Assistance project costs, FEMA's project procurement process, the agency's Public Assistance decision-making, and Louisiana staff resources. We recommended that FEMA develop project management policies, procedures, and timelines for Public Assistance projects that are 100 percent federally funded, coordinate with Louisiana and local governments to evaluate the status of Public Assistance projects, and expedite project closures.

FEMA must have a trained, effective disaster workforce to carry out its mission. As part of this effort, FEMA has a system to credential, or qualify and certify emergency

[17] DHS-OIG, *Opportunities to Improve FEMA's Public Assistance Preliminary Damage Assessment Process* (OIG-12-79, May 2012).
[18] GAO, *Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own* (GAO-12-838, September 2012).
[19] DHS-OIG, *Efforts to Expedite Disaster Recovery in Louisiana* (OIG-12-30, January 2012).

response providers through experience, training, and demonstrated performance. At the time of our June 2012 audit, however, FEMA had not completely implemented a credentialing program and had not identified an IT system to track the training, development, and deployment of disaster employees.[20] Additionally, the agency did not provide a detailed IT plan, documented costs, project schedule, and capability and/or performance requirements.

Our December 2011 audit report showed that some recipients of FEMA Public Assistance grants did not comply with a requirement to obtain and maintain insurance.[21] We also reported that States and FEMA could improve their monitoring and oversight to ensure recipients satisfy this requirement and do not receive financial aid for damages that are, or should be, covered by insurance. State and local governments are encouraged to obtain insurance to supplement or replace Federal Government assistance, but the Public Assistance program provides a disincentive to carry insurance. Although FEMA has been aware of this issue for more than 10 years, it has been slow to address it.

Providing the most efficient and cost-effective temporary post-disaster housing has been a major challenge for FEMA. The deployment of a large number of such housing after Hurricanes Katrina and Rita proved to be difficult. Later, some homes were found to contain high levels of formaldehyde, which led to health problems for disaster survivors. In the aftermath of these disasters, Congress provided FEMA funds to explore options for mitigating future disaster housing issues, including $400 million for an Alternative Housing Pilot Program and $1.4 million for the Disaster Housing Pilot Project.[22]

In the Alternative Housing Pilot Program, it was determined that the units developed were unlikely to match FEMA's needs for temporary housing. The Disaster Housing Pilot Project tested and evaluated 10 different types of housing units and provided options for more cost-effective, future housing, but FEMA put the project on hold because of inadequate funding. FEMA also terminated efforts to develop temporary housing units without indoor air quality issues, although in 2011, these efforts had resulted in model units with acceptable air quality levels. For future disasters, FEMA decided to house displaced disaster victims exclusively in mobile homes built to Department of Housing and Urban Development standards, which will eliminate many past problems. However, these units will likely cost more, are not suitable for flood plains, and will not fit on most urban home sites. The inability to use urban sites may hinder FEMA's capability to

[20] DHS-OIG, *FEMA's Progress in Implementing Employee Credentials* (OIG-12-89, June 2012).
[21] DHS-OIG, *FEMA's Process for Tracking Public Assistance Insurance Requirements* (OIG-12-18, December 2011).
[22] DHS-OIG, *Future Directions of FEMA's Temporary Housing Assistance Program* (OIG-12-20, December 2011).

respond quickly to disasters because alternative sites are limited, take more time to develop, and are frequently blocked by local communities. These sites are also much more expensive than private sites.

Accomplishments

FEMA continues to work on improving preliminary disaster assessments and recovery operations, keeping us informed of the progress made in response to our work. The Disaster Housing Pilot Project was created to evaluate innovative housing options by using them as student housing at a FEMA training facility. It is part of the effort to identify and evaluate alternative means of housing disaster survivors as directed by the Post-Katrina Act. Although the results of the evaluations are not yet complete, the project is providing a cost-effective means of identifying and testing alternative housing units.

FEMA is also pursuing data collection tools that will provide enhanced capabilities to perform Preliminary Damage Assessments (PDA) and record information in an efficient and consistent manner. FEMA is assessing the best available options for development of such a tool for PDAs, based on efforts to explore development of such a tool and in light of available technologies. Based on the findings of the assessment, FEMA plans to develop and implement the improved PDA data collection tool in FY13. This will improve PDA data collection, streamline the PDA process through use of an electronic system for data collection and reporting, and enhance the effectiveness of the PDA process.

According to FEMA, as of October 1, 2012, the FEMA Qualification System (FQS) became operational. FQS establishes the system for qualification and certification of the FEMA incident workforce through experience, training, and demonstrated performance. Throughout the year, milestones have been met to implement this critical program along with our other disaster workforce initiatives. While there will be continued development and expansion of the program FQS has been implemented for the entire incident management workforce.

FEMA is implementing other initiatives to improve disaster budgeting and program management once a declaration has been made that will enhance FEMA's ability to manage and budget for expenditures from the Disaster Relief Fund.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Accountability Issues

As the third largest agency in the Federal Government, DHS is responsible for managing a large workforce, and significant Federal resources. DHS is responsible for an annual budget of more than $59 billion, employs more than 225,000 employees and operates in more than 75 countries. At its establishment in 2003, DHS faced building a cohesive and efficient organization from 22 disparate agencies, while simultaneously performing the critical mission for which it was created. As a whole, DHS has made progress in coalescing into a more effective organization, establishing policies and procedures to set the groundwork for effective stewardship over its resources but challenges remain.

Acquisition Management

Overview

Effective oversight and management of acquisition processes is vital to DHS. At the time of our reporting in 2012, the Department had approximately 160 acquisition programs with estimated life cycle costs of more than $144 billion. DHS' acquisitions were numerous, varied, and complex, including everything from ships, aircraft, and vehicles to real estate, computer technology, and maintenance services.

Challenges

During FY 2012 both OIG and GAO conducted audits of acquisition management, examining individual acquisition programs and the underlying policies and procedures. We identified challenges the Department faces in the Secure Border Initiative. For example, along the southwest border, CBP has spent $1.2 billion to construct physical barriers as part of the Secure Border Initiative. As part of that effort, CBP did not effectively manage the purchase and storage of steel for fence construction, which cost about $310 million. It purchased steel before legally acquiring land or meeting international treaty obligations. In addition, CBP did not provide effective contract oversight, including not paying invoices on time and not reviewing the contractor's selection of a higher-priced subcontractor. As a result of these issues, CBP purchased more steel than needed, incurred additional storage costs, paid interest on late

payments, and approved a higher-priced subcontractor, resulting in expenditures of nearly $69 million that could have been put to better use.[23]

A November 2011 GAO review of the subsequent southwest border strategy, the Arizona Border Surveillance Technology Plan, showed that DHS did not document the analysis justifying the specific types, quantities, and deployment locations of border surveillance technologies proposed in the plan.[24] Without documentation DHS was hindered in its ability to verify that processes were followed, identify underlying analyses, assess the validity of the decisions made, and justify the requested funding.

Acquisition and resource management will continue to be a challenge for the United States Coast Guard (USCG) as it strengthens acquisition management capabilities and develops acquisition program baselines for each asset. According to GAO, the approved baselines for 10 of 16 programs did not reflect cost and schedule plans because programs breached the cost or schedule estimates in those baselines, changed in scope, or were not expected to receive funding to execute baselines as planned.[25] According to DHS, during 2012, two USCG program baselines were approved by DHS, two are pending DHS approval, and one is in USCG routing.

Since 2003, under a program to replace its aging HU-25 Falcon fleet, the USCG has taken delivery of 13 Ocean Sentry Maritime Patrol medium-range surveillance aircraft. In most instances, the USCG awarded the Ocean Sentry Maritime Patrol aircraft contracts effectively. However, it could have improved its oversight of the latest contract, awarded in July 2010 to the European Aeronautic Defense and Space Company North America for three aircraft valued at nearly $117 million. For this contract, the USCG was aware of conclusions by the Defense Contract Audit Agency regarding non-chargeable costs and noncompliance with the Federal Acquisition Regulation by the subcontractor, European Aeronautic Defense and Space Company/Construcciones Aeronáuticas Sociedad Anónima. The USCG was aware of the conclusions, and could have conducted additional follow up to ensure that the subcontractor had implemented recommendations made by the Defense Contract Audit Agency. The USCG also did not obtain sufficient support to ensure it excluded non-chargeable costs when awarding the latest contract.[26]

The Department continues to face challenges in integrating the 22 disparate legacy agencies and these challenges have a direct affect on acquisition management

---

[23] DHS-OIG, *U.S. Customs and Border Protection's Management of the Purchase and Storage of Steel in Support of the Secure Border Initiative* (OIG-12-05, November 2011).
[24] GAO-OIG, *Portfolio Management Approach Needed to Improve Major Acquisition Outcomes*, (GAO-12-918, September 2012).
[25] GAO, *More Information on Plans and Costs Is Needed before Proceeding* (GAO-12-22, November 2011).
[26] DHS-OIG, *U.S. Coast Guard's Maritime Patrol Aircraft* (OIG-12-73, April 2012).

decisions. According to a September 2012 GAO report, DHS acquisition policy does not fully reflect several key portfolio management practices, such as allocating resources strategically, and DHS has not yet re-established an oversight board to manage its investment portfolio across the Department.[27] For example, there have been numerous efforts to find efficiencies between CBP's and USCG's aviation fleets. The Secretary's FY 2013 budget emphasized consolidating and streamlining systems and operations to ensure cost savings. In a March 2012 hearing, the Secretary highlighted efforts to increase the effectiveness of DHS' aviation assets through increased coordination and collaboration. In 2010, CBP and the USCG signed a joint strategy to unify their aviation management information systems. However, as of July 2012, CBP planned to acquire a new, separate IT system for its aircraft, which would continue past practices of obtaining disparate systems that did not share information with other components, including the USCG. We recommended that CBP terminate this planned acquisition and transition its aviation logistics and maintenance tracking to the USCG's system, in accordance with the Secretary's efficiency initiatives and the joint strategy. By transitioning to the USCG's system, CBP could improve the effectiveness of aviation management information tracking and save more than $7 million.[28]

Accomplishments

According to DHS, it has made progress in improving program governance, increasing insight into program performance, and building acquisition and program management capabilities. DHS has implemented requirements for tiered acquisition program reviews intended to increase its ability to identify and mitigate program risk. The Department has also implemented a Decision Support Tool to provide visibility into program health and has established Centers of Excellence to provide guidance.

In August, 2012, we reported that DHS was progressing toward the implementation of an information technology infrastructure at the St. Elizabeth's Campus in Washington, DC.[29] Specifically, DHS partnered with the General Services Administration to use its interagency information technology contracting vehicles. The General Services Administration also awarded a task order on behalf of DHS to acquire information technology resources for the Technology Integration Program.

The Department has created an Acquisition Workforce Development initiative to improve its acquisition workforce. This initiative includes expanding training opportunities and offering certification programs in Cost Estimating, Program Financial

[27] GAO, *DHS Requires More Disciplined Investment Management to Help Meet Mission Needs* (GAO-12-833, September 2012).
[28] DHS-OIG, *CBP Acquisition of Aviation Management Tracking System* (OIG-12-104, August 2012).
[29] DHS-OIG, *Adherence to Acquisition Management Policies Will Help Reduce Risks to the Technology Integration Program*, (OIG-12-107, August 2012).

Management, Life Cycle Logistics, and Test and Evaluation and Systems Engineering. When the outcomes of this initiative are achieved the Department's acquisition workforce will be ready to acquire and sustain the systems and services necessary to secure the homeland, while ensuring that the Department and taxpayers received the best value for the expenditure of public resources.

Financial Management

Overview

The Federal government has a fundamental responsibility to be an effective steward of taxpayer dollars. Sound financial practices and related management operations are critical to achieving the Department's mission and to providing reliable, timely financial information to support management decision-making throughout DHS. Congress and the public must be confident that DHS is properly managing its finances to minimize inefficient and wasteful spending, make informed decisions to manage government programs, and implement its policies.

Although DHS produced an auditable balance sheet and statement of custodial activity in FY 2011 and obtained a qualified opinion on those statements, challenges remain for the Department's financial management. Achieving a qualified opinion resulted from considerable effort by DHS employees, rather than through complete implementation of a reliable system of control over financial reporting. As a result of DHS obtaining a qualified opinion on its balance sheet and statement of custodial activity in FY 2011, the scope of the FY 2012 audit was increased to include statements of net cost, changes in net position, and combined statement of budgetary resources.

Challenges

Managerial Cost Accounting

The Department does not have the ability to provide timely cost information by major program, and by strategic and performance goals. The Department's financial management systems do not allow for the accumulation of costs, at the consolidated level, by major program, nor allow for the accumulation of costs by responsibility segments directly aligned with the major goals and outputs described in each entity's strategic and performance plan. Further, the Department needs to develop 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 consolidated data.

OIG conducted several audits during FY 2012 and identified a number of components that did not have the ability to provide various cost data when requested. For example:

- During the audit of TSA's Aviation Channeling Service Provider program (OIG 12-132-AUD-TSA) we learned that TSA did not track and report all project costs related to the program. According to TSA program officials, it was impossible to provide exact costs because the expenditures were not tracked in detail.
- During the audit examining CBP's acquisition and conversion of H-60 helicopters (OIG 12-102-AUD-CBP), CBP officials received high-level cost information from the U.S. Army, but it did not include the detail necessary to adequately oversee the CBP H-60 programs. For example, the Army conducted approximately 15,000 tests on CBP H-60 components, but CBP could not identify the tests that were completed or the specific costs. In addition, for each CBP H-60 helicopter, financial data from three sources listed a different total cost for each helicopter.
- During the audit of CBP's use of radiation portal monitors at seaports (OIG 12-033-AUD-CBP), we found instances in which the acquisition values for the monitors were incorrect and could not be supported.

Anti-Deficiency Act Violations

The Department continues to have challenges in complying with the Anti-Deficiency Act (ADA). As of September 30, 2012, the Department and its components reported five potential ADA violations in various stages of review, including one potential ADA violation identified in FY 2012, which the Department is currently investigating. The four other ADA violations involve: (1) expenses incurred before funds were committed or obligated; (2) pooled appropriations to fund shared services; (3) a contract awarded before funds had been re-apportioned; and (4) improper execution of the obligation and disbursement of funds to lease passenger vehicles.

Financial Statement Audit

The following five items show the status of DHS' effort to address internal control weaknesses in financial reporting. These were identified as material weaknesses in the FY 2011 independent audit of DHS' consolidated balance sheet and statement of custodial activity. All five material weaknesses remain in FY 2012.

Financial Reporting

Financial reporting presents financial data on an agency's financial position, its operating performance, and its flow of funds for an accounting period.

In FY 2011 the USCG, USCIS, and TSA contributed to the material weakness in this area. While some findings reported in FY 2011 were corrected, other findings at USCG and TSA remained in FY 2012. Also, in FY 2012, new financial reporting findings were identified at ICE.

As in the previous year, the auditors reported this year that the USCG does not have properly designed, implemented, and effective policies, procedures, processes, and controls surrounding its financial reporting process. The USCG uses three general ledgers, developed over a decade ago. This legacy system has severe functional limitations that contribute to its ability to address systemic internal control weaknesses in financial reporting, strengthen the control environment, and comply with relevant Federal financial system requirements and guidelines.

The auditors identified deficiencies that remain in some financial reporting processes at TSA. For example, there are weak or ineffective controls in some key financial reporting processes, of the management's quarterly review of the financial statements, and in supervisory reviews over journal vouchers. In addition, TSA has not fully engaged certain program and operational personnel and data into the financial reporting process and is not fully compliant with the United States Government Standard General Ledger requirements at the transaction level. In recent years, TSA implemented several new procedures and internal controls to correct known deficiencies, but some procedures still require modest improvements to fully consider all circumstances or potential errors. The control deficiencies contributed to substantive and classification errors reported in the financial statements and discovered during the audit.

During FY 2012, the auditors noted financial reporting control weaknesses at ICE, primarily resulting from expanded audit procedures for the full-scope financial statement audit. ICE has not fully developed sufficient policies, procedures, and internal controls for financial reporting. It also needs adequate resources to respond to audit inquiries promptly, accurately, and with the ability to identify potential technical accounting issues. ICE faces challenges in developing and maintaining adequate lines of communication within its Office of Financial Management and among its program offices. Communication between financial managers and personnel responsible for contributing to financial reports was not sufficient to consistently generate clear and usable information. In addition, ICE does not have sufficient coordination with IT personnel, including contractors, who are responsible for generating certain financial reports.

Information Technology Controls and Financial Systems Functionality

IT general and application controls are essential to effective and reliable reports of financial and performance data.

During the FY 2011 financial statement audit, the independent auditor noted that the Department remediated 31 percent of the prior year IT findings. The most significant FY 2011 weaknesses include: (1) excessive unauthorized access to key DHS financial applications, resources, and facilities; (2) configuration management controls that are not fully defined, followed, or effective; (3) security management deficiencies in the certification and accreditation process and an ineffective program to enforce role-based security training and compliance; (4) contingency planning that lacked current, tested contingency plans developed to protect DHS resources and financial applications; and (5) improperly segregated duties for roles and responsibilities in financial systems. These deficiencies negatively affected the internal control over DHS' financial reporting and its operation and contributed to the FY 2011 financial management and reporting material weakness.

For FY 2012, DHS made some progress in correcting the IT general and application control weaknesses identified in FY 2011. DHS and its components remediated 46 percent of the prior year IT control weaknesses, with CBP, FEMA, and TSA making the most progress in remediation. Although CBP and FEMA made progress in correcting their prior year issues, in FY 2012, the most new issues were noted at these two components. New findings resulted primarily from new IT systems and business processes that came within the scope of the FY 2012 financial statement audit and that were noted at all DHS components.

The auditors noted many cases in which financial system functionality inhibits DHS' ability to implement and maintain internal controls, notably IT application controls supporting financial data processing and reporting. As a result, ongoing financial system functionality limitations are contributing to the Department's challenge to address systemic internal control weaknesses and strengthen the overall control environment.

In FY 2012, five IT control weaknesses remained and presented 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 (PP&E) operating materials, as well as supplies, including boats and vessels at the USCG,

passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA. The USCG maintains approximately 50 percent of all DHS PP&E.

During FY 2011, TSA, the USCG, CBP, and the Management Directorate contributed to a departmental material weakness in PP&E. During FY 2012, TSA and Management Directorate substantially completed corrective actions in PP&E accounting processes. In FY 2012, the USCG continued to remediate PP&E process and control deficiencies, specifically those associated with land, buildings and other structures, vessels, small boats, aircraft, and construction in process. However, remediation efforts were not fully completed in FY 2012. The USCG had difficulty establishing its opening PP&E balances and accounting for leases, primarily because of poorly designed policies, procedures, and processes implemented more than a decade ago, combined with ineffective internal controls and IT system functionality difficulties.

As in prior years, CBP has not fully implemented policies and procedures, or does not have sufficient oversight of its adherence to policies and procedures, to ensure that all PP&E transactions are recorded promptly and accurately, or to ensure that all assets are recorded and properly valued in the general ledger. Further in FY 2012, ICE did not have adequate processes and controls in place to identify internal-use software projects that should be considered for capitalization.

Environmental and Other Liabilities

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

The USCG's environmental liabilities represent approximately $500 million or 75 percent of total DHS environmental liabilities. The USCG completed the final phases of a multi-year remediation plan to address process and control deficiencies related to environmental liabilities later in FY 2012. However, the USCG did not implement effective controls to ensure the completeness and accuracy of all underlying data components used to calculate environmental liability balances. Further, the USCG did not have documented policies and procedures to update, maintain, and review schedules to track environmental liabilities (e.g., Formerly Used Defense Sites) for which it was not primarily responsible at the Headquarters level. Additionally, the USCG did not effectively implement existing policies and procedures to validate the prior year accounts payable estimate.

Budgetary Accounting

Budgetary accounts are general ledger accounts for recording transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources. DHS has numerous sources and types of budget authority, including annual, multi-year, no-year, and permanent and indefinite appropriations, as well as several revolving, special, and trust funds. Timely and accurate accounting for budgetary transactions is essential to managing Department funds and preventing overspending.

The USCG implemented corrective actions plans over various budgetary accounting processes in FY 2012; however, some control deficiencies reported in FY 2011 remain, and new deficiencies were identified. Although FEMA also continued to improve its processes and internal controls over the obligation and monitoring process, some control deficiencies remain.

As the financial service reporting provider, ICE is responsible for recording budgetary transactions and administers budgetary processes across different types of funds at the National Protection and Programs Directorate, Science and Technology Directorate, Management Directorate, and Office of Health Affairs. In FY 2011, ICE identified and began remediating deficiencies in the financial management system that impact accounting transactions such as positing logic related to adjustments of prior year unpaid, undelivered orders. In FY 2012, ICE continued to address these issues with certain types of obligations.

Accomplishments

The Department continues to work on improving financial reporting. In FY 2012, DHS received a qualified opinion on its financial statements. Improvements were seen at various components. For example, USCIS corrected control deficiencies in financial reporting that contributed to the overall material weakness. Likewise, TSA made significant progress in addressing PP&E, removing its contribution to the Department's material weakness. Further, the USCG continued to make financial reporting improvements in FY 2012 by completing its planned corrective actions over selected internal control deficiencies. These remediation efforts allowed management to make new assertions in FY 2012 related to the auditability of its financial statement balances. In addition, management was able to provide a qualified assurance of internal control over financial reporting in FY 2012.

According to DHS' Office of Financial Management, there is improved access to and better quality of financial management information. The Department has implemented

business intelligence tools to help organize, store, and analyze data more efficiently. According to the office, the Department can now take information from individual budgets and display it for the enterprise, allowing views of DHS' budget allocation by mission area. Additionally, the Department is developing management tools (Decision Support Tool) to help compile department-wide program cost information. The Decision Support Tool should provide a central dashboard to assess and track the health of acquisition projects, programs, and portfolios by showing key indicators of program health, such as cost, funding, and schedule.

IT Management

Overview

As technology constantly evolves, the protection of the Department's IT infrastructure becomes increasingly more important. The Department's Chief Information Officer (CIO) has taken steps to mature IT management functions, improve IT governance, and integrate IT infrastructure. Specifically, at the Department level, the CIO has increased IT governance oversight and authority by reviewing component IT programs and acquisitions. Although the Department's documented processes were still draft, these steps have enabled the CIO to make strategic recommendations to reduce costs and duplication through activities such as infrastructure integration, as well as data center and network consolidation.

Challenges

Several DHS components continue to face IT management challenges. For example, in a November 2011 audit, we reported that USCIS delayed implementing its transformation program because of changes in the deployment strategy and system requirements that were insufficiently defined prior to selecting the IT system solution.[30] Other challenges, such as the governance structure, further delayed the program. As a result, USCIS continued to rely on paper-based processes to support its mission, which made it difficult for the component to process immigration benefits efficiently, combat identity fraud, and provide other government agencies with information to identify criminals and possible terrorists quickly. USCIS took steps to address some of these challenges by moving to an agile development approach, instead of a "waterfall" process. This change improved program monitoring and governance and increased the focus on staffing issues.

[30] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG-12-12, November 2011).

According to a June 2012 audit, CBP needs to address systems availability challenges, due in part to an aging IT infrastructure.[31] Limited interoperability and functionality of the technology infrastructure made it difficult to fully support CBP mission operations. As a result, CBP employees chose to use alternative solutions, which may have hindered CBP's ability to accomplish its mission and ensure officer safety.

DHS has matured key information IT functions, such as portfolio management. However, in May 2012, we reported that recruiting people with the necessary skills to perform certain management functions remains a challenge. Also, DHS needs to improve its budget review process so that the CIO can identify and resolve issues before components finalize their IT investments.[32] In addition, GAO reported in July 2012 that DHS had a vision for its new IT governance process, which included a tiered oversight structure with distinct roles and responsibilities throughout the Department. However, DHS' IT governance policies and procedures were not finalized, which meant less assurance that its new IT governance would consistently support best practices and address previously identified weaknesses in investment management.[33]

CBP needs to improve its compliance with Federal privacy regulations. It also needs to establish an Office of Privacy with appropriate resources and staffing. Although DHS has a directive to ensure compliance with all privacy policies and procedures issued by the Chief Privacy Officer, an April 2012 audit disclosed that CBP made limited progress toward instilling a culture of privacy that protects sensitive personally identifiable information.[34] Without a component-wide approach that minimizes the collection of employee Social Security numbers, privacy incidents involving these numbers will continue to occur.

Accomplishments

The Department has created initiatives to improve IT Program Governance and Information Security. These programs are designed to prioritize programs to meet Department business needs, eliminate duplicate functions and systems, increase program accountability and strengthen internal controls.[35] Progress has been made to meet the goals of these initiatives and once fully achieved, the Department will have increased accountability for its information technology programs.

---

[31] DHS-OIG, *CBP Information Technology Management: Strengths and Challenges* (OIG-12-95, June 2012).
[32] DHS-OIG, *DHS Information Technology Management Has Improved, But Challenges Remain* (OIG-12-82, May 2012).
[33] GAO, *DHS Needs to Further Define and Implement Its New Governance Process* (GAO-12-818, July 2012).
[34] DHS-OIG, *U.S. Customs and Border Protection Privacy Stewardship* (OIG-12-78, April 2012).
[35] DHS, *Integrated Strategy for High Risk Management: Implementation and Transformation* (June 2012).

According to DHS, the CIO has created performance measures to help establish accountability and determine progress and accomplishments in IT Program Governance. For example, one measure is the number of IT segments covered by portfolio governance. Since IT segments represent a subset of the Department's mission and a business portfolio, this measure has resulted in an increase in the number of IT functions that have governance in place. In the beginning of FY 2012, only 5 of 30 IT segments were covered by portfolio governance. By the end of FY 2012, the Office of the CIO achieved its target to attain portfolio governance for 10 of 30 (33 percent) IT segments. By the end of FY 2013, the office will capture an additional 5 segments to reach its goal of 50 percent (15 of 30). By FY 2016, the goal is to have all 30 functional areas with IT governance.

Grants Management

Overview

More than $35 billion in homeland security grants have been provided over the past 10 years to States, territories, local, and tribal governments to enhance capabilities to plan, prepare for, prevent, respond to, and recover from natural disasters, acts of terrorism, and other manmade disasters. In grants management, FEMA is challenged to ensure the grants process is transparent, efficient, and effective. FEMA must also provide oversight to a large number of geographically dispersed grant recipients to ensure Federal funds are used for their intended purposes.

Challenges

FEMA can improve its efforts in strategic planning, performance measurement, oversight, and sustainment, including tracking States' milestones and accomplishments for homeland security grant-funded programs. FEMA needs to improve its strategic management guidance for State Homeland Security Grants. In our most recent *Annual Report to Congress*, we summarized State Homeland Security strategies and identified deficiencies related to measurable goals and objectives. Although current guidance for State Homeland Security strategies encourage revisions every 2 years, such revisions are not required. Additionally, we identified State Homeland Security strategies that do not have goals and objectives that are specific, measurable, achievable, results-oriented, and time-limited. Without a measurable goal or objective, or a process to gather results oriented data, States may not be assured that their preparedness and response capabilities are effective. States are also less capable of determining progress toward goals and objectives when making funding and management decisions.

FEMA has not provided sufficient guidance on establishing metrics and measuring performance. Our audits show that States continue to need the proper guidance and documentation to ensure accuracy or track milestones. Providing guidance on the appropriate metrics and requiring documentation of those metrics would help States understand the effectiveness of each grant program.

FEMA also needs to strengthen its guidance on reporting progress in achieving milestones as part of the States' annual program justifications. We determined that States' milestones for these continuing investment programs could not be compared to those in previous years' applications. Additionally, the status of the previous year milestones was not always included in applications. Because of these weaknesses, FEMA could not determine, from the annual application process, whether a capability had been achieved, what progress had been made, or how much additional funding was needed to complete individually justified programs. Without this information, FEMA could not be assured it made sound investment decisions.

Because of insufficient information on milestones and program accomplishments, FEMA annually awarded Homeland Security Grant Program funds to States for ongoing programs without knowing the accomplishments from prior years' funding or the extent to which additional funds were needed to achieve certain capabilities. Tracking accomplishments and milestones are critical to making prudent management decisions because of the changes that can occur between years or during a grant's period of performance.

FEMA needs to improve its oversight to ensure States are meeting their reporting obligations in a timely manner so that the agency has the information it needs to make program decisions and oversee program achievements. Improved oversight will also ensure that States are complying with Federal regulations on procurements and safeguarding of assets acquired with Federal funds. In our annual audits of the State Homeland Security Program, we repeatedly identified weaknesses in the States' oversight of grant activities. Those weaknesses include inaccuracies and untimely submissions of financial status reports; untimely allocation and obligation of grant funds; and not following Federal procurement, property, and inventory requirements.

Delays in the submission of Financial Status Reports may have hampered FEMA's ability to monitor program expenditures effectively and efficiently. They may also have prevented the States from drawing down funds in a timely manner and ultimately affected the functioning of the program. Delays also prevented the timely delivery of plans, equipment, exercises, and training for first responders.

In our audits in FYs 2011 and 2012, we noticed an emerging trend with issues related to program sustainment. States did not prepare contingency plans addressing potential

funding shortfalls when DHS grant funding was significantly reduced or eliminated. In an era of growing budget constraints it is important to use resources for projects that can be sustained. FEMA addressed this issue in its FY 2012 grant guidance by focusing on sustainment rather than new projects.

Accomplishments

Although significant issues in grants management remain, progress has been made. In most instances, audited States efficiently and effectively fulfilled grant requirements, distributed grant funds, and ensured available funds were used. The States also continued to use reasonable methodologies to assess threats, vulnerabilities, capabilities, and needs, as well as allocate funds accordingly. Our audits have identified several effective tools and practices used by some States that could benefit all States; FEMA and the States also willingly shared information. FEMA has been responsive to our recommendations and the agency is taking action to implement those recommendations. At the Headquarters level, DHS is establishing a governance body that will determine high-risk areas such as those cited above, develop strategies to mitigate those risks and employ standardized formats, templates, and processes to ensure consistent financial assistance activities throughout DHS. Some of these standardized templates and processes are already in place.

Employee Accountability and Integrity

Overview

The smuggling of people and goods across the Nation's borders is a large scale business dominated by organized criminal enterprises. The Mexican drug cartels today are more sophisticated and dangerous than any other organized criminal groups in our law enforcement experience. Drug trafficking organizations are becoming increasingly more involved in systematic corruption of DHS employees to further alien and drug smuggling. The obvious targets of corruption are front line Border Patrol Agents and CBP officers; less obvious are those employees who can provide access to sensitive law enforcement and intelligence information, allowing the cartels to track investigative activity or vet their members against law enforcement databases. Although the number of DHS employees implicated in such enterprises is very small — less than 1 percent — the damage from even one corrupt employee represents a significant management challenge to the Department.

Border corruption affects national security. As demonstrated by investigations led by our investigators, border corruption may consist of cash bribes, sexual favors, or other

gratuities in return for allowing contraband or undocumented aliens through primary inspection lanes; orchestrating illegal border crossings; leaking sensitive law enforcement information to persons under investigation; selling law enforcement intelligence to smugglers; and providing needed documents such as immigration papers. Corrupt employees most often are paid not to inspect, as opposed to allowing prohibited items, such as narcotics, to pass into the U.S. A corrupt DHS employee may accept a bribe for allowing what appears to be simply undocumented aliens into the U.S. while unwittingly helping terrorists enter the country. Likewise, what seems to be drug contraband could be weapons of mass destruction, such as chemical or biological weapons, or bomb-making material.

Challenges

We have seen a 95 percent increase in complaints against CBP employees alone since FY 2004 and a 25 percent increase from just fiscal year 2010 to 2011. In FY 2011, we received and disposed of 17,998 allegations involving all DHS employees. As of July 15, 2012, we had 1,591 open cases. Corruption-related allegations are a priority of the Office of Investigations, which opens 100 percent of all credible allegations of corruption it receives. The majority of both complaints received and investigations initiated by the OIG, however, are for allegations of other than corruption-related activity.

Since FY 2004, our investigations have resulted in 358 CBP related convictions and 166 ICE related convictions. In one case, we received information that a CBP Officer was using his position at a large urban airport to support an international drug trafficking organization. Our investigators joined a multiagency investigation, led by the ICE Office of Professional Responsibility (OPR), which resulted in the dismantling of the entire drug trafficking organization and the arrest of multiple offenders, including the CBP Officer. On at least 19 separate occasions, the CBP Officer had bypassed airport security using his own badge to smuggle money and weapons for the drug traffickers. In December 2010, he was convicted and sentenced to 8 years in prison.

A Border Patrol Agent at the Sonoita, Arizona, Border Patrol Station, was observed acting suspiciously while questioning others about the technology used to interdict smugglers. The agent had only entered on duty at Sonoita in March 2009, shortly after graduating from the Border Patrol Academy. We opened an investigation and developed evidence that the agent had sold to a purported drug trafficker sensor maps, trail maps, landmarks, and terminology used by the Border Patrol to combat smuggling. Evidence showed that on at least four occasions, the agent accepted bribes totaling around $5,000. The agent was arrested in October 2009. On August 12, 2010, he pled guilty in Federal court to one count of bribery. On May 3, 2011, he was sentenced to 20

months incarceration, 36 months supervised release, and was ordered to pay restitution in the amount of $5,500.

Proper filing of Office of Government Ethics (OGE) forms is vital to ensuring public trust in high-level Federal officials and executive branch employees. In FY 2012, auditors observed that the ethics management function at DHS is decentralized. Ethics officials in each component's Office of Counsel are delegated the authority to implement ethics program requirements in their component. The Headquarters Ethics Office did not have internal written policies and procedures to ensure required financial disclosure reports were received, reviewed, and certified within the timelines established by OGE. The auditors discovered that some employees were submitting forms late, ethics officials were not certifying them timely, and in some cases, employees did not submit the required forms.

Additionally, TSA reported that an attorney-advisor had backdated employee public financial disclosure forms provided to the auditors in the prior year so the forms appeared to comply with the OGE requirements. According to a DHS ethics official, TSA's management acted promptly to report this information and to rescind the attorney's ethics authority and to reassign the attorney, as well as his first and second line supervisors to other work. The attorney subsequently resigned from TSA on the day he was scheduled to be interviewed by TSA's Office of Inspection.

Accomplishments

Within DHS, the primary authority for investigating allegations of criminal misconduct by DHS employees lies with OIG; ICE OPR has authority to investigate those allegations involving employees of ICE and CBP. The components play a crucial, complementary role to our, as well as, ICE OPR investigative function. The components focus on preventive measures to ensure the integrity of the DHS workforce through robust pre-employment screening of applicants, including polygraph examinations at CBP; thorough background investigations of employees; and integrity and security briefings that help employees recognize corruption signs and dangers. These preventive measures are critically important in fighting corruption and work hand-in-hand with OIG's criminal investigative activities.

Congress recognized the importance of these complementary activities by enacting the *Anti-Border Corruption Act of 2010*. This Act requires CBP, by January 4, 2013, to administer applicant screening polygraph examinations to all applicants for employment in law enforcement positions prior to hiring. CBP met this goal in October 2012. The Act also requires CBP to initiate timely periodic background reinvestigations of CBP personnel. Agency statistics reveal that CBP declares 60 percent of applicants who are administered a polygraph examination unsuitable for employment because of prior drug

use or criminal histories.

It is important to emphasize that the vast majority of employees within DHS are dedicated civil servants focused on protecting the Nation. Less than one percent of employees have committed criminal acts or other egregious misconduct.

Cyber Security

Overview

Cyber security is our Nation's firewall because it is always on alert for constant threats to networks, computers, programs, and data. It contains technologies, processes, and practices that protect our systems from attack, damage, or unauthorized access.

Challenges

In FY 2012, we reviewed the Department's efforts to guide components on securing portable devices that connect to networks, as well as how several components were applying this guidance; examined threats to IT security, including those from international and insider sources; and performed the annual *Federal Information Security Management Act of 2002* (FISMA), as amended, audit for the Department to determine its compliance with the development, documentation, and implementation of a DHS-wide information security program.

Portable Device Security

In a June 2012 audit, we determined that DHS still faced challenges using portable devices to carry out its mission and increase the productivity of its employees.[36] For example, some components had not developed policies and procedures to govern the use and accountability of portable devices. Unauthorized devices were also connected to workstations at selected components. Finally, DHS had not implemented controls to mitigate the risks associated with the use of portable devices or to protect the sensitive information that these devices store and process.

Another June report showed weaknesses in the component-wide adoption of FEMA's automated property management system, reporting of lost and stolen laptops, implementation of hard drive encryption, use of a standardized laptop image, timely installation of security patches, documentation of laptop sanitization, and accounting

[36] DHS-OIG, *DHS Needs To Address Portable Device Security Risks* (OIG-12-88, June 2012).

for wireless networks.[37] These weaknesses put laptops and the sensitive information stored and processed on them at risk of exploitation.

In a May 2012 audit, we reported that USCIS' laptop controls did not sufficiently safeguard its laptops from loss or theft and did not protect the data on the laptops from disclosure.[38] Specifically, USCIS did not have an accurate and complete inventory of its laptops, and its inventory data was not reported accurately and consistently in electronic databases. Additionally, many laptops were not assigned to specific users; USCIS did not provide adequate physical security for its laptops; and not all of USCIS' laptops used the latest encryption software or operating systems and associated service packs.

International Threats

In August 2012, we reported that the NPPD Office of Cybersecurity and Communications needed to establish and implement a plan to further its international affairs program with other countries and industry to protect cyberspace and critical infrastructure.[39] For more efficient and effective operations, NPPD should streamline its international affairs functions to coordinate foreign relations better and consolidate resources. In addition, the United States Computer Emergency Readiness Team needs to strengthen its communications and information-sharing activities with and among its counterparts to promote international incident response and the sharing of best practices.

Although TSA has shown progress, it can further develop its cyber security program by implementing insider threat policies and procedures, a risk management plan, and insider threat specific training and awareness programs for all employees. TSA can also strengthen its situational awareness security posture by centrally monitoring all information systems and augmenting current controls to better detect or prevent instances of unauthorized removal or transmission of sensitive information outside of its network.[40]

Federal Information Security Management Act

Although the Department's efforts have resulted in some improvements in its security program, components are still not executing all Department's policies, procedures, and

[37] DHS-OIG, *Progress Has Been Made in Securing Laptops and Wireless Networks at FEMA* (OIG-12-93, June 2012).
[38] DHS-OIG, *U.S. Citizenship and Immigration Services' Laptop Safeguards Need Improvements* (OIG-12-83, May 2012).
[39] DHS-OIG, *DHS Can Strengthen Its International Cybersecurity Programs* (OIG-12-112, August 2012).
[40] DHS-OIG, *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain* (OIG-12-120, September 2012).

practices. DHS needs to improve its oversight of the components' implementation of its policies and procedures to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system authorizations. Other information security program areas also need improvement including configuration management, incident detection and analysis, specialized training, account and identity management, continuous monitoring, and contingency planning.

Accomplishments

DHS and its components have taken actions to govern, track, categorize, and secure portable devices in support of their missions. Specifically, DHS and some components have developed policies, procedures, and training on the use of portable devices. Additionally, some components include portable devices as part of overall accountable personal property inventory. FEMA has improved its inventory and configuration management controls to protect its laptop computers and the sensitive information it stores and processes. It has also implemented technical controls to protect the information stored on and processed by its wireless networks and devices.
Threats to, and emanating from, cyberspace are borderless and require robust engagement and strong partnerships with countries around the world. Thus, the NPPD has established multiple functions to support its international affairs program, to promote cyber security awareness and foster collaboration with other countries and organizations. To foster collaboration and develop international cyber security partnerships, NPPD and its subcomponents participate in international cyber exercises, capacity building workshops, and multilateral and bilateral engagements. The directorate also uses innovative technologies to share cyber data with its partner nations.

TSA's progress in addressing the IT insider threat is evidenced by its agency-wide Insider Threat Working Group and Insider Threat Section responsible for developing an integrated strategy and program to address insider threat risk. Further, TSA conducted insider threat vulnerability assessments that included personnel, physical, and information systems at selected airports and offsite offices, as well as reviews of privileged user accounts on TSA unclassified systems. Additionally, TSA has strengthened its Security Operations Center responsible for day-to-day protection of information systems and data that can detect and respond to insider threat incidents.

The *Federal Information Security Management Act* evaluation showed that the Department continued to improve and strengthen its security program.[41] Specifically, DHS implemented a performance plan to improve in four key areas: remediation of

[41] Title III of the *E-Government Act of 2002*, Public Law 107-347.

weaknesses in plans of action and milestones, quality of certification and accreditation, annual testing and validation, and security program oversight.

OIG Focus in 2013

In planning projects for FY 2013, we have placed particular emphasis on major management challenges, while aligning our work with DHS' missions and priorities in its *Strategic Plan for Fiscal Years 2012 Through 2016*. In addition, we will respond to legislative mandates, as well as undertake congressionally requested projects that may arise. DHS' mission is to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disaster. The Department places priority on providing essential support to national and economic security and on maturing and becoming stronger.

In the mission areas of intelligence, transportation security, border security, infrastructure protection, and disaster preparedness and response, we are planning reviews of TSA, CBP, and FEMA, among other components and directorates. In addition to projects already in progress, our upcoming work will cover various aspects of airport security and passenger screening, securing our land borders, and disaster assistance. We also have work underway and are planning to review programs at USCIS, the USCG, and ICE. In the area of accountability, we are examining or plan to examine DHS' and its component's and directorate's controls over acquisitions and critical financial systems and data, information security, privacy stewardship, management of disaster preparedness grants, and cyber security, among other mandated and discretionary reviews.

Although not all planned projects may be completed in the upcoming fiscal year, we will continue to work with DHS to enhance effectiveness and efficiency and prevent waste, fraud, and abuse.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
Management Comments to the Draft Report

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

Homeland Security

November 1, 2012

Charles K. Edwards
Acting Inspector General
Office of Inspector General
U.S. Department of Homeland Security
245 Murray Lane SW, Building 410
Washington, DC 20528

Re: OIG Draft Report: "Major Management Challenges Facing the Department of Homeland Security, Fiscal Year (FY) 2012" (Project No. 12-169-AUD-NONE)

Dear Mr. Edwards:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) perspective on the most serious management and performance challenges facing the Department. A more detailed response is provided in the Department's FY 2012 *Annual Financial Report (AFR)*.

This month marks the tenth anniversary of the creation of DHS, the largest federal reorganization since the formation of the Department of Defense. Since its inception, DHS has made significant progress becoming a more effective and integrated Department, strengthening the homeland security enterprise, and building a more secure America that is better equipped to confront the range of threats our Nation faces. As Secretary Napolitano has stated, "America is a stronger, safer, and more resilient country because of the work DHS and its many partners do every day."

The Department continues to grow and mature by strengthening and building upon existing capabilities, enhancing partnerships across all levels of government and with the private sector, and streamlining operations and increasing efficiencies within its five key mission areas: (1) preventing terrorism and enhancing security, (2) securing and managing our borders, (3) enforcing and administering our immigration laws, (4) safeguarding and securing cyberspace, and (5) ensuring resilience to disasters.

Through frameworks such as the *Quadrennial Homeland Security Review*, *Bottom-Up Review*, and *DHS Strategic Plan for FYs 2012–2016*, DHS has developed and implemented a comprehensive, strategic management approach to enhance Department-wide maturation and integration. DHS has also made significant progress to integrate and transform its management functions through the *Integrated Strategy*, first published in January 2011, which presents a clear roadmap to transform management by enhancing both vertical and horizontal integration. The strategy focuses on *all* management disciplines, especially human capital, acquisition, and financial management.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

The Under Secretary for Management has led the Department-wide effort to coalesce, or integrate, the Department's management infrastructure. The Department's strategy for the past 2 years has been to make substantial progress to implement 18 specific initiatives, each with clear action plans and performance metrics. By doing so, the degree of risk has been reduced proportionately and the Department is moving closer to a transformative state. To date, nearly 65 percent of the stated outcomes have been "mostly" or "fully" addressed and the Department is on track to meet the outcome goals for the remaining outcome metrics.

Again, thank you for the opportunity to review and comment on this draft report. This report and the Department's detailed management response to the issues identified will be included in the Department's FY 2012 AFR, as required by law. Technical comments on the draft were previously provided under separate cover for OIG consideration.

Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Report Distribution

Department of Homeland Security

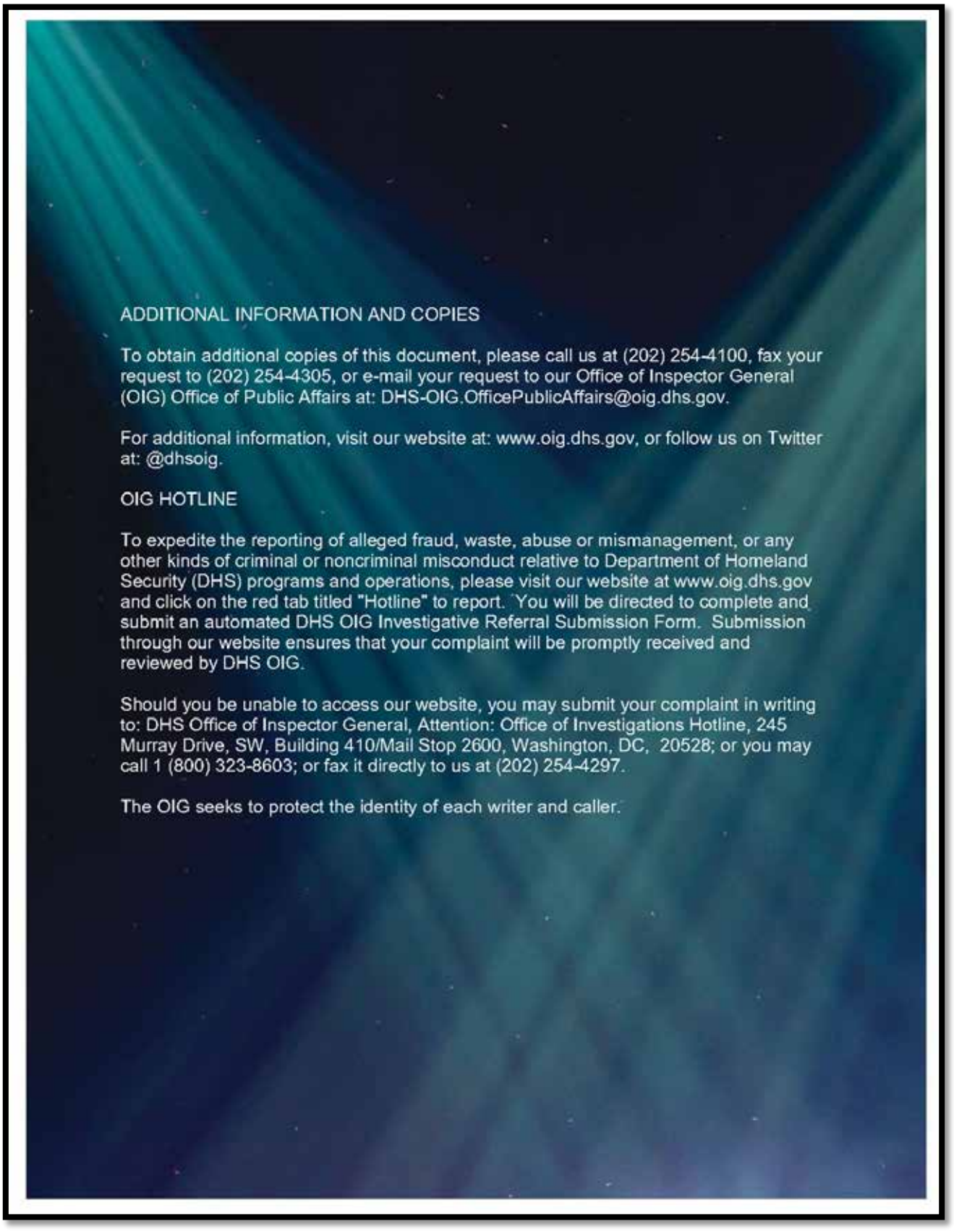
Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary Management
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Acting 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 document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.
OIG HOTLINE
To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.
Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.
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 most serious management and performance challenges facing the Department and an assessment of the Department's progress in addressing those challenges. For Fiscal Year (FY) 2012, OIG has identified the Department's major challenges in 11 broad areas, including 5 it characterized as Mission Areas and 6 as Accountability Issues:

Mission Areas

- Intelligence
- Transportation Security
- Border Security
- Infrastructure Protection
- Disaster Preparedness and Response

Accountability Issues

- Acquisition Management
- Financial Management
- IT Management
- Grants Management
- Employee Accountability and Integrity
- Cyber Security

Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners across the Federal Government, public and private sectors, and communities throughout the country have strengthened the homeland security enterprise to better mitigate and defend against dynamic threats. DHS missions include preventing terrorism and enhancing security, securing and managing our borders, enforcing and administering our immigration laws, safeguarding and securing cyberspace, and ensuring resilience to disasters.

The Department appreciates OIG's work in identifying specific areas for improvement as well as for preparing its statement on the related audits. 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 and as new initiatives begin, new management challenges can arise.

Overcoming major management challenges requires long-term strategies for ensuring stable operations as well as 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 OIG.

Challenge #1: Intelligence

DHS is focused on getting resources and information out of Washington D.C., and into the hands of state and local law enforcement to provide them with the tools to identify and combat threats in their communities. Because state and local law enforcement are often in the best position to notice the first signs of a planned attack, homeland security efforts must be integrated into the police work that they do every day, providing officers on the front lines with a clear understanding of the tactics, behaviors, and other indicators that could point to terrorist activity.

OIG's assessment focused specifically on the November 2011 review of the Office of Intelligence and Analysis's role in fusion centers. The Department appreciates OIG's acknowledgement of the progress made in providing field support to fusion centers and improving fusion center capabilities to prevent, protect against, and respond to threats.

DHS has enhanced the abilities of the National Network of Fusion Centers to:

- Receive classified and unclassified threat information from the Federal Government;
- Analyze that information in the context of their local environment in order to assess the risk posed to the local environment;
- Disseminate relevant information to local agencies to inform operational activities and resource planning; and
- Gather and assess tips, leads, and suspicious activity reporting from local agencies, and share terrorism-related reports with the Federal Bureau of Investigation-led Joint Terrorism Task Forces for further investigation.

Challenge #2: Transportation Security

The Transportation Security Administration (TSA) has created a multi-layered system of transportation security that mitigates risk and maximizes TSA's ability to stay ahead of evolving terrorist threats while protecting privacy and facilitating the flow of legitimate travel and commerce. TSA has addressed a number of OIG's concerns regarding aviation security, including those highlighted below:

Passenger and Baggage Screening
TSA holds all employees to the highest professional and ethical standards and has zero tolerance for misconduct in the workplace. Accountability is an important aspect of the Agency's work, and TSA takes prompt and appropriate action with any employee who does not follow procedures.

Although TSA concurs with OIG's recommendations regarding the evaluation of new or changed procedures and steps to improve supervision of personnel, it disagrees with the assertion that screening violations might not have occurred if TSA developed changes in screening procedures more comprehensively and fully evaluated the effects of such changes.

TSA has addressed OIG's recommendations by conducting a review of job duties, responsibilities, and competencies to update position descriptions for checked baggage supervisors and managers. In 2011, TSA established the Office of Professional Responsibility to provide greater consistency in employee misconduct penalty determinations and a more expeditious and standardized adjudication process. In 2012, TSA launched a new training course designed to help supervisors establish a leadership presence while on duty as well as technical training to support security screening measures. TSA also created an Integrated Project Team to develop best practices and tailor metrics to aid management at airports across the Nation and continues to monitor standard operating procedure compliance across the agency.

Additionally, TSA has made progress in implementing training initiatives associated with front-line supervisors and managers, such as the Essentials of Supervising Screening Operations course that includes leadership, technical, and administrative training modules specifically designed for the Supervisory Transportation Security Officer workforce. TSA has also designed a Leading People and Managing Operations course for Transportation Security Managers, which combines both leadership and technical training into one comprehensive program. TSA will continue to develop and analyze the training needs of our supervisory and management workforce to improve overall effectiveness and performance.

Airport Security

TSA is responsible for implementing a process to ensure employees working in secured airport areas are properly vetted and badged while providing oversight for the designated airport-operator employees who perform the badging application process.

DHS agrees with OIG's recommendation to refine and use one comprehensive definition of what constitutes a security breach and to develop a comprehensive oversight program to ensure accurate reporting and corrective actions take place. To address concerns regarding access control, TSA issued tools to all airports that airport operators can use to recognize fraudulent documents. TSA also offered "Airport Fraud ID Training" for all airport operators as well as briefings from Transportation Security Inspectors to augment available threat information. TSA continues to work to ensure airport operators are aware of the tools available to them, including OIG's unique algorithm tool, which may be used by airport operators to verify IDs.

In addition, the TSA Office of Compliance conducts regular briefings on fraudulent documentation and identification and will continue to discuss the issue during inspectors' monthly compliance conference calls.

Passenger Air Cargo Security

DHS agrees with OIG's assertion that improvements can be made in the air cargo screening process to prevent the introduction of explosives into air cargo on passenger aircraft. TSA has taken important steps to enhance the security of international inbound cargo on passenger and all-cargo aircraft. These include:

- Issuing new screening requirements aimed at focusing more detailed screening measures on high-risk shipments;
- Instituting working groups with air cargo stakeholders to identify ways to enhance air cargo security; and

- Initiating an Air Cargo Advance Screening pilot to more readily identify high-risk cargo for additional screening prior to aircraft departing from foreign airports to the United States.

TSA has also worked closely with its international and private-sector partners to increase the security of air cargo without restricting the movement of goods and products. By December 2012, TSA will require 100-percent physical screening of all air cargo bound for the U. S. This important step not only builds on the 100-percent screening of identified high-risk international cargo, it also incorporates TSA's risk-based, intelligence-driven procedures into the prescreening process to determine screening protocols on a per-shipment basis.

TSA continues to pursue bilateral efforts with foreign government partners through its National Cargo Security Program recognition program, which leverages foreign government supply chain security programs by allowing an air carrier to implement the security program of the country from which it is operating once TSA has determined that such programs provide a level of security commensurate with current U.S. air cargo security requirements.

Security Incident Reporting
DHS agrees with OIG's recommendation to refine its processes to better identify, track, report, and reduce breaches.

To address security vulnerabilities, TSA and the Federal Emergency Management Agency (FEMA) use the Quilt, which incorporates technology tools and best practices to facilitate management, tracking, and execution of all mitigation projects. In addition, Amtrak has updated the Transit Risk Assessment Model (TRAM), which formed the basis for the Quilt and has helped Amtrak focus its resources in a risk-based fashion. The updated TRAM, together with the DHS Top Transit Asset List and the TSA-conducted Baseline Assessment for Security Enhancement reviews of Amtrak's system, ensure that the Quilt remains the key tracking mechanism and management tool for Amtrak's security vulnerabilities.

Challenge #3: Border Security

U.S. Customs and Border Protection (CBP) screens all travelers entering the United States using a risk-based approach. Automated advance data, combined with intelligence and new biometric travel documents, facilitate travel while keeping our borders safe. CBP ensures the efficient and secure movement of cargo, using a multi-layered approach to identify risk, including enhanced screening requirements for known and established shippers.

National Protection and Programs Directorate's (NPPD's) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is working to develop a comprehensive corrective action plan to address the two recommendations from OIG. US-VISIT continues to work with domestic and international partners to provide biometric and biographic identity services. Addressing OIG recommendations, US-VISIT has reviewed the discrepant records provided by OIG, identified preliminary data filters to run against OIG's identified data inconsistencies, and assessed preliminary results. In addition, US-VISIT is developing a list of common data entries that can be identified as obviously erroneous. If US-VISIT's review of the OIG-referred data inconsistencies

identifies instances of biographic fraud, US-VISIT will refer these instances to the appropriate law enforcement entities for identity fraud resolution and possible inclusion on the biometric watchlist.

Trusted Traveler Programs

CBP's Trusted Traveler Programs provide expedited travel for pre-approved, low-risk travelers through dedicated lanes and kiosks. The Free and Secure Trade (FAST) program is a commercial clearance program for known low-risk commercial truck drivers entering the United States from Canada and Mexico. Using FAST to help manage risk enables CBP to direct more resources to high or unknown risk commerce.

OIG found that CBP's initial enrollment process for FAST generally ensures that only low-risk drivers participate in the program; however, OIG identified some vulnerabilities in the enrollment process. To address these recommendations, CBP has worked to improve processing and oversight of the carrier enrollment certification process.

Cargo Security

In late 2011, OIG conducted a review of CBP cargo security systems at bonded facilities, which are privately owned and operated buildings in which merchandise may be stored without payment of duty for up to 5 years from the date of importation. OIG encouraged CBP to implement management controls to ensure employees are properly vetted at bonded facilities.

The bonded facilities used by CBP have physical and custodial security measures in place to ensure the safety and security of the merchandise. CBP is developing a streamlined and cost-effective process to conduct background vetting of bonded facility applicants, officers, and principals. This process will add significant oversight, tracking, and reporting capabilities to the background vetting process. In addition, CBP has a layered approach to cargo security and takes a number of actions to mitigate security risks though cargo targeting and screening before the cargo arrives at a bonded facility.

Unmanned Aircraft Systems (UAS)

The UAS program provides command, control, communication, intelligence, surveillance, and reconnaissance capability to complement crewed aircraft and watercraft, and ground interdiction agents for CBP. OIG made recommendations to improve planning of the CBP UAS program, including the level of operation and resource requirements, along with addressing stakeholder needs.

CBP's Strategic Air and Marine Plan, currently under review, details operational plans and capabilities assessments, which define CBP's planned UAS acquisition and sustainment over the next 5 years and beyond. CBP continues to refine its processes for coordinating and supporting stakeholders' mission requests, working closely with DHS, the Office of Management and Budget (OMB), and Congress.

Challenge #4: Infrastructure Protection

Our Nation's critical infrastructure—both physical and cyber—enables people, goods, capital, and information to move across the country and underpins the Nation's defense, manufacturing of goods, production of energy, and overall system of commerce. Protecting our critical infrastructure and enhancing its resilience is imperative to our economic and national security.

Working with Industry

Through our work with interagency and private-sector partners, DHS has made great strides in enhancing the security of critical infrastructure. DHS has the lead in enhancing security and resilience in 11 critical infrastructure sectors, including the Dams Sector where the Department has worked with private-sector partners to develop guidance and training resources on protective measures, crisis management, and security awareness.

DHS supports the Dams Sector at the regional level, providing 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. As recommended by OIG, DHS is working with partners to assess whether regulatory authority is needed over the Dams Sector. At the same time, the Department continues to make strides under the voluntary framework, which includes DHS assessments on 100 percent of privately owned assets included on the FY 2011 Dams Sector critical assets list.

Working with Federal Partners

Under the National Infrastructure Protection Plan risk management framework, the Federal Protective Service (FPS) is the sector-specific lead agency for the government facilities sector, which includes a wide variety of critical facilities and assets owned or leased at the federal, state local, tribal, and territorial levels.

One area of significant progress related to risk assessment and the implementation of a risk management program is the ongoing implementation of FPS's solution for conducting facility security assessments using an automated assessment tool. DHS agrees with OIG's recommendation to cease development of the legacy application known as the Risk Assessment and Management Program and to pursue a standalone tool for facility security assessments. In cooperation with the National Protection and Programs Directorate, FPS has identified an interim solution to process facility security assessments by leveraging the Infrastructure Survey Tool and its host portal and environment, the Link Encrypted Network System. FPS has completed development efforts of the Modified Infrastructure Survey Tool, which was deployed in April 2012.

FPS has also taken actions to enhance coordination efforts as the sector-specific agency for the Government Facilities Sector, including establishing new relationships with the State, Local, Tribal, and Territorial Government Coordinating Council to ensure broader state and local participation in sector coordination mechanisms and engaging with the Government Facilities Sector Government Coordinating Council and the Interagency Security Committee to identify and address cross-cutting issues. Through these partnerships, FPS will develop an action plan to develop appropriate data on critical government facilities, a sector-specific risk assessment methodology, and metrics and performance data to track progress toward the sector's strategic goals.

Challenge #5: Disaster Preparedness and Response

As noted by OIG, over the past few years, FEMA has experienced a substantial increase in the number of events it responds to annually, while making significant improvements in disaster response and recovery.

Federal Disaster Declarations
Both OIG and the GAO issued reports this past year concerning the indicators used to assess governors' requests for major disaster declarations authorizing public assistance (PA) funding. When making PA disaster declaration recommendations, FEMA considers all factors in 44 CFR 206.37, including the per capita indicator as well as the estimated cost of the assistance, the available resources of state and local governments, localized impacts, insurance coverage, recent multiple disasters, hazard mitigation, and other federal assistance programs.

While it is important to note that more factors than the per capita indicator are currently considered when evaluating a governor's request for a major disaster declaration, FEMA agrees that a review of the criteria used to determine a state's response, recovery, and fiscal capabilities is warranted. In response to OIG and GAO recommendations, FEMA will conduct a review of the indicators currently used, and will assess whether the current statewide per capita indicator appropriately addresses a state's capacity to effectively respond to and recover from a major disaster. FEMA will also review potential guidance or criteria that could be used in assessing requests for an adjustment of the federal cost share to 100-percent federal funding for emergency work (PA Categories A and B) in the initial days after an incident.

FEMA is also implementing other initiatives to improve disaster budgeting and program management once a disaster declaration has been made, which will enhance FEMA's ability to manage and budget for expenditures from the Disaster Relief Fund.

Preliminary Damage Assessments and Public Assistance
In an effort to improve the quality and consistency of PA Preliminary Damage Assessments (PDA), FEMA developed the "Preliminary Damage Assessment" course to provide guidance and training on the PA PDA process. The class provides instruction on working with state and local governments to perform damage assessments, accurately document damages, formulate cost estimates, and ensure that appropriate eligibility issues are considered for the assessment of the work scope and project costs. The course is taught on a regular basis and often includes participation by state representatives.

FEMA is also pursuing data collection tools that will provide enhanced capabilities to perform PDAs and record information in an efficient and consistent manner. FEMA is currently assessing the best available options for this tool, building on previous efforts and currently available technologies. Based on the findings of the assessment, FEMA plans to develop and implement the improved PDA data collection tool in FY 2013. This will improve PDA data collection, streamline the PDA process through use of an electronic system for data collection and reporting, and enhance the effectiveness of the PDA process.

FEMA is committed to improving its services to PA applicants in Louisiana and has addressed two OIG recommendations designed to improve the PA project management process by developing

Standard Operation Procedures (SOPs) and training courses. FEMA also meets regularly to ensure continuing progress on the closeout process. FEMA has drafted an updated SOP, *Public Assistance Program Management and Grants Closeout*, which defines and standardizes the activities associated with the closeout phase, promotes consistency in delivering and monitoring the PA program, and creates a common understanding of the expectations and requirements for the assistance provided. Additionally, FEMA has implemented an incentive for rapid project closeout, as authorized under the *Post-Katrina Emergency Management Reform Act*. Under this initiative, FEMA will provide reimbursement for eligible additional direct management costs for projects that are completed by August 29, 2013.

Insurance Requirements

FEMA agrees with OIG's recommendations to improve oversight and tracking of its PA insurance requirements to ensure that all PA applicants have obtained and maintained insurance as a condition of receiving federal disaster assistance. FEMA is working with regional personnel to develop a new process designed to streamline the insurance review process and prevent duplication, while completing insurance reviews earlier in the project formulation process. Additionally, FEMA is planning to migrate data from the National Emergency Management Information System into the Emergency Management Mission Integrated Environment to create a more robust centralized source for verification of insurance information.

OIG references a proposed rulemaking that was published approximately 10 years ago as evidence that FEMA has been slow to address insurance issues. FEMA acknowledges that there are certain issues regarding insurance requirements that must be addressed through the long-term regulatory process but notes that the agency has addressed issues pertaining to insurance requirements through the issuance of guidance, including both to recipients of PA funding and to field personnel involved in the implementation of the PA Program.

Temporary Housing

OIG recommended increased FEMA oversight, reporting requirements on cost and program effectiveness, and an evaluation of administrative fees for the Disaster Housing Assistance Programs. In response to this recommendation, FEMA is currently evaluating and incorporating preliminary lessons learned from both the Alternative Housing Pilot Program and Joint Housing Solutions Group into future direct housing operations as deemed appropriate by local state-led Disaster Housing Task Forces and coordinated through the Housing Recovery Support Function of the National Disaster Recovery Framework.

Additionally, FEMA and the Department of Housing and Urban Development are developing an interagency agreement that would increase the frequency of reports and ensure the inclusion of specific program and financial data. The agreement will also contain a new administrative fee structure. FEMA will continue to assess the safety and efficient delivery of direct housing units during future disasters.

Workforce Tracking and Training

FEMA agrees with OIG that credentialing emergency providers will strengthen FEMA's ability to deliver high-quality and efficient services during disaster response. Since November 2011[1], FEMA

[1] Not reflected in the period of time in which the OIG conducted its review.

has made significant progress in implementing employee credentialing and addressing the recommendations in OIG's report. The progress has been so significant that OIG praised FEMA for their responsive actions and now considers all three recommendations resolved.

Among the improvements, the FEMA Qualification System (FQS) became operational on October 1, 2012, and has been implemented for the entire incident management workforce. FQS establishes the system for qualification and certification of the FEMA incident workforce through experience, training, and demonstrated performance. In addition, the Incident Workforce Management Office is working to address the immediate lessons learned and incorporate them into longer-term metrics that should be completed in the next 2 to 3 months.

Additionally, since the June 2012 audit, FEMA began using the Bureau of Land Management's Incident Qualifications and Certification System (IQCS). IQCS is an information system that tracks training and certifications for FQS and shares training and certification data across all involved agencies. The Reservist workforce data is currently being added to IQCS, with expected completion by December 31, 2012. Specific training on the FEMA IQCS, "Train the Trainer," is scheduled for November 2012, and additional trainings will be scheduled in each FEMA Region and Headquarters for all FEMA users.

Lastly, the budget for training and course development was approved for FY 2012 and submitted for FY 2013 and many of the courses that support the FQS have been developed and implemented. This is an ongoing process, and the Incident Workforce Management Office staff continues to coordinate with the FEMA Response Training, Exercise, and Doctrine office for further development, revision, and consolidation of coursework that supports the FQS.

Challenge #6: Acquisition Management

As noted by OIG, the Department has made significant progress in the area of acquisition management and DHS appreciates OIG's recognition of its work improving the acquisition workforce.

DHS recognizes the importance of effective acquisition management and has worked to improve program governance at both the Department and Component level. One of DHS's key changes was the establishment of a three-tiered governance model. The first part of the model is the Acquisition Review Board (ARB), which serves as the principal decision authority. The second component of the system is the Executive Steering Committee, which the ARB may establish on a case-by-case basis to provide interim oversight and guidance to select programs between Acquisition Decision Events. The third part of the governance model consists of regular portfolio reviews for groupings of programs with related missions. Each Component also conducts its own internal reviews. The tiered system provides more nimble, responsive oversight capability, enhancing vertical integration, improving program oversight, and reducing risk.

Another improvement is the establishment of the Component Acquisition Executive (CAE) structure, which creates a single program management authority within each Component. The CAE structure encourages collaboration and promotes standardization. As a result, the Department is better able to conduct oversight, share information and verify that *all* acquisition programs are

complying with Management Directive (MD) 102-01, the policy that governs program management across the Department.

In an effort to further improve the ARB and provide more empirical data for decision making, DHS implemented the Decision Support Tool (DST) and the Quarterly Program Accountability Report (QPAR). The DST provides DHS leaders, governance boards, and program managers a central dashboard for assessing and tracking major acquisition projects, programs, and portfolios, improving the acquisition process. The QPAR, a byproduct of the DST, provides DHS leadership with a high-level analysis of program health and identifies early warning signs of issues that can be rectified through increased technical support, monitoring, and training. By using these tools, DHS is better positioned to mitigate risks within acquisition management.

Components are also taking important steps to ensure efficient, effective acquisitions management. For example, after the ARB identified opportunities for improved documentation and planning for its new border security technology plan, CBP began working closely with the DHS Management Directorate to ensure all documentation followed DHS guidance and internal controls. Separately, and in response to an OIG recommendation, CBP is coordinating with the U.S. Coast Guard and other partners to develop a comprehensive assessment of commercial and/or other government-owned alternative aviation logistics and maintenance information technology (IT) systems, to further ensure efficiencies and intradepartmental collaboration where appropriate.

In response to an OIG recommendation to improve the award and oversight of U.S. Coast Guard's Ocean Sentry Maritime Patrol Aircraft and future acquisitions, U.S. Coast Guard agrees that for cost-type contract actions, it is important to give full consideration to Defense Contract Audit Agency (DCAA) audit reports, and plans to use cost analysis that use DCAA findings for any future modifications to the Ocean Sentry Maritime Patrol Aircraft (MPA) and any other contract that requires certified cost data action. U.S. Coast Guard notes, however, that not conducting a cost analysis for this particular contract award was in full compliance with the applicable regulations. In the case of the award of this MPA contract, submission of certified cost or pricing was not required or permitted under the Federal Acquisition Regulation because the Contracting Officer appropriately determined and documented that the proposed price was established in a competitive environment subject to price analysis.

In late 2011, OIG released a report regarding CBP's internal controls related to the purchase and use of steel. While DHS disagreed with OIG's overall conclusions, it recognized that the subcontract review included some deficiencies. DHS conducted an independent review of issues presented in the report, and CBP established an integrated working group to develop and communicate policies and procedures for reconciling invoices and identifying risk-based steps for processing contracts. Remaining steel not used for initial construction work is being used for maintenance and new construction work, which allows CBP to use existing infrastructure and ensure the steel is of the same quality and finish as the currently installed steel.

Challenge #7: Financial Management

DHS is committed to demonstrating the highest level of accountability, transparency, and stewardship of taxpayer dollars. In January 2011, Secretary Napolitano committed the Department

to the goal of receiving a qualified audit opinion on the Consolidated Balance Sheet and Statement of Custodial Activity. DHS met that goal. Secretary Napolitano set a goal for FY 2012 to obtain a qualified opinion on a full-scope financial statement audit. DHS met the Secretary's goal yet again.

From FY 2006–2012, 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 from FY 2011–2012 the number of Component conditions contributing to material weaknesses from 7 to 4 while expanding the audit from two financial statements to all five financial statements. Also, in FY 2012, the FY 2011 environmental liabilities qualification on the financial statements was retroactively removed.

In FY 2012, the Department obtained a qualified full-scope audit opinion on the Consolidated Balance Sheet, and the Statements of Custodial Activity, Budgetary Resources, Net Cost and Net Position. The Department is now in compliance with the *Chief Financial Officers Act of 1990* by completing a full-scope financial statement audit. In addition, DHS completed the Quadrennial Homeland Security Review, released a strategic plan, presented its net cost of operations by major mission that relate to major goals described in the strategic plan, and achieved compliance with the *Government Performance and Results Act of 1993.*

The Department was also able to provide a qualified assurance on internal control over financial reporting: our first major milestone toward obtaining an opinion on internal control.

DHS made significant progress in strengthening internal controls and implementing corrective actions within several key financial management areas. Management developed an internal controls and risk management strategy to outline material line items and an approach to ensure controls were in place to prevent and/or detect and correct material misstatements. As part of this strategy, management incorporated key objectives and risks from multiple offices within the Department as well as the Components. In FY 2012:

- The Department prepared audit readiness risk assessments from each Component identifying potential risks related to a full-scope financial statement audit;
- Components developed corrective actions to remediate deficiencies in select business process;
- Component Heads committed to correct material weaknesses, significant deficiencies, reportable conditions, or any other internal control deficiencies that could impact the Secretary's goal of obtaining an opinion on a full scope financial statement audit and to support remediation actions listed in the Mission Action Plans. These commitment statements were included as an element of each Component Head's performance plan to the Secretary;
- The Department conducted assessments over business processes impacting the first-ever audited Statements of Budgetary Resources, Net Cost, and Net Position and developed mission action plans for weaknesses identified;
- Leadership met regularly throughout the fiscal year with Components to review the status of progress against mission action plans;

The progress made in financial management at DHS over the past few years is 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 training, policies, processes, and structures to help ensure consistent operations for each of our financial accounting centers and financial management offices within DHS Components.

- The Department implemented a new training program that offered 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.
- The Department 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.
- U.S. Coast Guard remediated remaining control deficiencies related to Fund Balance with Treasury and corrected the Department's significant deficiency.
- U.S. Citizenship and Immigration Services (USCIS) substantially corrected financial reporting deficiencies reported in previous years.
- The U.S. Coast Guard made progress by correcting financial reporting control deficiencies in accounts receivable, and improving their ability to provide accurate and timely information for financial statement reporting.
- The U.S. Coast Guard was able to fully assert to the reliability of approximately $3 billion of real property balances.
- The U.S. Coast Guard continued to execute remediation efforts to address property, plant, and equipment (PP&E) process and control deficiencies.
- TSA substantially corrected PP&E control deficiencies reported in previous years.
- Management Directorate implemented new PP&E processes to correct deficiencies and has made improvements.

This progress has created momentum and further motivated DHS to reach the goal of a clean opinion on a full-scope audit in the future. The Department's Chief Financial Officer (CFO) will remain actively engaged with senior management and staff at each Component, overseeing corrective actions to ensure continued progress across the Department.

Managerial Cost Accounting

With the expansion to a full-scope audit in FY 2012, the DHS Statement of Net Cost (SNC) underwent audit for the first time. The Department focused audit readiness efforts for bringing the SNC into compliance with Federal Accounting Standards Advisory Board, *Standard SFFAS 4, Managerial Cost Accounting*, and OMB Circular A-136. A DHS Office of the Chief Financial Officer (OCFO) team researched SNC presentations from 22 other *Chief Financial Officers Act of 1990* agencies and OMB A-136 to learn and apply best practices and to develop an approach of presenting SNC by 'major missions' that are related to DHS's strategic goals. The team led representatives from all 15 reporting Components through a series of workshops and individual working sessions. They worked with each Component to establish and document cost/revenue-tracing methods and allocation methodologies for aligning costs to mission areas that would stand up to the scrutiny of the test work for the expanded scope audit.

The team partnered with DHS senior leadership to develop meaningful groupings of the seven strategic goals that effectively illustrate and communicate DHS net costs to the general public. This presentation allows the reader of the SNC to better understand how resources are spent toward the Department's common goal of a safe, secure, and resilient America.

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 DHS Components. Improving access to and the quality of financial management information is a key leadership priority at DHS. To effectively support the DHS mission, the Department has implemented the use of a group of business intelligence tools that help organize, store, and analyze data more efficiently. Through the use of business intelligence, we are beginning to provide mission-level views of resources. We can now take information from individual budgets and display them for the enterprise, providing views of how our dollars are allocated by mission area.

The Department is developing a suite of management tools, including the Decision Support Tool (DST), to assist in compiling Department-wide program cost information. The DST reached full operating capability in May 2012. The DST provides DHS leadership, governance boards, and program managers with a central, web-enabled dashboard for assessing and tracking the health of acquisition projects, programs, and portfolios. It creates graphs, charts, and other views of key indicators of program health, such as cost, funding, and schedule. The DST has proven to be an effective tool for increasing the accuracy and currency of major acquisition performance data, as well as leadership's access to that data. This has resulted in greater transparency and more informed decision making.

Antideficiency Act

In FY 2012, 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. The Department also continued to work to increase awareness of funds control across the Department and to mitigate the risk of future violations. We conducted specific training on appropriations law and how to avoid ADA violations. In FY 2012 we completed development of an online course scheduled for launch through Department and Component learning systems in FY 2013.

Financial Statements Audit

In FY 2011, the Department achieved a significant milestone by earning a qualified audit opinion on the Balance Sheet and Statement of Custodial Activity. Earning this opinion was a pivotal step to increasing transparency and accurately accounting for the Department's resources.

Building on this success, in FY 2012 the Department presented all five financial statements for audit for the first time in its history, bringing the Department into compliance with the *Chief Financial Officers Act of 1990.* Our first full-scope audit resulted in a qualified audit opinion. This opinion is a significant step toward a clean audit opinion, and evidence of our continued commitment to good governance as we strengthen and mature management processes and standards across the Department.

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

- Continue targeted risk assessments to identify and remediate material weaknesses and significant deficiency conditions in accounting and financial reporting.
- Continue to implement our plan to modernize our core financial management systems. The DHS CFO issued a *Financial Systems Modernization Playbook,* which presents the Department's plan for strengthening financial systems and business intelligence capabilities as we prioritize essential system modernization for Components with the most critical need.
- 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.
- Obtain a retroactive clean, full-scope audit opinion on FY 2012 financial statements.

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.

Challenge #8: IT Management

DHS recognizes that as security risks and technology change, the adaptability of the Department's IT Infrastructure becomes critical. As a result, DHS and its Components have worked to improve several areas of IT management, including program governance, information security, and security awareness.

For example, U.S. Citizenship and Immigration Services (USCIS) has demonstrated success in agile software development. In May 2012, the USCIS Office of Transformation launched the first release of the USCIS Electronic Immigration System and plans to push releases every 4 months. The initial release facilitates a move towards electronic systems and contains many of the foundational elements needed for all form types. It also enables Immigration Service Officers to review and adjudicate online filings from multiple agency locations across the country. Customers are provided with multiple functions, including online applications to extend or change their status for certain nonimmigrant classifications. USCIS employees are also provided with several electronic tools that support their mission, some of which include running additional background check rules and updating fraud or system check risk records. The second release, in September 2012, further enhances tools available to USCIS employees to view, access, and update records, and allows customers to submit supporting documentation.

In April 2012, OIG recognized USCIS efforts to ensure that staff in the Office of Transformation possess the necessary skills to implement the transformation program. These efforts included an emphasis on Project Management Professional certification and the scheduling and implementation of Agile and Scrum Product owner classes and workshops. As a result of these advancements, USCIS was able to address concerns from previous OIG reports.

In the area of systems availability, CBP acknowledges OIG's concern regarding an aging IT infrastructure and its effect on mission operations. CBP is conducting a comprehensive study of IT infrastructure investment priorities and has dedicated funding to replace the outmoded switches

identified by OIG by t August 31, 2013. Further, CBP is taking steps to address the problem of employees choosing to use alternative investment strategies by enforcing the Information Technology Acquisition Review (ITAR) process, identified by OIG. By increasing employee awareness of the ITAR process and identifying proposed acquisitions that are non-compliant, IT acquisitions are expected to be more timely and conform to approved technologies.

CBP also acknowledges the importance of protecting personally identifiable information (PII) and continues to make progress in minimizing its exposure. To this end, CBP has begun modernizing the TECS, which will provide access with DHS standard user names and discontinue use of Social Security Numbers as user identification. Other PII will also be masked. Moreover, CBP requires users to undergo privacy training and pass a test before gaining access to the system, which further sensitizes employees to the protections required for handling PII and encourages a culture of privacy.

DHS is conducting annual portfolio reviews to improve the IT budget review process. These reviews enable the Chief Information Officer to make recommendations to the Components in the Resource Allocation Decision process before IT investments are finalized. The Department's IT governance policies and procedures have been developed and are in the formal approval process. The policy on IT Portfolio Management addresses how IT investments are managed as portfolios, defines portfolio criteria (including selection, control, and evaluation criteria), and includes accompanying instructions that address board/council roles and responsibilities. In addition, the IT governance policies and procedures address how the Investment Review Board is to maintain responsibility for lower-level board activities, investment selection, and prioritization criteria. These improvements further support DHS's IT governance, which is addressing identified weaknesses in investment management.

Challenge #9: Grants Management

DHS has been supporting state and local efforts across the homeland security enterprise to build capabilities for the past 10 years, awarding more than $37 billion in grant funding. FEMA concurs with OIG's recommendations to strengthen management, performance, and oversight of ongoing individual state Homeland Security Grant Program projects.

As a result of improvement efforts in grants management, FEMA has met all agency-established and congressionally mandated deadlines and requirements for more than 2,700 grant awards and cooperative agreements and has issued 26 funding opportunity announcements with clear strategic objectives and priorities. Additionally, FEMA has continued to document policies, SOPs, and processes in order to ensure open competition, prevent Anti-Deficiency Act violations, and comply with congressional notification requirements. At the Headquarters level, DHS is establishing a governance body that will determine high-risk areas, develop strategies to mitigate those risks and employ standardized formats, templates, and processes to ensure consistent financial assistance activities throughout DHS. Some of these standardized templates and processes are already in place. With regards to Environmental and Historic Preservation reviews and budget reviews, FEMA will continue to refine it processes and procedures related to outstanding reviews and evaluations.

While FEMA has made significant improvements in monitoring grantees, it agrees with OIG that a more robust grants monitoring process is critical. FEMA has reduced the number of open OMB Circular A-133 audits by more than 60 percent and has overseen more than 1,200 grants in accordance with risk management strategies—focusing not only on congressional and other mandates, but also on audit findings and improper payments. FEMA has also continued to work toward ensuring that all grant funding was obligated by the grantees within the grant's original period of performance, and that those awards were accepted within 90 days and expended within 90 days of the end of the period of performance.

FEMA has developed and implemented a Grant Closeout Process SOP that has streamlined the closeout process. Through a new tracking tool that captures the status of all FEMA grants and a new 6-month pre-closeout management requirement for the early identification of grant closeout issues, FEMA had closed more than 800 grants as of September 30, 2012.

FEMA has also improved the grant reporting system and state reporting through both workforce and system changes. FEMA is currently developing and completing the build for the Non-Disaster (ND) Grant System, a project-based application and reporting system that will allow FEMA to track and measure individual project completion. The project is scheduled for completion in FY 2014 and will help to modify the grant reporting system and ensure grantees report adjustments to project milestones during the grant period of performance. System improvements also include additional training opportunities through newly implemented computer-based training, expanded external communications of emerging grant issues for stakeholders, and development and implementation of relevant standard reporting forms and formats for grant management updates.

When fully implemented, ND Grants will consolidate all of FEMA's non-disaster grant programs into one system that covers the entire grants management lifecycle. Once fully deployed, ND Grants will:

- Support the entire grants management lifecycle from application to closeout;
- Provide real-time acknowledgement of information as well as notify FEMA employees and grantees of pending actions;
- Offer integrated reporting that effectively measures award outlays and demonstrates how awards impact the overall preparedness of the Nation;
- Provide a user-friendly interface that clearly highlights pending actions to be completed;
- Automate and standardize processes to manage the entire grants management lifecycle; and
- Collect grant data in a structured, searchable format allowing data manipulation and customization for preparation, analysis, and reporting.

FEMA is also developing a curriculum for a comprehensive grantee technical assistance program that ensures that all Grants Program Directorate staff complete training requirements within 90 days of assignment or within 6 months of joining FEMA.

Strategic Management

In response to an OIG recommendation to improve strategic management guidance for State Homeland Security Grants, FEMA's National Preparedness Directorate—the group responsible for

the Homeland Security Strategy and its guidance—plans to release updated guidance on strategic planning by January 31, 2013. States will then revise their homeland security strategies to comply with the updated guidelines.

Looking forward, several of OIG's recommendations to improve the grants management process are addressed by the proposed FY 2013 National Preparedness Grants Program (NPGP). As part of the FY 2013 NPGP, FEMA will consolidate current grant programs into a comprehensive grant program (excluding Emergency Management Performance Grant (EMPG) and Assistance to Fire Fighter Grants). This consolidation will enable grantees to develop and sustain core capabilities outlined in the National Preparedness Goal (NPG) instead of requiring grantees to meet the mandates from multiple individual, often disconnected, grant programs. Consolidating grant programs will also support the recommendations of the Redundancy Elimination and Enhanced Performance for Preparedness Grants Act and streamline the grant application process. This increased efficiency will enable grantees to focus on how federal funds can add value to the jurisdiction's prioritization of threats, risks, and consequences, while contributing to national preparedness capabilities. The FY 2012 grants budget begins to prepare grantees for this transition by combining several grant programs.

Performance Measurement

FEMA GPD is actively working to better assess current preparedness capabilities and capability gaps nationwide. All states and territories that receive federal preparedness assistance are required to submit an annual State Preparedness Report (SPR) capability assessment. In 2011, FEMA redesigned the SPR assessment to account for capability targets relevant to the jurisdiction and to measure current capability levels for each of the 31 core capabilities associated with the NPG. As a result of this redesign, all grantees are required to demonstrate how proposed projects address gaps and deficiencies in core capabilities, satisfying an OIG recommendation. States and urban areas are also required to complete Threat and Hazard Identification and Risk Assessments (THIRA) by December 31, 2012. The THIRA will be used to develop capability targets for FY 2013 and beyond.

Grant funding will be focused on projects that are resolving gaps or sustaining existing capabilities identified in the state and urban area THIRAs.

FEMA has also adjusted its grant application process and the FY 2013 Investment Justification (IJ) template to include information on whether an investment is a continuation of an existing investment from a previous fiscal year. The IJ will request information about the scope and milestones of the previous investment and whether the investment is meeting its stated goals and objectives. This will allow FEMA and/or peer reviewers to evaluate the IJ and the proposed investment within the context of previous investments for the same activity.

Oversight

In an effort to improve FEMA's oversight to ensure states are meeting their reporting obligations in a timely manner, FEMA grantees will leverage the information contained within the THIRA when applying for homeland security grants. In addition, FEMA launched a long-term approach to enhance financial and programmatic monitoring within its regions. This approach implements risk management principles to direct resources to grantees and programs with the greatest need. As part of a multi-year process, FEMA has refined criteria for deciding which grants to monitor,

standardized regional financial and program monitoring activities, and expanded ongoing oversight activities to ensure early identification of issues. This approach builds upon the established monitoring approach and will continuously advance FEMA's grants management capability.

FEMA develops annual monitoring plans with individual region-specific schedules and an overview of FEMA's annual approach to monitoring grants. GPD's multi-year monitoring initiative employs a standard set of activities that can be prioritized and implemented on the basis of the grantee's or program's risk or need. The monitoring initiative also uses information that is collected through a variety of methods, including site visits, desk reviews, and regular financial and programmatic reporting by grantees.

The FY 2012 approach lays the foundation for future risk-based monitoring, which will support FEMA's and DHS's risk management philosophy. Regions and headquarters assess the monitoring needs of each grant/grantee selected for monitoring, using eight key indicators: 1) spending patterns, 2) grant dollar value, 3) grantee responsiveness, 4) Administrator's priority, 5) new FEMA grantee/grantee with new personnel, 6) number of grants managed by grantee, 7) prior financial monitoring findings, and 8) program type.

FEMA will continue working with the regions and headquarters in FY 2013 to develop a risk-based monitoring approach. Anticipated features of the FY 2013 approach include:

- Increased communication and collaboration among financial and programmatic monitoring stakeholders to identify grants and grantees in need of monitoring;
- Integrated financial and programmatic monitoring for preparedness grants managed within the Preparedness Grants Division, including a joint monitoring pilot of HSGP grants; and
- Expanded "Standard Oversight Activities."

This approach will build on the FY 2012 monitoring approach and drive FEMA toward continuously advancing its grants management capability.

GPD is also increasing the regional role in managing grant awards, which has resulted in more robust regions and an increased level of monitoring of grantees. FEMA regions are currently responsible for the EMPG, Driver's License Security Grant Program, Emergency Operations Center, Regional Catastrophic Grant Program, Metropolitan Medical Response Grants, and Citizen Corps Program awards from award to closeout. This ongoing regionalization has enabled grantees to quickly implement projects related to these awards.

Sustainment

FEMA believes it is essential that a portion of grant funding be used to sustain core capabilities through the training of personnel and lifecycle replacement of equipment. Beginning in FY 2012, in order to use grant funding to build new capabilities, grantees must ensure that the capabilities are cross jurisdictional and readily deployable, helping to elevation nationwide preparedness. All capabilities being built or sustained must have a clear linkage to one or more core capabilities in the NPG.

Challenge #10: Employee Accountability and Integrity

DHS supports OIG in its role conducting investigations of misconduct cases, including direct investigative support on such cases by ICE and CBP upon OIG request or referral.

Specifically, under the terms of a Memorandum of Understanding (MOU) between OIG and CBP, the CBP Office of Internal Affairs (IA) provides investigative support, upon request, to DHS OIG on CBP-related misconduct cases. Further, under the terms of a separate MOU between ICE and CBP, CBP IA partners with ICE Office of Professional Responsibility (OPR) to conduct investigations on CBP-related misconduct cases referred to ICE OPR by OIG.

The OIG has realized efficiencies created by cooperative investigative efforts of employee misconduct and corruption allegations. A new business model, based on the foundation established by the MOUs, has led to improved information sharing, cooperative investigations, and sharing of resources among the components. These combined efforts have helped to eliminate the case backlog and significantly accelerate the investigation of corruption allegations.

CBP's employs a comprehensive integrity strategy which includes a thorough initial screening of applicants, pre-employment polygraph examinations of law enforcement candidates, and a background investigation that commences upon the initial selection of a prospective employee. Each tool is capable of identifying vulnerabilities and in combination provides for a thorough vetting of the men and women seeking employment with, or employed by, CBP. Periodic reinvestigations of an employee's background are conducted every five years throughout an onboard employee's career and may identify emerging integrity and conduct concerns that have the potential to impact execution of the CBP mission.

CBP currently polygraphs all applicants for law enforcement positions before being hired consistent with the statutory requirements of the Anti-Border Corruption Act.

DHS views employee integrity to be crucial to ensuring that all Department operations are performed with the highest degree of ethical conduct. DHS recognizes that its ethics program plays a critical role in ensuring that employees have resources and counselors to provide them with guidance, information, and training, and to assist them in remedying potential conflicts of interest and other ethics questions. DHS agrees with the OIG that improvements in the financial disclosure process and procedures will strengthen the ethics program.

The OIG observed that DHS ethics program management is decentralized. The Department follows the requirements for management of an ethics program which are set forth in U.S. Office of Government Ethics (OGE) regulations and aligns ethics program management with the way in which legal services are delivered to component officials. The Department also agrees that increased oversight regarding the ethics program throughout DHS is warranted.

The Department's ethics program aims for 100 percent compliance with ethics regulations, including the timely filing of financial disclosure reports. For the 2012 filing season, less than one percent of the public filers (i.e., the officials holding the most senior or sensitive Department positions) filed their reports late. Those that file late incur a financial penalty that they must pay to the U.S. Treasury.

In 2012, DHS completed the second year of using an electronic financial disclosure filing system for public filers, which has significantly improved the overall management of processing the reports across DHS. The headquarters Ethics Office has implemented an improved database tracking system and expanded the information that is tracked for each filer. In addition, the headquarters Ethics Office is drafting and will issue formal procedural guidance for financial disclosure reporting across the Department and the Ethics Office is developing a process to enhance its oversight of financial disclosure reporting in the Department's components. These improvements will strengthen the ethics program and support a DHS culture of high ethical standards.

Challenge #11: Cyber Security

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

Portable Device Security
DHS agrees with OIG's recommendation to track and promote the use of portable devices in support of the Department's missions. The following are examples of the Department's commitment to mitigate security risks posed by portable devices:

- Three Components have developed specific portable device policies and procedures and aligned them with the Department's guidance.
- Five Components use an asset management system to record and track inventory of sensitive items, such as smartphones, tablet computers, and thumb drives.
- Four Components provide specific training on the acceptable use of portable devices to their users, in addition to general IT security awareness.

By engaging in these activities, Components are able to ensure that users have a full understanding of use, management, accountability, and incident response in the event that a device is lost or stolen.

Additionally, the policies governing the use of portable devices provide another layer of controls. DHS has mandated that Universal Serial Bus (USB) thumb drives are to be classified, captured, and tracked in DHS's asset management systems as sensitive personal property. The Department has also revised its asset management Equipment Control Class matrix to include USB thumb drives and provides designations on the basis of whether they meet DHS's encryption requirements. This designation helps ensure that sensitive information is placed on the appropriate storage device. The Department's property manual was also revised to include language referencing the DHS Sensitive Systems Policy, which covers USB drives.

In the laptop security audit, OIG reported that USCIS's controls did not sufficiently safeguard laptops from loss or theft, while information on these systems was not protected from disclosure. In response to OIG's recommendations, USCIS has completed the annual inventory on all personal property and is working to ensure that:

- Government-furnished equipment is appropriately addressed in contracts;
- Procedures adequately address the process to update laptops with encryption software and patches;
- Rules of behavior cover laptop protection and maintenance rules; and
- Laptop locks are issued to all laptop owners.

International Threats
OIG reviewed TSA's progress toward protecting its information systems and data from the threat posed by trusted employees. This includes insider threat management processes, the ability of selected employees to monitor and report suspicious behavior, as well as insider threat security training and awareness.

OIG found that TSA has made progress in addressing the IT insider threat and conducting vulnerability assessments, but recommended that TSA further develop its program by implementing insider threat policies and procedures for all employees.

TSA implements a risk-based strategy to address insider threat, including protective measures to detect and prevent unauthorized use of sensitive information outside TSA's network and recognizes that sensitive information can be copied or disseminated through various methods and implements physical and automated security controls to prevent inadvertent access to sensitive data. TSA has also implemented a robust program to mitigate insider cyber threats including operating a 24-hour hotline number and email address for employees and stakeholders to report possible insider cyber threat incidents. The agency has also developed policies and procedures for the establishment, integration, and implementation of the Insider Threat Program as well as specific insider cyber threat training.

The OIG also found that DHS has established policies and procedures to build upon and create new relationships to facilitate collaboration with international partners and is taking steps to strengthen operational collaboration with international counterparts to reduce cyber vulnerabilities and improve incident response and information sharing capabilities. In addition, DHS is working with the international community and industry to share its expertise and goals regarding cybersecurity.

DHS recognizes the importance of information sharing and operational collaboration at all levels and has dedicated significant resources to physical and cybersecurity international engagement. To that end, NPPD's Office of Cybersecurity & Communications (CS&C) is developing a strategic implementation plan for its international engagement with clearly defined priorities and goals. DHS continues to streamline its international affairs activities and processes to improve transparency and will examine its current internal policies and procedures related to establishing open dialogues with foreign partnerships regarding cyber threats and vulnerabilities. Finally, DHS will conduct information sharing assessments and develop operational policies and procedures subject to Federal government information sharing and privacy requirements.

Federal Information Security Management Act (FISMA)
DHS agrees with OIG's assessment that DHS needs to make improvements in several information security program areas, including incident detection and analysis, continuous monitoring, account

and identity management, and specialized training. In order to address these issues, DHS has taken several steps to align with the Administration's cybersecurity priorities, including:

- Implementation of trusted Internet connections;
- Continuously monitoring the Department's information systems;
- Employing personal identity verification compliant credentials to improve logical access for its systems; and
- Updating the DHS Information Security Performance Plan with enhanced metrics.

In the area of FISMA compliance, DHS continued to improve and strengthen its information security program during FY 2012. For example, the Chief Information Security Officer:

- Developed the *FY 2012 DHS Information Security Performance Plan* to enhance DHS's information security program and improve existing processes, such as continuous monitoring, Plans of Action and Milestones, and security authorization.
- Updated the Department's governing IT security policies and procedures in both the *DHS Sensitive Systems Policy Directive 4300A* and its companion, *DHS 4300A Sensitive Systems Handbook*, to reflect the changes made in DHS security policies and various National Institute of Standards and Technology guidance.
- Issued the second *State of Cybersecurity at The Department of Homeland Security* report outlining how DHS anticipates and addresses emerging security risks from new technology products and advanced threat actor techniques, including its new initiatives and programs that ensure a secure computing environment within the Department. The report presents relevant information to employees for protecting their information and increasing the Department's cybersecurity awareness.

Concluding Comment

The Department concurs with OIG's assessment that:

> …DHS has made progress in coalescing into a more cohesive organization to address its key mission areas to secure our Nation's borders, increase our readiness, capacity, 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.

The Department appreciates OIG's perspective on the most serious management and performance challenges facing the Department as well as recognition of the significant progress and substantial accomplishments DHS has made to date.

Acronym List

Acronyms

ADA – Anti-Deficiency Act
AFG – Assistance to Firefighters Grants
AFR – Annual Financial Report
ARB – Acquisition Review Board
ARRA – American Recovery and Reinvestment Act
ATA – American Trucking Association
BP – British Petroleum
BPD – Bureau of Public Debt
BUR – Bottom-Up Review
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAE – Component Acquisition Executive
CBP – U.S. Customs and Border Protection
CBRN – Chemical, Biological, Radiological, and Nuclear
CDL – Community Disaster Loan
CDP – Center for Domestic Preparedness
CFO – Chief Financial Officer
CFR – Code of Federal Regulations
CIO – Chief Information Officer
CISO – Chief Information Security Officer
CMAS – Commercial Mobile Alert Service
COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985
COR – Contracting Officer Representative
COTR – Contract Officer's Technical Representative
COTS – Commercial Off-the-Shelf
CSO – Chief Security Officer
CSRS – Civil Service Retirement System
CY – Current Year
DADLP – Disaster Assistance Direct Loan Program
DC – District of Columbia
DCAA – Defense Contract Audit Agency
DHS – Department of Homeland Security
DHS FAA – Department of Homeland Security Financial Accountability Act
DIEMS – Date of Initial Entry into Military Service
DNDO – Domestic Nuclear Detection Office
DOC – U.S. Department of Commerce
DOD – U.S. Department of Defense
DOJ – U.S. Department of Justice
DOL – U.S. Department of Labor
DST – Decision Support Tool (DST)
EDS – Explosive Detection System
EFSP – Emergency Food and Shelter Program
ELIS – Electronic Immigration Application System
EMI – Emergency Management Institute
EMPG – Emergency Management Performance Grant Program
ERO – Enforcement and Removal Operations
FAA – Department of Homeland Security Financial Accountability Act
FAST – Free and Secure Trade Program
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
FLETA – Federal Law Enforcement Training Accreditation
FLETC – Federal Law Enforcement Training Center
FMD – Foot-and-Mouth Disease
FMFIA – Federal Managers' Financial Integrity Act

FOSC – Federal On-scene Coordinators
FPS – Federal Protective Service
FQS – FEMA Qualification System
FY – Fiscal Year
GAAP – Generally Accepted Accounting Principles
GAO – U.S. Government Accountability Office
GCCF – Gulf Coast Claims Facility
GPD – Grant Programs Directorate
GSA – General Services Administration
HSA – Homeland Security Act of 2002
HSAM – Homeland Security Acquisition Manual
HSGP – Homeland Security Grant Program
HSPD – Homeland Security Presidential Directive
HS-STEM – Homeland Security Science, Technology, Engineering and Mathematics
IA – Internal Affairs
I&A – Office of Intelligence and Analysis
ICCB – Internal Control Coordination Board
ICE – U.S. Immigration and Customs Enforcement
ICS-CERT – Industrial Control Systems Cyber Emergency Response Team
IEFA – Immigration Examination Fee Account
IHP – Individuals and Household Programs
IJ – Investment Justification
INA – Immigration Nationality Act
IP – Improper Payment
IPERA – Improper Payments Elimination and Recovery Act
IPIA – Improper Payments Information Act of 2002
IQCS – Incident Qualifications and Certification System
IT – Information Technology
ITAR – Information Technology Acquisition Review
LOI – Letters of Intent
LOR – Local Recipient Organization
MD – Management Directive
MD&A – Management's Discussion and Analysis
MERHCF – Medicare-Eligible Retiree Health Care Fund
MGMT – Management Directorate
MHS – Military Health System
MOU – Memorandum of Understanding
MPA – Maritime Patrol Aircraft
MRS – Military Retirement System
MSA – Marshal Service Agreements
MTS – Metric Tracking System
NATO – North Atlantic Treaty Organization
ND – Non-Disaster
NFIP – National Flood Insurance Program
NPFC – National Pollution Funds Center
NPG – National Preparedness Goal
NPGP – National Preparedness Grants Program
NPPD – National Protection and Programs Directorate
NPR – National Preparedness Report
NSSE – National Security Special Event
OCFO – Office of the Chief Financial Officer
OCHCO – Office of the Chief Human Capital Officer
OCIO – Office of the Chief Information Officer
OHA – Office of Health Affairs
OIG – Office of Inspector General
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
OPR – Office of Professional Responsibility
OPS – Office of Operations Coordination and Planning
ORB – Other Retirement Benefits
OSLTF – Oil Spill Liability Trust Fund
OTA – Other Transaction Agreements

OTIA – Office of Technology Innovation and Acquisition
PA – Public Assistance
PARM – Program Accountability and Risk Management Office
PCS – Permanent Change of Station
PDA – Preliminary Damage Assessments
PII – Personally Identifiable Information
POE – Port of Entry
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
QPAR – Quarterly Program Accountability Report
RAMP – Risk Assessment and Management Program
RSSI – Required Supplementary Stewardship Information
SAT – Senior Assessment Team
SBR – Statement of Budgetary Resources
SCDL – Special Community Disaster Loan
SFFAS – Statement of Federal Financial Accounting Standards
SFRBTF – Sport Fish Restoration Boating Trust Fund
SMC – Senior Management Council
SNC – Statement of Net Cost
SOP – Standard Operation Procedure
SPR – State Preparedness Report
S&T – Science and Technology Directorate
TAFS – Treasury Account Fund Symbol
THIRA – Threat and Hazard Identification and Risk Assessments
TRAM – Transit Risk Assessment Model
Treasury – U.S. Department of the Treasury
TSA – Transportation Security Administration
TSGP – Transit Security Grants Program
U.S. – United States
USB – Universal Serial Bus
U.S.C. – United States Code
USCG – U.S. Coast Guard
USCIS – U. S. Citizenship and Immigration Services
USSS – U.S. Secret Service
US-VISIT – United States Visitor and Immigrant Status Indicator Technology
VA – U.S. Department of Veterans Affairs
WYO – Write Your Own

Homeland
Security

Homeland
Security