Other Accompanying Information

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

Tax Burden/Tax Gap

Revenue Gap

The Compliance Measurement Program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations and agreements, and is used to estimate the revenue gap.

The revenue gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and agreements using a statistically valid sample of the revenue losses and overpayments detected during Compliance Measurement entry summary reviews conducted throughout the year.

For FY 2007 and 2006, the estimated revenue gap was $412 and $450 million, respectively. The preliminary estimated revenue gap for FY 2008 is $347 million. The preliminary estimated over-collection and under-collection amounts due to noncompliance for FY 2008 were $70 and $417 million, respectively. The preliminary estimated over-collection and under-collection amounts due to noncompliance for FY 2007 were $90 and $502 million, respectively. The preliminary overall trade compliance rate for FY 2008 and FY 2007 is 98 and 98.1 percent respectively. With overall compliance at a high level, CBP has been able to emphasize matters of significant trade risk.

The final overall trade compliance rate and estimated revenue gap for FY 2008 will be issued in February 2009.

Summary of Financial Statement Audit and Management Assurances

Table 8 and Table 9 below provide a summary of the financial statement audit and management assurances for FY 2008.

Table 8. FY 2008 Summary of the Financial Statement Audit

Audit Opinion	Disclaimer				
Restatement	Yes				
Material Weakness	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
Financial Management and Entity-Level Controls	1		✓		0
Financial Reporting	1	✓	✓		1
Financial Systems Security	1				1
Fund Balance with Treasury	1				1
Capital Assets and Supplies	1	✓	✓		1
Actuarial and Other Liabilities	1	✓	✓		1
Budgetary Accounting	1	✓	✓		1
Total Material Weaknesses	**7**	**4**	**(5)**	**0**	**6**

The Department's Independent Public Auditor reported six material weakness conditions at the Department level in FY 2008, a reduction from the seven reported in FY 2007. This improvement reflects a decrease in the severity of Financial Management and Entity-Level Control conditions at U.S. Coast Guard and FEMA from a material weakness in FY 2007 to a significant deficiency in FY 2008. Portions of other material weakness conditions were resolved. However, new conditions were identified causing the other material weaknesses to repeat at the consolidated level. For example, the DHS OCFO resolved its Financial Reporting material weakness conditions but TSA's prior year significant deficiency in Financial Reporting was elevated to a material weakness condition. Similarly, FEMA resolved its prior year material weakness conditions for Capital Assets and Supplies related to stockpile inventory but a new material weakness condition associated with internal use software was identified at FEMA and TSA. FEMA also resolved its Other Liabilities material weakness conditions related to grant accruals but new significant deficiencies were identified related to environmental liabilities at ICE, FLETC, and S&T. As a result, the Actuarial and Other Liabilities material weakness repeated. Finally, FEMA and TSA resolved prior year conditions for Budgetary Accounting. However, new conditions were identified with undelivered orders at FEMA causing this material weakness to repeat.

Table 9. FY 2008 Summary of Management Assurances

Effectiveness of Internal Control Over Financial Reporting (FMFIA Section 2)						
Statement of Assurance	No Assurance					
Material Weaknesses	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Entity Level Controls	1		✓			0
General Ledger Management: Including Financial Reporting and Intragovernmental Reconciliations	1	✓	✓			1
Fund Balances with Treasury	1					1
Financial Systems Security	1					1
Budgetary Resource Management	1	✓	✓			1
Property Management	1	✓	✓			1
Grants Management	1				✓	0
Insurance Management	1				✓	0
Human Resource and Management	1					1
Total Material Weaknesses	**9**	**3**	**(4)**	**0**	**(2)**	**6**

Effectiveness of Internal Controls over Operations (FMFIA Section 2)						
Statement of Assurance	Qualified					
Material Weaknesses	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Entity Level Controls	1					1
Improper Payments Information Act	1					1
Anti-Deficiency Act Controls	1					1
Security Controls over Collection and Depositing of Fees	1					1
Federal Protective Service Transformation	1					1
DHS Headquarters Consolidation	1				✓	0
Acquisition Management	1					1
Human Capital Management	1					1
Information Technology Management	1				✓	0
Long Term Strategic Planning and Outcome Based Management	1				✓	0
Grants Management	0	✓				1
Administrative Management	0	✓				1
US-VISIT System Security	0	✓				1
Total Material Weaknesses	**10**	**3**	**0**	**0**	**(3)**	**10**

Conformance with financial management systems requirements (FMFIA Section 4)						
Statement of Assurance	Systems do not conform to financial management systems requirements					
Non-Conformances	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Federal Financial Management Systems Requirements, including Financial Systems Security and Integrated Financial Management Systems	1					1
Noncompliance with the U.S. Standard General Ledger	1					1
Federal Accounting Standards	1					1
Total Non-conformances	**3**	**0**	**0**	**0**	**0**	**3**

Compliance with Federal Financial Management Improvement Act (FFMIA)	DHS	Auditor
Overall Susbstantial Compliance	No	No
1. System Requirements	No	
2. Accounting Standards	No	
3. USSGL at Transaction Level	No	

Effectiveness of Internal Control Over Financial Reporting

Pursuant to the DHS FAA, the Department focused its efforts on corrective actions to design and implement Department-wide internal controls. Although the Secretary made no assertion about the operating effectiveness of internal controls over financial reporting, a qualified assurance on the design effectiveness was provided to appropriately represent the status of DHS's corrective action efforts and to facilitate implementation of the Act's audit opinion requirement.

The Secretary reported six material weakness conditions at the Department level in FY 2008, which is reduced from nine reported in FY 2007. Most significantly, the U.S. Coast Guard and FEMA implemented corrective actions to reduce the severity of the prior year Entity-Level Control material weaknesses to reportable conditions. Management concurred with the material weakness conditions reported by independent audit. Additions and deletions to beginning balances are consistent with the summary of financial statement audit results described above. Grants Management was reassessed and reported as an internal control over operations material weakness condition. In addition, Insurance Management at FEMA was reassessed and was considered a supporting condition of Financial Reporting at FEMA as opposed to a stand alone material weakness condition. Differences between condition titles reported by DHS Management and the Independent Public Auditor (IPA) are due to the Department's grouping of material weakness conditions by financial management processes as defined by the General Services Administration's Financial Systems Integration Office (FSIO). The FSIO process definitions used by management aid corrective actions and facilitate development of standard controls and business processes.

Significant internal control challenges remain at U.S. Coast Guard, FEMA, and TSA. To support these Components, the Department's Chief Financial Officer will conduct monthly corrective action meetings with Senior Management and weekly working group meetings with Senior Staff. Table 10 below summarizes material weaknesses in internal controls as well as planned corrective actions with estimated target correction dates.

Table 10. FY 2008 Internal Controls Corrective Actions

Material Weaknesses in Internal Controls Over Financial Reporting	Year Identified	DHS Component	Corrective Actions	Target Correction Date
Financial Reporting: U.S. Coast Guard, TSA, and FEMA have not established an effective financial reporting process due to limited staffing resources, informal policies and procedures, and lack of integrated financial processes and systems.	FY 2003	U.S. Coast Guard, TSA, and FEMA	The DHS OCFO corrected prior year financial reporting conditions and will continue efforts to support U.S. Coast Guard, TSA, and FEMA in implementing corrective actions to address staffing shortfalls and develop policies and procedures to establish effective financial reporting control activities.	FY 2010
Financial Systems Information Technology (IT) Controls: The Department's Independent Public Auditor had identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to a myriad of inherited control deficiencies surrounding general computer and application controls. The *Federal Information Security Management Act* mandates that Federal Agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance.	FY 2003	U.S. Coast Guard, TSA, and FEMA	Prior year Department-wide IT control findings were reduced by 40 percent. Additional financial audit support for U.S. Coast Guard, FEMA, and TSA will be provided from the Offices of the Chief Financial Officer and the Chief Information Security Officer in order to design and implement internal controls in accordance with *DHS 4300A Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Financial Systems.*	FY 2010
Fund Balance with Treasury: U.S. Coast Guard did not implement effective internal controls to accurately clear suspense transactions in order to perform accurate and timely reconciliations of Fund Balance with Treasury accounts.	FY 2004	U.S. Coast Guard	U.S. Coast Guard will develop short term compensating controls to reconcile significant payroll classes of transactions, while longer term corrective actions are implemented to sustain Fund Balance with Treasury Reconciliations.	FY 2010
Capital Assets and Supplies: The controls and related processes surrounding U.S. Coast Guard Property Plant and Equipment (PPE) and Operating Materials and Supplies (OMS) to accurately and consistently record activity are either not in place or contain errors and omissions. FEMA and TSA have not implemented policies and procedures to identify and account for software capitalization in accordance with Statement of Federal Financial Accounting Standard (SFFAS) No. 10, *Accounting for Internal Use Software* .	FY 2003	U.S. Coast Guard, TSA, and FEMA	FEMA implemented corrective actions to address the prior year material weakness condition related to stockpile inventory. U.S. Coast Guard will implement policies and procedures to support completeness, existence, and valuation assertions for PPE and OMS. In addition, acquisition, construction, improvement, and construction in progress controls will be implemented to properly capitalize PPE. FEMA and TSA will develop policies and procedures to account for software capitalization in accordance with SFFAS No. 10.	FY 2010
Actuarial Liabilities and Other Liabilities: U.S. Coast Guard has not implemented policies and procedures to account for actuarial liabilities. In addition, internal control weaknesses exist in developing estimates for accounts payable and environmental liabilities at U.S. Coast Guard. New significant deficiencies were identified related to environmental liabilities at ICE, FLETC, and S&T, which contributed to repeating the Actuarial and Other Liabilities material weakness.	FY 2006	U.S. Coast Guard	TSA implemented corrective actions to address the prior year material weakness condition related to unfunded employee leave. In addition, FEMA reduced the severity of its prior year grant accrual material weakness condition. U.S. Coast Guard will implement corrective actions to support financial assertions for the Actuarial Pension Liability associated with unfunded military retirement pay by improving data quality and establishing controls at servicing personnel offices. The DHS OCFO will support U.S. Coast Guard, ICE, FLETC, and S&T in developing a cross cutting corrective action plan for environmental liabilities.	FY 2010
Budgetary Accounting: Policies and procedures over obligations, disbursements, and validation and verification of undelivered orders for accurate recording of accounts payable were not effective.	FY 2004	U.S. Coast Guard and FEMA	TSA corrected its portion of the prior year budgetary accounting material weakness. In addition, FEMA implemented corrective actions to improve the deobligation of mission assignments, however new corrective actions will need to be developed for other FEMA undelivered orders. U.S. Coast Guard developed corrective actions to improve budgetary accounting however corrective actions may extend beyond FY 2010 due to resource constraints and magnitude of other corrective actions.	FY 2010

Effectiveness of Internal Control Over Operations

The DHS Management Directorate is dedicated to ensuring that Departmental Offices and Components perform as an integrated and cohesive organization, focused on leading the national effort to secure America. Critical to this mission is a strong internal control structure. As we strengthen and unify DHS operations and management, we will continually assess and evaluate

internal control to evaluate our progress in ensuring the effectiveness and efficiency of operations and compliance with laws and regulations. For the second consecutive year, we have made tremendous progress in strengthening Department wide internal controls, as evidenced by the following FY 2008 achievements:

- Reinvigorated the Department's Senior Management Council to establish mechanisms to provide corrective action governance and oversight.
- Finalized the Department's Strategic Plan and strengthened performance management.
- Established a Departmental acquisition oversight function and conducted reviews of five Level One Programs with an aggregate value of $26 billion.
- Successfully migrated fifty-one application systems to the first enterprise data center and took delivery of 10,000 square feet of raised floor at a second data center. There are thirty-nine migration projects for both centers now in progress.
- Implemented a standard E-mail system (Microsoft Exchange) across the enterprise and established a unified address list for the entire Department, improving departmental communications.
- Implemented web based shipping procedures to drive operational efficiencies and improvements.
- Updated the DHS Headquarters Continuity of Operations Plan with new operational concepts and operational procedures for the Department to better respond internally to continuity of operations events.
- Led a complete Mission Essential Function and Primary Mission Essential Function analysis for the Department in support of Homeland Security Presidential Directive (HSPD) 20 implementation.
- Implemented HSPD-12 to strengthen security employee identification and the State and Local Field Coordinator Program; conducted six security compliance reviews; continued the Defensive Counterintelligence Program in conjunction with the Office of Intelligence and Analysis; and trained more than 10,000 DHS employees in security awareness issues.
- Addressed strategic human capital priorities through the development of the FY 09-13 DHS Human Capital Strategic Plan and implemented the DHS University System as defined by the Learning and Development Strategic Plan; established the DHS Diversity Strategy and Council; and launched action plans to address concerns raised in the Annual Employee Surveys.

For the first time, Mission Action Plans were prepared for internal control over operations. During the year, responsible officials briefed the DHS Senior Management Council on the status of corrective actions for material weaknesses identified in their component heads annual assurance statement to the Secretary. Corrective actions were completed at TSA and USCIS as described below:

- TSA Personnel Data Security was identified in May 2007 when a portable storage device containing sensitive personnel data on TSA employees was reported missing. Immediate action was taken to remedy the known deficiency and all corrective actions have been completed to prevent future recurrences.
- USCIS IT Management: Internal control assessments in FY 2007 by USCIS' Office of Information Technology disclosed serious internal control weaknesses. Corrective actions to be completed, starting in FY 2006, were captured in the Mission Action Plan. Critical actions to remedy this issue were completed this fiscal year, including assessing the

qualifications of IT staff and updating training requirements, position descriptions and performance work plans.

For the following two Mission Action Plans, all corrective actions were completed. However, additional reviews and/or an expansion of the scope of the challenge will require DHS Components to develop re-baselined Mission Action Plans for FY 2009 with new milestones.

- CBP Laptop Security: All the milestones identified in the FY 2008 Mission Action Plan were completed, including reviewing documentation on disposing laptops to assure offices are complying with guidance for disposals, performing semi-annual inventories of laptops, and conducting two site visits per month to perform laptop reviews. New controls and training have been implemented; and while significant progress has been made, additional controls and monitoring are still required given the number of laptops at CBP. Therefore, CBP will have a FY 2009 Mission Action Plan on Laptop Security, with corrective actions and milestones.
- USCIS Security of Controls over Collection and Depositing Fees: All the actions identified in the Mission Action Plan to resolve the reported Material Weakness were completed. These included steps to correct deficiencies identified at USCIS' Texas Service Center. USCIS' ultimate solution is to transition the processing of applications and fees to a lockbox environment. Steps to complete the transition to a lockbox environment are still in process. During FY 2008, USCIS assessed the application and fee collection processes at the California and Nebraska Service Centers and identified weaknesses. This assessment completed USCIS' internal control testing of application and fee collection processes for all four of its Service Centers. Consequently, while the actions identified in the FY 2008 Mission Action Plan pertaining to the security over the front log of applications and fees and the deposit of fees within Department of Treasury guidelines were completed, USCIS is developing a new Mission Action Plan in the area of general security over applications and fees for all USCIS Service Centers for FY 2009, with new milestones identified, to address new findings.

Work continues for the following Mission Action Plans, which have, or will have, milestones extending beyond FY 2008:

- Human Capital Management: The Human Capital Management Mission Action Plan was based on the FY 2007-2008 Human Capital Operational Plan, which identified short-term initiatives that supported the long-term outcomes of integrating programs for hiring, retention, training and development, and performance. Half of the critical milestones targeted for completion by the end of this fiscal year were completed, including deploying e-Recruitment at Headquarters, providing standards and model for the nine mandatory training activities, and meeting FY 2008 hiring targets. During FY 2008, the Office of the Chief Human Capital Officer (OCHCO) experienced a significant backlog in staffing actions that impacted DHS Headquarter organizations. This backlog arose due to a significant increase (surge) in staffing actions for NPPD and human capital contractor services transitioning from one provider to another during the NPPD surge. Corrective actions were taken, resulting in a full elimination of the backlog. OCHCO has developed a new strategic plan, and the implementation of this new strategic plan will be the basis for an updated Human Capital Management Mission Action Plan beginning in FY 2009.

- Acquisition Management: One of the three critical milestones identified for completion this year was accomplished. The Office of the Chief Procurement Officer briefed the Acting Deputy Secretary on the results of Program Quick Looks to examine the current status and priority of major programs. The second milestone, which was not completed, involved modifying Management Directive 0003 to provide DHS-wide coverage and expanding contracting to acquisition. USSS has not agreed to the modification eliminating their exemption from Headquarters oversight. The third milestone to update Management Directive 1400, Investment Review Process, is near completion. The document has been drafted into a more comprehensive directive (102-01) and will be implemented by November 2008.
- CBP Secure Border Initiative Acquisition: Correcting weaknesses identified in the Secure Border Initiative's acquisition organization and processes is a long-term process, as reflected in the Mission Action Plan's target completion date of September 30, 2009. Only three of ten critical milestones were targeted for completion by the end of this fiscal year. Two milestones were completed: 1) Creating a SBI Acquisition Office (completed in FY 2007); and 2) Establishing Executive Level SBI Governance Structure within CBP (completed in FY 2008). One critical milestone, to develop and implement a process for program and milestone review and approvals within Secure Border Initiative and CBP was targeted for completion in FY 2008 and is in progress, but not yet completed. Reviews have been conducted since early summer, but the policy and procedures that formally document the process have not yet been completed. For the remaining critical milestones, work is planned or in progress.
- U.S. Coast Guard Deepwater Acquisition: Substantial progress has been made to address internal control deficiencies in the Deepwater acquisition program and work continues to implement controls and monitor compliance in areas of acquisition, design, delivery, program management, contractor accountability, human capital, and cost control. Of 102 identified critical milestones, 67 percent have been completed. The target completion date for this Mission Action Plan is July 1, 2009.
- Federal Protective Service (FPS) Transformation: All of the 45 milestones identified in the FPS Transformation Mission Action Plan were targeted for completion by October 1, 2008. Of these, 17 milestones were completed. While significant progress has been made, FPS still does not have the optimal number of resources to fully execute its financial management and budget functions while implementing all of the necessary internal controls. During FY 2008, FPS made significant efforts to meet the goals and objectives included in their Mission Action Plan by undergoing key transformations while it worked to execute its DHS mission with the right resources as proposed in the President's FY 2009 budget. Ongoing FPS efforts are focused on ensuring that FPS operations are effective and efficient, the organization is meeting its mandate and customer requirements, and that it has the right people in the right positions.
- FEMA Improper Payments Information Act: While FEMA continues to be non-compliant with IPIA, substantial progress was made in completing the critical milestones identified in FEMA's Mission Action Plan. Most of the milestones related to two programs, the Individuals and Households Program and the Disaster Relief Program Vendor Payments. Of the 13 critical milestones that were not completed, one milestone was to conduct statistically valid testing to estimate improper payments for all FEMA high-risk programs, and another was to conduct a recovery audit of contract payments. Both tasks are key components of a successful IPIA program. To address the former, a test pilot was conducted this year,

enabling FEMA to develop methodologies to sample test four high-risk grant programs and the National Flood Insurance Program in the future.

Federal Financial Management Improvement Act

The Federal Financial Management Improvement Act of 1996 (FFMIA) requires Federal agencies to implement and maintain financial management systems that comply substantially with:

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

In assessing compliance with FFMIA, DHS utilizes OMB guidance and considers the results of the OIG, annual financial statement audits, and Federal Information Security Management Act (FISMA) compliance reviews. As reported in the Secretary's Management Assurance Statements, DHS financial management systems do not substantially conform to government-wide requirements. However, significant consolidation efforts are in progress to modernize, certify, and accredit all financial management systems.

Financial Management Systems Framework

The President's Management Agenda: The President's Management Agenda (PMA) specifies that a clean financial audit and timely, useful, and reliable financial information are critical to improving financial and budget management performance government-wide. In support of these PMA objectives, the DHS Office of the Chief Financial Officer (OCFO) has undertaken a Department-wide initiative to consolidate 13 disparate baselines. A top priority for the OCFO, this initiative is part of the strategic DHS financial management framework that addresses a full range of issues in the areas of people, policy, process, systems, and assurance to achieve the goals of the PMA and the Department.

Financial Management Systems Strategy and Vision: Transformation and Systems Consolidation (TASC) is an effort to consolidate financial management systems across DHS with a focus on standardizing and centralizing business processes, moving to a single OMB-compliant accounting line, facilitating clean audit opinions and yielding timely and accurate financial data. On March 17, 2008, the U.S. Court of Federal Claims issued a ruling adverse to the Department. The revised TASC acquisition strategy is moving forward under a full-and-open competition to include a broader range of technology solutions already existing in the federal space. A Request for Information (RFI) was released to industry in May 2008. Twenty industry responses were received and 10 meetings conducted between industry and DHS headquarters/component representatives. A draft RFP was released in October 2008. The award date is approximated for quarter two 2009.

The Under Secretary for Management, Chief Financial Officer, Chief Information Officer, Chief Procurement Officer, and the Chief Administrative Officer are unified in achieving efficiencies in business processes and in the systems used throughout DHS.

Benefits and Compliance: The TASC initiative facilitates compliance with applicable Federal laws and regulations and satisfies the requirements of the PMA for improving financial and budget management government-wide by:

- Supporting an OMB-compliant accounting line to provide DHS decision makers with more accurate, timely, and reliable reporting;
- Strengthening Department-wide financial accountability, moving DHS closer to a sustainable clean audit opinion;
- Providing the foundation for effective internal controls and segregation of duties supported by a compliant software baseline;
- Removing manual processes and strengthening internal controls;
- Utilizing real-time interoperability to streamline reporting across the financial management enterprise;
- Supporting an approved Chart of Accounts compliant with the United States Standard General Ledger (USSGL) and OMB Circular A-127;
- Ensuring compliance with the National Institute of Standards and Technology Special Publication 800-53 – Recommended Security Controls for Federal Information Systems and the GAO's Federal Information System Controls Audit Manual;
- Achieving Financial Management Line of Business compliance by standardizing data collection and transaction processes throughout the organization; and
- Providing optimal mission support through efficient finance, procurement, and asset management operations and business processes.

Federal Information Security Management Act (FISMA)

The E-Government Act of 2002 (Public Law 107-347) Title III FISMA provides a framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. FISMA provides a statutory definition for information security.

The U.S. Department of Homeland Security *2008 Federal Information Security Management Act (FISMA) Report and Privacy Management Report* consolidated reports from three DHS offices:

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

In FY 2008, the Department continued to implement improvements to the DHS information system security program, and the CIO documented improvements in the following areas of FISMA:

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

FISMA Department Oversight - Policy and Procedures

A number of policy updates to the DHS Sensitive Systems Policy (DHS 4300A) were issued over the past year and are published on the DHS intranet Web site at the CISO home page.

The Department uses two enterprise tools for facilitating agency-wide security management and compliance tracking against DHS policies and procedures, and a number of procedural updates were provided during the course of the year. These tools serve as the basis for generating monthly FISMA scorecards to the Components that track six compliance metrics for both classified and unclassified systems. The six compliance metrics include:

- Annual testing (system tests and evaluations and annual self-assessments);
- Plans of action and milestones (POA&Ms);
- Certifications and accreditation (C&A);
- Configuration management;
- Incident reporting; and
- Information security training.

The latest DHS 4300A Version 6.1, dated September 23, 2008, includes security control tests and reporting requirements for CFO-designated financial systems that must be performed annually. These controls and requirements were based on OMB Circular A-123, and grouped into the following control domains:

- Entity-wide security program planning and management;
- Access controls;
- Application software development and change control;
- System software;
- Service continuity; and
- Segregation of duties.

Information System Inventory

In FY 2008, DHS maintained a single inventory of its sensitive but unclassified general support systems and major applications, including contractor owned and operated systems, as illustrated below. The DHS inventory remains under strict change control processes and all additions, deletions, or changes to the Component's inventory are tracked by the Department to ensure completeness. The Department identified 591 information systems in FY 2008, as shown in the table below.

Table 11. DHS FY 2006 - 2008 System Inventory Breakdown

Type of System	FY 2006	FY 2007	FY 2008
DHS-Owned Systems	486	396	376
Contractor Owned/Operated	206	207	215
Total	692	603	591

In addition, the Department conducts site visits at Components to identify systems that were not included in the annual inventory update process.

The FY 2009 DHS Information Security Performance Plan requires the DHS Inventory Team to participate in the certification and accreditation (C&A) approval process to ensure that system boundary definitions and subsystems are identified and documented.

Certification and Accreditation

As part of the Department's FY 2008 Information Security Performance Plan, the CIO raised the bar on accuracy and completeness of ten artifacts used to support the DHS system certification and accreditation process. The ten artifacts include:

- FIPS 199 Assessment;
- Authority to Operate Accreditation Letter;
- System Security Plan;
- Security Assessment Report;
- Risk Assessment;
- Security Test & Evaluation Plan;
- Contingency Plan;
- Contingency Plan Test Results;
- E-authentication Analysis; and
- Privacy Threshold Analysis.

DHS established monthly metrics to monitor Component C&A compliance against published criteria in order to ensure the ten C&A documents met departmental standards. The Department's Chief Information Officer has documented significant improvements in key system certification and accreditation areas, as shown in the table below.

Table 12. DHS Certification and Accreditation Improvements

C&A Improvement	FY 2006		FY 2007		FY 2008	
	Number	Percent	Number	Percent	Number	Percent
Systems C&A'd	589	85	506	84[a]	560	95
Control Testing	613	89	579	96	584	99
Contingency Plan Testing	413	60	507	84	552	93
Total Systems	692	--	603	--	591	--

[a] One Component failed to provide completed C&A packages for 26 percent of its systems. This significantly reduced the Department's total for accredited systems

The Department's FY 2009 Information Security Performance Plan incorporates additional metrics for reviewing and approving C&A related documents. All Component C&A packages must be approved by the Component CISO prior to Headquarters review and all C&A artifacts will have the same approval and expiration dates. The Department also plans to perform continuous monitoring of key security controls, including key financial system security controls and system configuration controls.

Plans of Action and Milestones (POA&M)

In FY 2008, the Department continued to improve Component POA&M oversight, adding a number of quality checks, as well as, new requirements for managing and closing POA&Ms within reasonable timeframes for the scorecard. A "reasonableness" matrix was developed to allow POA&M schedules and resources to be checked automatically to ensure that both were realistic. Additionally, the DHS POA&M Process Guide (Attachment H of DHS 4300A) was updated to address issues raised in OIG audit reports. In particular, root cause analysis was included as part of the PO&AM process and a new attachment detailing a root cause analysis process and worksheet were added. POA&M scorecards and detailed completeness reports were distributed to the Information System Security Managers (ISSMs) and Component POA&M point-of-contacts daily. The POA&M scorecard measured the following six key elements:

- POA&M quality;
- System POA&M closure within one year;
- All audit recommendations captured;
- POA&Ms less than 90 days overdue;
- POA&Ms are validated and approved by Component ISSMs; and
- POA&M remediation schedules and resources are reasonable.

As of July 31, 2008, 99 percent (586 out of 591) of the Department's systems had no deficiency in any POA&M element.

To help in these efforts, CISO staff provided POA&M related training to more than 500 ISSO and compliance staff personnel in FY 2008. Training included 39 site visits to 16 different Components as well as three sessions at the DHS FY 2008 Security Conference held in Baltimore, Maryland.

The Department's FY 2009 Information Security Performance Plan addresses all of the FY 2008 OIG recommendations for POA&M improvements and new policies and procedures have been developed to ensure that the root causes of each weakness is addressed in a POA&M. Additional Departmental oversight is now planned to ensure that:

- All system acquisition and security architecture related weaknesses are captured in a POA&M;
- New system POA&Ms are scheduled for completion within a 6 month period; and
- Existing system POA&Ms are closed within 1 year.

Configuration Management

During FY 2008, the Department strengthened its oversight at the Components and conducted 15 compliance reviews of Component level configuration management processes. In addition, the Department issued a baseline configuration guide for the Components to follow when configuring their Windows Vista workstations.

The Department's FY 2009 Information Security Performance Plan incorporates additional requirements to further the continuous monitoring process for configuration management at the system level.

Incident Detection, Handling, and Analysis

In FY 2008, the Department continued to provide employees specialized training on the Departments' security incidents handling policies and procedures through its annual security awareness program. The DHS Security Operations Center (SOC) also implemented a comprehensive vulnerability alert, assessment, remediation, and reporting process to more effectively identify computer security vulnerabilities as part of a department-wide vulnerability assessment program. The SOC performed comprehensive vulnerability assessment scans at three components during FY 2008.

During FY 2009, the Department plans to increase the percentage of Component systems visible to the DHS SOC's vulnerability assessment scans and perform more vulnerability assessment reviews.

Security Training

In FY 2008, the Office of Human Capital implemented a department-wide web-based learning management system "*DHScovery*" to provide standardized security awareness training across the Department and track employee completion of training. In addition, the Department continued to provide a high level of security awareness and specialized security training to its employees as the table below illustrates.

Table 13. DHS Security Training Improvements

Security Training	FY 2006		FY 2007		FY 2008	
	Number	Percent	Number	Percent	Number	Percent
Total Employees	207,776	--	220,149	--	231,425	--
Employees Receiving Awareness Training	155,212	74	209,309	95	222,694	96
Employees w/Specialized Security Responsibilities	1,277	--	1,372	--	2100	--
Employees Receiving Specialized Training	1,283[1]	99	1,352	99	1967	94

1. One Component reported training provided to non-Federal employees.

At the 2008 DHS Security Conference and Workshop, the Chief Information Security Officer and Chief Security Officer presented the following tracks that focused on specialized information security topics:

- ISSO Roles and Responsibilities: Introductory Level;
- ISSO Roles and Responsibilities: Experienced Level;
- C&A for Designated Accreditation Authorities and Program Managers;
- DHS Security Management Tools;
- IT Security for CFO-Designated Financial Systems;
- Security Essentials;
- Information Security Policy and Architecture;
- Security Assessments;
- Identity Management;
- Operations and Security; and
- Privacy Policy.

These topics form the basis for defining DHS specific specialized training requirements. The Department's FY 2009 Information Security Performance Plan will incorporate additional requirements to address the OIG recommendations to track individuals and establish appropriate training.

FISMA Summary

In FY 2008, the OIG reported that the Department continued to improve and strengthen its enterprise-wide security program and show improvement in four key performance areas: POA&M weakness remediation, quality of C&As, annual testing and validation, and security program oversight. The OIG report, "Evaluation of DHS's Information Security Program for Fiscal Year 2008," identified seven recommendations for information security improvements and two recommendations for privacy compliance. POA&Ms have been developed to resolve the information security weaknesses identified in the OIG report. The OCIO plans to utilize the FY 2009 Information Security Performance Plan's enhanced metrics to further improve compliance.

The Department's requirements to support privacy controls has increased. Currently, 288 systems in the DHS inventory contain personally identifiable information; 169 systems require a privacy impact assessment; and 265 systems require systems of records notice. The privacy office is working to improve compliance in these areas and has published policies to address privacy breach notifications, and rules of behavior and consequences for failures to comply. Additional plans have also been prepared to eliminate unnecessary use of social security numbers and reduce usage of personally identifiable information.

Improper Payments Information Act

The *Improper Payments Information Act* (IPIA) of 2002 (P.L. No. 107-300) requires agencies to review their programs and activities to identify those susceptible to significant improper payments. In addition, the *Defense Authorization Act* (P.L. No. 107-107) established the requirement for government agencies to carry out cost-effective programs for identifying and recovering overpayments made to contractors, also known as "Recovery Auditing." OMB has established specific reporting requirements for agencies with programs that possess a significant risk of improper payments and for reporting on the results of recovery auditing activities.

I. Risk Assessments

In FY 2008, risk assessments were conducted on 74 DHS programs, totaling $52 billion in FY 2007 disbursements. Assessments were not conducted on programs with disbursements less than $10 million ($50 million at FEMA). Two FEMA Disaster Relief Programs, Individuals and Households Program (IHP) and Vendor Payments, were not risk-assessed as they had well established high-risk error measurements and corrective actions established from prior year testing. FEMA also excluded Mission Assignments and the Technology Transfer Program from the scope of their IPIA work. In FY 2007, DHS risk assessments included all payments (contracts, payroll, grants, travel, etc) except intra-governmental payments. In FY 2008, DHS risk assessments were expanded to include all payments.

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

Payment Processing Controls – Management's implementation of internal controls over payment processes including existence of current documentation, the assessment of design and operating effectiveness of internal controls over payments, and the identification of deficiencies related to payment processes.

Quality of Internal Monitoring Controls – Periodic internal program reviews to determine if payments are made properly.

Human Capital – Level of turnover and average tenure of program staff.

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 – Type, volume, and size of payments. Length of payment period.

Operating Environment – Existence of factors which necessitate or allow for loosening of financial controls. Any known instances of fraud.

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

A weighted average of these qualitative factors was calculated. This figure was then weighted with the size of the payment population to calculate an overall risk score. Scoring was done on a 1 (low) to 5 (high) scale. Programs with an overall score of 3 or above were considered to be high-risk for issuing improper payments.

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

Table 14. Programs at High-Risk for Improper Payments Based on FY 2008 Risk Assessments and Prior Year Payment Sample Testing

Component	Program Name	FY 2007 Disbursements ($ Millions)
CBP	Custodial – Refund & Drawback	$6,709[1]
CBP	Custodial – Continued Dumping & Subsidy Offset Act (CDSOA) & Payments to Wool Manufacturers	$409[1]
FEMA	Disaster Relief Program – Individuals and Households Program	$636[2]
FEMA	Disaster Relief Program – Vendor Payments	$1,908[2]
FEMA	Insurance – National Flood Insurance Program (NFIP)	$55
FEMA	Grants – Public Assistance Programs	$3,481
FEMA	Grants – Homeland Security Grant Program (HSGP)	$2,041
FEMA	Grants – Assistance to Firefighters Grants (AFG)	$485
FEMA	Grants – Infrastructure Protection Program (IPP)	$112[3]
ICE	Detention and Removal Operations (DRO)	$1,232[4]
ICE	Investigations	$227[4]
ICE	Federal Protective Service (FPS)	$723[4]
TSA	Aviation Security – Payroll	$2,012
U.S. Coast Guard	Active Duty Military Payroll	$2,448
U.S. Coast Guard	Contract Payments – Operating Expenses	$966[5]
U.S. Coast Guard	Contract Payments – Acquisition, Construction & Improvements	$845[5]
Total FY 2007 Disbursements		**$24,289**

1. CBP's programs were reported as one program, Custodial, in the FY 2007 DHS AFR.
2. FEMA's two Disaster Relief Programs are high-risk based on prior year payment sample testing.
3. The only exception to the rating scale used to identify high-risk programs in FY 2007 was for FEMA's Infrastructure Protection Program (IPP). This grant program received an overall score of 3.1 for FY 2006 disbursements but dropped to 2.3 for FY 2007 disbursements. The scores for the risk conditions were exactly the same in both years, but relative to other programs, expenditures dropped to the lowest impact category. Since IPP was not tested for FY 2006 disbursements when it was rated a high-risk, the risk condition rating remained the same, and expenditures increased, it was determined that IPP would remain classified as a high-risk program until payments underwent sample testing.
4. Only the non-payroll portion of ICE programs was found to be high-risk. Disbursement figures are for non-payroll disbursements.
5. Contracts were reported as a single program for U.S. Coast Guard in the FY 2007 DHS AFR.

DHS has no programs previously identified in the former Section 57 of Circular A-11 (now covered under OMB Circular A-123, Appendix C).

II. Statistical Sampling Process

A stratified sampling design was used to test payments based on FY 2007 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 was completed by a statistician under contract.

Sampling plans generally provided an overall estimate of the percentage of improper payment dollars within +/-2.5 percent precision at the 90 percent confidence level, as specified by OMB guidance. An expected error rate of 5 percent of total payment dollars was generally used in the sample size calculation.

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

The following procedure describes the sample selection process:

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

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

DHS sample test results are listed in Table 15.

Table 15. DHS Sample Test Results

Component	Program	FY 2007 Payment Population ($millions)	FY 2007 Sample Size ($millions)	Est. Error Amount ($millions)	Est. Error Percentage (%)
CBP	Refund & Drawback	6,709	48	2	0.03
	Custodial – Continued Dumping & Subsidy Offset Act (CDSOA) & Payments to Wool Manufacturers	409	315	0	0
FEMA	Disaster Relief Program - Individuals and Households Program	636	3	46[1]	7.22[1]
	Disaster Relief Program - Vendor Payments	1,908	597	144	7.57
ICE	Detention and Removal Operations	1,232	358	10	0.85
	Federal Protective Service	723	87	267[2]	36.92[2]
	Investigations	227	64	4	1.87
TSA	Aviation Security - Payroll	2,012	1	2	0.09
U.S. Coast Guard	Operating Expenses - Active Duty Military Payroll	2,448	4	21	0.84
	Operating Expenses - Contracts	966	203	0	0.02
	Acquisition, Construction, and Improvements - Contracts	845	452	0	0.001
DHS	**All Programs**	**18,115**	**2,132**	**496**	**2.74**
DHS	**High-Risk Programs (Est. Error Amount >$10 Million)**	**5,715**	**691**	**478**	**8.36**

1. The estimated error amount and rate for Hurricanes Katrina and Rita are $43 million and 10.22 percent. The estimated error amount and rate for all other disasters is $3 million and 1.21 percent. FEMA IHP payments for Hurricanes Katrina and Rita used a 15 percent expected error rate.
2. The precision rate for ICE's Federal Protective Service program was +/- 5.0 percent at the 90 percent confidence level because the actual error rate was higher than the sample design estimate.

The DHS Office of the Chief Financial Officer devoted significant staff and contractor resources to: strengthen sample testing guidance; work with Components in developing test plans; and independently review sample test results. Several programs considered at high-risk based on risk assessment grading were not confirmed as at high-risk based on sample test results. The main reason for the estimated error rates falling below $10 million for these programs was the presence of strong compensating controls such as additional levels of payment review for manually intensive processes. Compensating controls will be considered more prominently in future risk assessments.

Based on the results of sample testing, corrective action plans are required for the following five programs due to estimated error amounts above $10 million: FEMA's Disaster Relief Program - Individuals and Households Program, FEMA's Disaster Relief Program - Vendor Payments, ICE's Detention and Removal Operations, ICE's Federal Protective Service and U.S. Coast Guard's Operating Expenses – Active Duty Military Payroll.

IPIA Pilot Study

Due to the complexity of testing grant programs, developing robust test plans, defining the sampling unit, and obtaining the underlying source documentation for testing, FEMA and DHS determined that for FY 2007 payments, the most effective approach was to conduct a test pilot study of five FEMA programs in order to gain an understanding of the most effective way to test each program in FY 2009.

During FY 2008, FEMA conducted a test pilot review of five programs identified as high-risk during the FY 2007 risk assessments. The five programs are: the National Flood Insurance Program (NFIP), and four high-risk grant programs – Public Assistance (PA), Homeland Security Grant Program (HSGP), Assistance to Firefighters Grant (AFG) Program, and Infrastructure Protection Program (IPP). This pilot developed approaches for conducting an IPIA assessment and a methodology for testing payments.

During the pilot study, FEMA developed draft test plans for the five programs and determined sampling methodologies focusing on the areas of highest risk within each program. The pilot study included a review of program specific policies, grant documents, and data from the systems of record, site visits, and interviews of key staff at Headquarters and the Regions. During the pilot study, FEMA confirmed that the programs vary in complexity depending on the relationship between FEMA, the States (applicants), sub-applicants, and private insurance companies. FEMA identified recommended assessment options conducive to IPIA testing and is in a position to conduct testing in FY 2009. Improper payment targets will be developed upon completion of sample testing.

III. Corrective Action Plans

Corrective Action Plans for High-Risk Programs

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

FEMA IHP

Table 16. Completed IHP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Insufficient system edits.	1. Ownership / Occupancy feature in NEMIS was not fully operational.	1. Upgrade system edits.	June 2006	ChoicePoint contract made verification feature operational.
	2. Address capability in NEMIS needed improvements.	1. Update system edits.	April 2007	
	3. NEMIS system lacked data to verify all eligibility amounts.	1. Update system with Federal maximum assistance amounts.	December 2007	

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Insufficient system edits.	4. NEMIS system lacked sufficient data and edits to prevent and detect improper payments in a timely manner.	1. Sign contract for data verification and pre-population of verified data.	December 2007	
2. Inadequate monitoring, training, and quality assurance work.	1. Incomplete real-time quality control monitoring.	1. Improve procedures and capabilities supporting real-time quality control monitoring.	August 2006	
	2. Inability to judge and improve caseworker performance.	1. Develop metrics to measure caseworker performance.	October 2006	Caseworker scoring metrics focus on whether disaster policies were followed and whether case correspondence and processing were correct.
	3. Improved quality controls needed for manual reviews.	1. Implement controls to prevent duplicate or incorrect payments.	July 2007	
	4. Additional IPIA testing needed to confirm progress, update error estimate, and comply with IPIA.	1. Conduct additional rounds of IPIA sample testing, assess findings, and update reporting.	July 2007 and Ongoing	Four rounds of IHP sample testing completed to date.
3. Poor or outdated policy and guidance.	1. Applicant recertification guidelines needed improvement.	1. Develop processes to prevent and detect improper payments in a timely manner.	December 2007	
	2. Processes lacking for approving policy and guidance.	1. Improve policies and guidance for approving and making payments to affected individuals and households for certain functional areas identified by IPIA sample testing.	March 2008	

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
3. Poor or outdated policy and guidance.	3. Inadequate Expedited Assistance policy.	1. Complete an Expedited Assistance policy memo.	September 2008	Expedited Assistance restrictions were addressed by Disaster Assistance Interim Policy 9462.1: Critical Needs Assistance for Displaced Individuals and Households which was signed into effect on September 2, 2008.
4. Inability to scale up operations to handle catastrophic disaster workload.	1. Additional, impartial housing inspectors needed.	1. Recompete housing inspection contract.	March 2007	
	2. Additional trained call center agents needed to process greatly increased number of claims.	1. Award a contract to make available 6,000 call center agents.	March 2008	

Table 17. In Process and Planned IHP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Insufficient system edits.	1. Separated Households policy needs to be reflected in system edits.	1. Clarify policy and develop consistent system edit checks.	March 2009	Developed draft policy on Separated Households to clarify in which circumstances FEMA will authorize separate applications and provide temporary housing assistance to more than one disaster application from a single household.

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
2. Inadequate monitoring, training, and quality assurance work.	1. Personnel need training with the Lodging Expense Reimbursement System.	1. Provide training and require employees to pass a certification test.	March 2009	Enhanced training was not provided in FY 2008 for Lodging Expense Reimbursement. FEMA uses an established policy dated August 1998. Training on this policy was provided in previous years. Recent disasters hindered the scheduling of training.
3. Poor or outdated policy and guidance.	1. Inconsistent application of disaster-specific policy.	1. Develop and implement a process which ensures consistent application of disaster-specific policy.	October 2008	Quality Control will expand its function to include review on a near real-time basis of special projects, new processing procedures, and disaster specific processing procedures.
	2. Separated Households policy is incomplete.	1. Develop policies and guidance needed to approve and make payments to affected individuals and households.	March 2009	

FEMA Vendor Payments

Table 18. Completed Vendor Payments Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Inadequate monitoring, training, and quality assurance work.	1. Training of COTR roles and responsibilities needed improvement.	1. Develop and require a standard COTR Appointment Letter identifying the COTR's authority.	November 2007	Implemented a standard COTR Appointment Letter and Nomination Form.
	2. Internal control gaps existed in the vendor payment process.	1. Initiate a quality assurance review process to reduce improper payments.	November 2007	
	3. Training of Accounting Technicians roles and responsibilities needed improvement.	1. Update training for Accounting Technicians to ensure it addresses improper payment problems.	January 2008	Multiple training presentations given on improper payments and internal controls.

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Inadequate monitoring, training, and quality assurance work.	4. Payments of invoices were sometimes authorized without proper signature authority, supporting documentation, and quality checks.	1. Strengthen the process and controls for designating authorized invoice reviewers and approvers so that designated signatories and alternates are properly documented and readily accessible.	July 2008	
2. Poor or outdated policy and guidance.	1. Policies for Accounting Technicians lacked precision and formal documentation.	1. Conduct a review of policies, procedures, and job descriptions for Accounting Technicians.	November 2007	Reviewed major duties, SOPs, policies, and process maps for Accounting Technicians. Reviewed job description for Financial Management Specialists.
		2. Document the Invoice Follow-up process responsibilities for Accounting Technicians to ensure invoices are paid in a timely manner.	January 2008	Process documented with emphasis on how to identify and return improper invoices and how to process corrected invoices.
3. Inability to scale up operations to handle catastrophic disaster workload.	1. Processes to expand operations in response to catastrophic disasters needed improvement.	1. Initiate a quality assurance review process to reduce improper vendor payments.	November 2007	Quality assurance review completed. Work from 50 percent of accounting technicians sampled.
		2. Analyze results of the policies, procedures, and job descriptions for Accounting Technicians and implement changes, as needed.	February 2008	Problems with signature authorities identified and resolved.

Table 19. In Process and Planned Vendor Payments Corrective Actions

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

ICE Detention and Removal Operations

Table 20. Planned Detention and Removal Operations Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Lack of Supporting Documentation.	1. Potential incidence of fraud, waste, and abuse of government funds.	1. Implement general oversight and monitoring to verify valid contract and obligation exists.	January 2009	All DRO offices will transition to a single point of receipt for invoices. This change will enable the ICE OCFO to perform an up-front verification that an invoice is associated with a valid contract and obligation.
2. Goods and services received prior to award of contract.	1. Unauthorized use of budgetary resources.	1. Build awareness of regulations and laws through focused training and improved dissemination of policies.	Ongoing	- In August 2008, ICE conducted comprehensive training for its Analysts on obligation recording, monitoring, and management. - Implementing further training to reiterate policies and procedures.
3. Proper invoice did not exist in that the invoice did not contain the vendor's name.	1. Illegitimate invoice that can lead to potential incidence of fraud, waste, and abuse of government funds.	1. Implement up-front verification to ensure invoices received are in compliance with the FAR regulations.	January 2009	All DRO offices will transition to a single point of receipt for invoices. This change will enable the ICE OCFO to verify that an invoice is compliant with FAR upon receipt.

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
3. Proper invoice did not exist in that the invoice did not contain the vendor's name.	1. Illegitimate invoice that can lead to potential incidence of fraud, waste, and abuse of government funds.	2. Improved documentation of award contract that clearly states the elements of a FAR compliant invoice.	January 2009	All DRO specific Contracting Specialists will be trained to include instructions for submission of invoice on the contract/award document.
4. Adjustments were not duly authorized.	1. Potential over/under payment of invoice.	1. Implement improved controls for monitoring invoice adjustments.	January 2009	All DRO offices will transition to a single point of receipt for invoices. This change will enable ICE OCFO to monitor the payment of each invoice and assist DRO with invoice adjustment, as needed.
		2. Monitor compliance with the standard operating procedure for processing invoice adjustment.	Ongoing	
5. No receiving report documentation	1. No formal documentation of receipt of goods and services	1. Implement improved controls for receiving and approval process.	January 2009	All DRO offices will transition to an improved invoice process where invoices are not paid unless authorized receiving and approval documentation is received by ICE OCFO.
6. Under paid interest.	1. Potential violation of Prompt Payment Act.	1. Ensure invoice receipt date is clearly indicated on the invoices.	January 2009	All DRO offices will transition to a single point of receipt for invoices. This change will enable ICE OCFO to stamp each invoice with the 'invoice received date' prior to forwarding it for processing.
		2. Ensure compliance with standard operating procedures.	January 2009	
7. Over paid interest.	1. Potential waste of government funds that could have been utilized for mission support activities.	1. Ensure invoice receipt date is clearly indicated on the invoices.	January 2009	All DRO offices will transition to a single point of receipt for invoices. This change will enable ICE OCFO to stamp each invoice with the 'invoice received date' prior to forwarding it for processing.
		2. Ensure compliance with standard operating procedures.	January 2009	

ICE Federal Protective Service

Table 21. Completed Federal Protective Service Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
1. Lack of Supporting Documentation.	1. Potential incidence of fraud, waste, and abuse of government funds.	1. Implement general oversight and monitoring to verify valid contract and obligation exists.	August 2007	Throughout FY 2007 and 2008, ICE implemented a single point of receipt for invoices. This change has enabled ICE OCFO to perform an up-front verification that an invoice is associated with a valid contract and obligation.
2. Goods and services received prior to award of contract.	1. Unauthorized use of budgetary resources.	1. Build awareness of regulations and laws through focused training and improved dissemination of policies.	Ongoing	- In August 2008, ICE conducted comprehensive training for its Analysts on obligation recording, monitoring, and management. - Implementing further training to reiterate policies and procedures.
3. Proper invoice did not exist in that the invoice did not contain the vendor's name.	1. Illegitimate invoice that can lead to potential incidence of fraud, waste, and abuse of government funds.	1. Implement up-front verification to ensure invoices received are in compliance with the FAR regulations.	August 2007	Throughout FY 2007 and 2008 ICE implemented a single point of receipt for invoices. This has enabled ICE OCFO to verify that an invoice is compliant with FAR.
		2. Improved documentation of award contract that clearly states the elements of a FAR compliant invoice.	August 2007	Throughout FY 2007 and 2008, ICE trained its Contracting Specialists to ensure award documents included specific instructions for submission of invoice.
4. Adjustments were not duly authorized.	1. Potential over or under payment of invoice.	1. Implement improved controls for monitoring invoice adjustments.	August 2007	Throughout FY 2007 and 2008, ICE implemented a single point of receipt for invoices. This change has enabled ICE OCFO to monitor the payment of each invoice and assist Programs with Invoice Adjustment as need.

Category of Error	Risk Factors	Corrective Actions	Completed Date	Comments
4. Adjustments were not duly authorized.	1. Potential over or under payment of invoice.	2. Monitor compliance with the standard operating procedure for processing invoice adjustment.	Ongoing	
5. No receiving report documentation.	1. No formal documentation of receipt of goods and services.	1. Implement improved controls for receiving and approval process.	August 2007	Throughout FY 2007 and 2008, ICE implemented improved invoice processes where invoices are not paid unless authorized receiving and approval documentation is received.
6. Under paid interest.	1. Potential violation of Prompt Payment Act.	1. Ensure invoice receipt date is clearly indicated on the invoice.	August 2007	Throughout FY 2007 and 2008, ICE implemented a single point of receipt for invoices. The ICE OCFO now stamps each invoice with the 'invoice received date' prior to forwarding it for processing.
		2. Ensure compliance with standard operating procedures.	Ongoing	
7. Over paid interest.	1. Potential waste of government funds that could have been utilized for mission support activities.	1. Ensure invoice receipt date is clearly indicated on the invoice.	August 2007	Throughout FY 2007 and 2008, ICE implemented a single point of receipt for invoices. The ICE OCFO now stamps each invoice with the 'invoice received date' prior to forwarding it for processing.
		2. Ensure compliance with standard operating procedures.	Ongoing	

U.S. Coast Guard Active Duty Military Payroll

Table 22. In Process and Planned ADMP Corrective Actions

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
1. Lack of supporting documentation.	1. Missing personnel record source documentation.	1. Issue contract to evaluate status of records and recommend corrective actions.	January 2009	90 day contract signed with report due mid-January.
		2. Update policy to include the retention of appropriate source documents within military personnel data records.	January 2009	Scanned oath is critical to proving person works at USCG. Interim policy by January 2009. Final policy to include monitoring procedures.
		3. Establish procedures to ensure appropriate source documentation is captured at the Accession points.	July 2009	Involvement of military recruiters and servicing personnel offices is key.
		4. Develop and implement monitoring procedures to ensure adequacy of personnel record source documentation.	December 2009	
2. Untimely updating of personnel system.	1. Incorrect housing allowance.	1. Through training, ensure payroll systems are updated timely with housing change information.	March 2009	When feeder system is not updated timely, payment systems do not know the housing allowance entitlement has changed. Pay stubs contain a message alerting payee that errors must be brought to the immediate attention of personnel officer.

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
2. Untimely updating of personnel system.	1. Incorrect housing allowance.	2. Expand use of housing report which identifies records with a housing action and housing allotment set to yes.	FY 2005 and Ongoing	USCG has been using such a report since FY 2005 which has resulted in a decline in overpayments from 15-20 per month to 0-5 per month. Summer transfer season is when error rate is greatest.
3. IPIA testing issues.	1. Delays in producing a correct payment detail file.	1. Reconcile transaction file total to accounting system trial balance.	December 2008	FY 2008 was the first year that USCG and DHS conducted IPIA sample testing of large payroll payment populations.
		2. Increase test time period to allow ample time for retrieval of supporting documentation.	December 2008	USCG should begin compiling detailed FY 2008 transaction file in late November. Other corrective actions and lessons learned should speed up document retrieval.
4. USCG organizational issues.	1. Competition for resources with actuarial pension liability testing and other financial statement audit testing.	1. Review, and when possible, synchronize time frames to minimize conflict and maximize efficiency.	December 2008	
	2. Need to reduce and standardize critical personnel source documentation.	1. Reach agreement between all critical parties on required data elements and source documentation.	January 2009	U.S. Coast Guard transformation team will host joint meetings in November with human resources, CFO, and CIO.
	3. No single owner of personnel offices.	1. The U.S. Coast Guard Modernization will result in organizational enhancements which will align recruiting, payroll, and personnel under one command.	March 2009	This issue is critical and resolution has proved elusive.

Category of Error	Risk Factors	Corrective Actions	Target Completion Date	Comments
4. USCG organizational issues.	4. Improve training for field personnel and housing officers (payroll processing is a secondary duty for majority of transaction processors).	1. Require completion of online training to acquire certification before transactions can be entered into feeder systems.	July 2009	This step will address geographic dispersion and the large number of officers. Roll out targets need to be established.

IV. Program Improper Payment Reporting

Table 23 summarizes improper payment amounts for DHS high-risk programs and projects future year improvements based on completing corrective actions. Improper payment (IP) percent and dollar figures are based on statistical estimates for FY 2007. These estimates are then projected for FY 2008 and beyond based on improvements expected from completing corrective actions.

Table 23. Improper Payment Reduction Outlook

Improper Payment Reduction Outlook ($ in millions)															
Program	FY 2007 Outlays	FY 2007 IP%	FY 2007 IP$	FY 2008 Outlays	FY 2008 IP%	FY 2008 IP$	FY 2009 Est. Outlays	FY 2009 IP%	FY 2009 IP$	FY 2010 Est. Outlays	FY 2010 IP%	FY 2010 IP$	FY 2011 Est. Outlays	FY 2011 IP%	FY 2011 IP$
IHP (FEMA)	$636	7.22	$46	$606	7.00	$42	$636	5.50	$35	$668	3.50	$23	$701	2.50	$18
Vendor Payments (FEMA)	$1,908	7.57	$144	$1,526	7.00	$107	$1,602	5.00	$80	$1,682	3.00	$50	$1,766	2.50	$44
DRO (ICE)	$1,232	0.85	$10	$1,738	0.75	$13	$2,332	0.48	$11	$2,205	0.30	$7	$2,198	0.18	$4
FPS (ICE)	$723	36.9	$267	$745	26.00	$194	$778	19.45	$151	$812	9.00	$73	$848	1.50	$13
Active Duty Military Payroll (USCG)	$2,448	0.84	$21	$2,551	0.84	$21	$2,628	0.74	$19	$2,707	0.59	$16	$2,788	0.44	$12
The following programs (with actual FY 2007 and FY 2008 Outlays and Projected FY 2009-2011 Outlays listed in $millions) will have measurements reported beginning in DHS's FY 2009 AFR: FEMA – National Flood Insurance Program (NFIP), (Outlays – FY 2007 $55; FY 2008 $53; FY 2009 $76; FY 2010 $112; and FY 2011 $137) FEMA – Public Assistance Grants, (Outlays – FY 2007 $3,481; FY 2008 $1,026; FY 2009 $2,324; FY 2010 $2,579; and FY 2011 $2,648) FEMA – Homeland Security Grant Program, (Outlays – FY 2007 $2,041; FY 2008 $2,189; FY 2009 $2,284; FY 2010 $2,348; and FY 2011 $2,450) FEMA – Assistance to Firefighters Grants, (Outlays – FY 2007 $485; FY 2008 $356; FY 2009 $378; FY 2010 $416; and FY 2011 $453) FEMA – Infrastructure Protection Program, (Outlays – FY 2007 $112; FY 2008 $417; FY 2009 $138; FY 2010 $153; and FY 2011 $164)														

Notes:

For FEMA's IHP and Disaster Relief Program vendor payments programs, two major assumptions are used. The first assumption involves estimating future year outlays. The difficulty is that these programs do not have stable outlays from year to year because emergency response to Presidential declared disasters and other emergencies varies through time. The estimated outlay figures above were based on an average of the five most recent fiscal years (in millions of dollars for vendor payments – FY 2003 $774; FY 2004 $1,322; FY 2005 $6,645; FY 2006 $6,747; and FY 2007 $1,782; in millions of dollars for IHP payments – FY 2003 $684; FY 2004 $982; FY 2005 $4,638; FY 2006 $3,902; and FY 2007 $932). Figures for FEMA's NFIP program are for payments made directly by FEMA and do not include payments made by insurance companies on FEMA's behalf. These excluded payments in millions of dollars were: FY 2007 $1,306; FY 2008 $2,522; FY 2009 $1,837; FY 2010 $1,568; and FY 2011 $1,628.

Outlay projections for Active Duty Military Payroll use a 3.0 percent cost-of-living adjustment applied to FY 2008 actuals.

Recovery of Improper Payments

As of September 30, 2008, FEMA has collected $20.6 million for Hurricanes Katrina, Rita, and Wilma IHP payments identified as improper as a result of payment sample testing. In January 2007, DHS published interim regulation 6 CFR Part 11, which took effect immediately and required FEMA to provide disaster applicants who were in recoupment with the opportunity for an oral hearing. This regulation applied to disasters declared on or after January 30, 2007. On June 13, 2007, the U.S. District Court in Ridgely applied the same criteria to disaster applicants from Hurricanes Katrina and Rita.

In response to the Ridgely lawsuit, FEMA published a notice in the *Federal Register* on September 5, 2008. This notice effectively withdrew previous recoupment notifications sent to disaster applicants affected by Hurricanes Katrina and Rita and announced FEMA's intention to implement a new recoupment process for those applicants in accordance with 6 CFR Part 11. The *de novo* process provides that FEMA will review the files of Katrina and Rita disaster applicants identified for recoupment. If FEMA's latest review indicates a debt may be owed, FEMA will send a new notice and commence new recoupment proceedings that include an opportunity for an oral or paper hearing.

V. Recovery Auditing Reporting

DHS completed recovery audit work for FY 2007 disbursements and continued collection activities for errors identified in prior year recovery audits. Work was completed at ICE, U.S. Coast Guard, and the Components they cross-service (DNDO, MGMT, NPPD, S&T, TSA, and USCIS). Work was also completed at CBP. In Table 24 which follows, CY equals FY 2007 disbursements and PY covers FY 2005 and FY 2006 for DNDO, TSA, and U.S. Coast Guard; FY 2004 to FY 2006 for ICE, MGMT, NPPD, S&T, and USCIS; and FY 2004 to FY 2005 for CBP.

Table 24. Recovery Audit Results

DHS Component	Amount Subject to Review for CY Reporting ($ Millions)	Actual Amount Reviewed and Reported CY ($ Millions)	Amounts Identified for Recovery CY ($000)	Amounts Recovered CY ($000)	Amounts Identified for Recovery PYs ($000)	Amounts Recovered PYs ($000)	Cumulative Amounts Identified for Recovery (CY + PYs) ($000)	Cumulative Amounts Recovered (CY + PYs) ($000)
CBP[1]	$1,765	$1,765	$90	$0	$180	$131	$270	$131
DNDO	$54	$54	$0	$0	$0	$0	$0	$0
ICE	$1,749	$1,749	$102	$50	$1,663	$1,479	$1,765	$1,529
MGMT	$292	$292	$11	$8	$146	$62	$157	$70
NPPD[2]	$297	$297	$0	$0	$190	$125	$190	$125
S&T	$362	$362	$1	$1	$53	$53	$54	$54
TSA[3]	$1,865	$1,865	$643	$625	$86	$67	$729	$692
USCG[4]	$2,505	$2,505	$74	$44	$90	$66	$164	$110
USCIS	$495	$495	$8	$0	$895	$850	$903	$850
Totals	**$9,384**	**$9,384**	**$929**	**$728**	**$3,303**	**$2,833**	**$4,232**	**$3,561**

1. Prior year amounts identified for recovery adjusted down from $184 to $180 based on additional FY 2008 research.
2. Includes the US-VISIT program and legacy Component Information Analysis and Infrastructure Protection.
3. Prior year amounts identified for recovery adjusted down from $91 to $86 based on additional FY 2008 research.
4. Prior year amounts identified for recovery adjusted down from $282 to $90 based on additional FY 2008 research.

VI. Ensuring Management Accountability

Managers are held accountable for reducing and recovering improper payments in a variety of ways. DHS receives quarterly grades from OMB on the President's Management Agenda (PMA) Eliminating Improper Payments scorecard. Managers are responsible for completing internal control work on payment processing as part of the Department's OMB Circular A-123 effort. Payment processing key controls were evaluated for test of design and documentation in FY 2007. In FY 2008, payment processing key controls were tested for their operating effectiveness.

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

VII. Agency Information Systems and Other Infrastructure

The Department is undertaking a Transformation and Systems Consolidation initiative which is discussed further in the Financial Management Systems Framework (see Page 206).

FEMA is improving its financial system interfaces to reduce improper payments in its Disaster Relief Program. CBP is upgrading its financial system to automate the handling of Custodial payments.

The Department applied additional contractor support resources in FY 2008 to strengthen its guidance, test plan development, and review of Component IPIA payment sample testing.

VIII. Statutory or Regulatory Barriers

None.

IX. Overall Agency Efforts

The Department focused its FY 2008 efforts on improving payment sample testing. Sample testing was based on risk assessment results. Additional guidance was provided on test attributes for different payment types. Sample test plan development and review were more rigorous. An independent review of Component reported sample test results was completed at three Components. The completion of a test pilot prepares the Department to begin reporting error measurements for the National Flood Insurance Program and four high-risk FEMA grant programs in FY 2009.

The Department completed several IPIA related initiatives in FY 2008 including: 1) expansion of IPIA related classes as part of DHS's Internal Control University and CFO New Hire Orientation training; 2) active participation in government-wide IPIA groups including the Improper Payments Transformation Team and a government-wide partnership examining how to better leverage IPIA and Single Audit Act grant payment work; and 3) completion of the testing of key controls over payments at several Components as required by OMB Circular A-123.

Other Key Regulatory Requirements

Prompt Payment Act

The *Prompt Payment Act* requires Federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's Components submit Prompt Payment data as part of data gathered for the OMB CFO Council's Metric Tracking System (MTS). Periodic reviews are conducted by the DHS components to identify potential problems. Interest penalties as a percentage of the dollar amount of invoices subject to the *Prompt Payment Act* has been measured between 0.01 percent and 0.04 percent for the period of October 2007 through September 2008, with an annual average of 0.02 percent (Note: MTS statistics are reported with at least a six week lag).

Debt Collection Improvement Act (DCIA)

The DHS Office of the Chief Financial Officer (CFO) is developing and implementing comprehensive debt collection regulations that would supersede Components' legacy agency regulations. The DHS-wide debt collection regulations will provide instructions to the components on meeting the reporting requirements in support of the *Debt Collection Improvement Act* of 1996 (DCIA). This act established the following purposes:

- To maximize collections of delinquent debts owed to the Federal Government by ensuring quick action to enforce recovery of debts and the use of all appropriate collection tools;
- To minimize the costs of debt collection by consolidating related functions and activities and utilizing interagency teams;
- To reduce losses arising from debt management activities by requiring proper screening of potential borrowers, aggressive monitoring of all accounts, and sharing of information within and among Federal agencies;
- To ensure that the public is fully informed of the Federal Government's debt collection policies and that debtors are cognizant of their financial obligations to repay amounts owed to the Federal Government;
- To ensure that debtors have appropriate due process rights, including the ability to verify, challenge, and compromise claims, and have access to administrative appeals procedures which are both reasonable and protect the interests of the United States;
- To encourage agencies, when appropriate, to sell delinquent debt, particularly debts with underlying collateral; and
- To rely on the experience and expertise of private sector professionals to provide debt collection services to DHS components.

To achieve these purposes, the Department's goals are to: 1) overcome DCIA deficiencies by having fair, aggressive, and consistent internal programs to recover non-tax delinquent debt; 2) improve the Department's non-tax debt collection performance by promoting the resolution of delinquencies as quickly as possible; 3) refer all eligible non-tax delinquent debts to Treasury (for Treasury Offset and/or Cross Servicing) at the 180 day point as required by the DCIA; 4) reduce future write-offs of debt by implementing a debt collection strategy incorporating the authorities

within OMB's Circular A-129, *Policies for Federal Credit Programs and Non-Tax Receivables (11/2000)*; 5) require that all DHS Components have finalized internal policies and procedures to ensure that potential debtors to the Federal Government have all appropriate due process rights; and, 6) ensure the accuracy and timeliness of reports on receivables by reporting, certifying, and verifying all required data on the Treasury Report on Receivables and Debt Collection Activities.

FY 2006 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 things of value provided to specific recipients, beyond those received by the general public. The purpose of these reviews is to identify those agencies assessing user fees, and to periodically adjust existing charges to 1) reflect unanticipated changes in costs or market values; and, 2) to review all other agency programs to determine whether fees should be assessed for Government services or the use of Government goods or services.

To ensure compliance with this biennial requirement, each DHS Component is required to compile and furnish individual summaries for each user fee by addressing the key points for each user fee, in sufficient detail, to facilitate a review by the OCFO. For FY 2007, five of the DHS Components were responsible for collecting forty-one different 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:

- ***United States Customs and Border Protection (CBP)*** – The user fee programs for CBP consist of 23 different fees covering various services that are provided to passengers and conveyances at ports of entry to the United States. In FY 2007, the fees collection totaled $2.311 billion and the costs for services provided relative to these fees totaled $2.977 billion. The shortfall from fee revenue is over $666 million.

- ***United States Citizenship and Immigration Services (USCIS)*** – USCIS is responsible for collecting fees from persons requesting immigration benefits and depositing them into the Immigration Examination Fee Account (IEFA). These fees are used to fund the full cost of processing immigration and naturalization benefit applications and petitions, biometric services, and associated support services. In addition, these fees must recover the cost of providing similar services to asylum and refugee applicants and certain other immigrants at no charge. Additionally, USCIS collects fees for Fraud Reporting and Nonimmigrant worker benefit applications. These fees generated a total of $2.160 billion in revenues and $1.783 billion in expenditures resulting in a surplus of $377 million. USCIS is currently conducting a new comprehensive review of the resources and activities funded by the IEFA to determine whether the current fees reflect current processes or recover the full costs of services that should be provided.

- ***Transportation Security Administration (TSA)*** – TSA is responsible for collecting nine different security fees which include: the Air Cargo Security Fee; the Aviation Security Infrastructure Fee; Fees for Security Threat Assessments for HAZMAT Drivers; Flight Training for Aliens Fee; the Passenger Civil Aviation Security Service Fee; the Registered Traveler Fee; the Protection of Sensitive Security Information Fee; the Transportation

Worker Identification Credential Fee and the Ronald Reagan Washington National Airport Enhanced Security Procedures for Certain Operations Fees. During FY 2007, TSA collected $2.560 billion for these five fees. The obligations incurred by TSA for providing these services were $10.222 billion. This amount exceeded related fee collections by $7.662 billion.

- ***U.S. Coast Guard*** – The U.S. Coast Guard charges fees for the following maritime services: 1) Merchant Mariner Licensing and Documentation User Fees, 2) Commercial and Recreational Vessel Documentation User Fees, 3) Vessel Inspection User Fees for U.S and Foreign Vessels requiring a certificate of inspection, and 4) Overseas Inspection and Examination Fees. In FY 2007, the fee collections from these services amounted to $27.3 million.

- ***Federal Emergency Management Agency (FEMA)*** – FEMA collects fees for Radiological Emergency Preparedness Program. This program provides site-specific, plume pathway Emergency Planning Zone (EPZ) biennial exercise-related component services. In FY 2007, the fees collected for this program totaled $24.9 million.

A preliminary review of DHS user fees was conducted by the Office of the Chief Financial Office (OCFO) in FY 2008. This review was based on the component's FY 2007 data and user fee structures that had been established through the legacy agencies.

Major Management Challenges

Office of Inspector General

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

Homeland Security

November 12, 2008

MEMORANDUM FOR: The Honorable Michael Chertoff
Secretary

FROM: Richard L. Skinner
Inspector General

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

Attached is our annual report, *Major Management Challenges Facing the Department of Homeland Security,* for inclusion in the DHS FY 2008 Annual Financial Report. This report, including the department's comments in their entirety, will also be posted on our public website.

Should you have any questions, please call me, or your staff may contact James Taylor, Deputy Inspector General, at (202) 254-4100.

Attachment

Department of Homeland Security
Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

OIG-09-08

November 2008

Office of Inspector General

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

Homeland Security

November 12, 2008

Preface

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

The attached report presents our FY 2008 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

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

Richard L. Skinner

Richard L. Skinner
Inspector General

Office of Inspector General

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

Major Management Challenges Facing the Department of Homeland Security

The creation of the Department of Homeland Security galvanized the Nation's fight against terrorism by consolidating and mobilizing the assets of the federal government under one roof with a single, focused mission: to ensure that the tragic events of Sept. 11, 2001, are never repeated again on American soil.

After just 5 short years, we are beginning to witness the positive effects of the department's efforts and initiatives: tighter security at the borders; increased immigration enforcement; greater cooperation with our international partners; expanded partnerships with the private sector; better and more efficient passenger screening at our airports; and regenerated disaster response and recovery management. Despite these considerable accomplishments, DHS still has much to do to establish a cohesive, efficient, and effective organization.

The major management challenges we have identified significantly affect the department's ability to protect our homeland and are decisive factors in setting priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

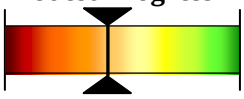
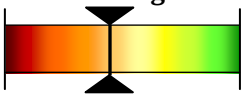
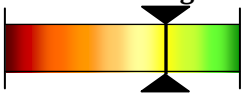
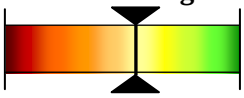
We have identified the following major management challenges:

- Acquisition Management
- Financial Management
- Information Technology Management
- Catastrophic Disaster Response and Recovery
- Grants Management
- Infrastructure Protection
- Border Security
- Transportation Security
- Trade Operations and Security

Since the major management challenges have tended to remain the same from year to year, we are developing scorecards to distinguish the department's progress in selected areas. Our

first scorecard, published in the *Semiannual Report to Congress*, October 1, 2006 – March 31, 2007, included an assessment of DHS' acquisition function. This report features scorecards for acquisition management, financial management, information technology management, and catastrophic disaster response and recovery. These four scorecards are summarized in Figure 1 and incorporated in our discussion of the major management challenges.

Figure 1.

DHS' OVERALL PROGRESS IN SELECTED AREAS	
Ratings are based on a four-tiered scale: Limited, Modest, Moderate, and Substantial.	
Acquisition Management	**Modest Progress** 
Financial Management	**Modest Progress** 
Information Technology Management	**Moderate Progress** 
Catastrophic Disaster Response and Recovery	**Moderate Progress** 

ACQUISITION MANAGEMENT

Contracting for goods and services consumes nearly 40% of the department's annual budget and is absolutely critical to achieving its mission. Acquisition management is a complex process that goes beyond simply awarding a contract. It begins with the identification of a mission need; continues with the development of a strategy to fulfill that need while balancing cost, schedule, and performance; and concludes with contract closeout after the terms have been satisfactorily met. A successful acquisition process requires an effective acquisition management infrastructure.

The following are critical acquisition success factors:

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

Acquisition Management Scorecard

The following scorecard demonstrates areas where DHS has strengthened its acquisition management practices. We based our assessment on pertinent reports, particularly recent audit work conducted at the Federal Emergency Management Agency (FEMA), reports published by the Government Accountability Office (GAO), and congressional testimony. Given the scope of our review, we did not perform an in-depth assessment of each cornerstone of the acquisition framework. We used the critical elements within each—organizational alignment and leadership, policies and processes, acquisition workforce, and knowledge management and information systems—as well as our broader knowledge of the acquisition function, to gauge overall progress in those cornerstones.

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

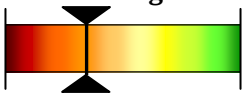
- **Limited:** While there may be plans to address critical success factors, few if any have been implemented;
- **Modest:** While some improvements have been made, many of the critical success factors have not yet been achieved;
- **Moderate:** Many of the critical success factors have been achieved;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

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

ACQUISITION MANAGEMENT SCORECARD

Organizational Alignment and Leadership

Modest Progress

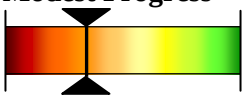


DHS' executive leadership has made "modest" progress in ensuring that the acquisition program achieves the organizational alignment needed to perform its functions. The department continues to face challenges associated with implementing an acquisition function that is not fully integrated. According to GAO,[1] the structure of DHS' acquisition function creates ambiguity about who is accountable for acquisition decisions. The Chief Procurement Officer (CPO) has used collaboration and cooperation with the components as the primary means of managing DHS-wide acquisition oversight. However, the CPO faces challenges in implementing the corrective actions, as they are only recommendations, and the component head determines what action will be taken.[2]

FEMA has made "modest" progress in aligning the acquisition function to serve as a partner, rather than a support function, for FEMA program offices. The Office of Acquisition Management (OAM) has created an Acquisition Program & Planning branch, which aligns acquisition personnel with program functions and will serve as the primary link between acquisitions and the program areas that generate requirements.[3] A major challenge is maintaining a sufficient acquisition workforce. In addition, OAM has experienced turnover of the senior leadership responsible for developing and communicating a strategic vision.

Policies and Processes

Modest Progress



DHS has made "modest" progress in developing policies and processes to ensure that components comply with regulations, policies, and processes to achieve department-wide goals. Previously, we reported that the department had begun implementation of its acquisition oversight plan, which incorporates DHS policy, internal controls, and elements of an effective acquisition function. However, the oversight program does not include an evaluation of outcomes from contracting methods such as performance-based acquisitions. According to GAO[4], the initial implementation of the plan has helped the components prioritize actions to address identified weaknesses, although it is too early to assess the plan's overall effectiveness.

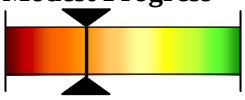
[1] GAO-07-948T, *Department of Homeland Security Ongoing Challenges in Creating an Effective Acquisition Organization*, June 2007.
[2] GAO-07-900, Department of Homeland Security, *Progress and Challenges in Implementing the Department's Acquisition Oversight Plan*, June 2007.
[3] DHS-OIG, *FEMA's Preparedness for the Next Catastrophic Disaster*, OIG-08-34, March 2008.
[4] GAO-08-646T, *Progress Made in Implementation of Management Functions, But More Work Remains*, April 2008.

ACQUISITION MANAGEMENT SCORECARD

FEMA has implemented the Virtual Acquisition Office ™ that provides an easily accessible, one-stop shop for useful acquisition guidance, and OAM has updated its *Emergency Acquisition Field Guide*. However, clear and transparent policies and processes for all acquisitions are still needed.

Acquisition Workforce

Modest Progress

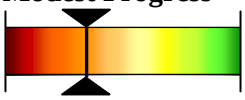


DHS has made "modest" progress in building and maintaining a skilled acquisition workforce. Previously, we reported that personnel budget increases had allowed the department to fill many acquisition staff positions. However, there are still workforce challenges across the department. GAO reported in April 2008 that approximately 61% of the minimum required staff and 38% of the optimal level of contract specialists were in place. Components within the department such as the U.S. Coast Guard (Coast Guard) have initiatives to develop and retain a workforce capable of managing complex acquisition programs, but they are still relying on contractors to fill key positions. DHS also needs to improve the tracking of its acquisition workforce training and qualifications to ensure workforce development and appropriate assignment to acquisition projects.

FEMA has significantly increased the number of its acquisition staff and has developed training initiatives for them. However, FEMA needs to focus on preparing the acquisition workforce to respond to a catastrophic disaster.

Knowledge Management and Information Systems

Modest Progress



DHS has made "modest" progress in developing and deploying information systems to track and analyze acquisition data and improve user efficiency. Some progress has been made in the integration of information systems. For example, according to the Coast Guard, it has completed the integration of three separate Coast Guard accounting systems into a single Acquisition, Construction, and Improvement data set that is usable by all Coast Guard acquisition personnel as part of its Blueprint for Acquisition Reform. However, the department and its components still need to improve database reliability and verification.

FEMA has made limited progress in providing staff with the tools they need to carry out their jobs. The outdated and nonintegrated information systems currently used by acquisition personnel were to be replaced by the PRISM contract-writing system in early 2008. The PRISM roll-out has now been pushed back to 2009. Until PRISM is instituted, acquisition personnel must use nonintegrated systems that require duplicate

ACQUISITION MANAGEMENT SCORECARD
input of data, thus increasing the possibility of errors. Logistics systems are not integrated with acquisition systems and do not provide complete asset visibility of disaster goods.[5]

FINANCIAL MANAGEMENT

DHS has continued to improve financial management in FY 2008, but challenges remain. As in previous years, our independent auditors were unable to provide an opinion on DHS' FY 2008 financial statements because the department could not provide sufficient evidence to support its financial statements or represent that financial statement balances were correct. The department has continued to remediate material weaknesses and has reduced the number of conditions that contribute to the disclaimer of opinion.

Although the Transportation Security Administration's (TSA) entity level controls deteriorated in FY 2008, the department made overall improvements in entity level controls at the departmental and component level. These improvements resulted in a reduction in the total number of material weaknesses from seven in FY 2007 to six in FY 2008. Even though new conditions were identified at FEMA and TSA, all components generally made progress in FY 2008.

As in FY 2007, the departmental material weaknesses in internal control were primarily attributable to the Coast Guard, FEMA, and TSA. The Coast Guard's material weaknesses, which have existed since 1994[6], contribute to all six of the department's material weaknesses, while FEMA contributes to four and TSA contributes to three. The Coast Guard also contributes to TSA's financial systems security material weakness due to TSA's reliance on the Coast Guard's financial systems. Although the other components did not have material weaknesses, some had significant deficiencies that, when combined, contributed to the departmental material weaknesses.

Financial Management Scorecard

The following scorecard presents the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2007. The scorecard is divided into two categories: (1) Military – Coast Guard and (2) Civilian – all other DHS components. The scorecard lists the seven material weaknesses and one other significant deficiency identified during the independent audit of the FY 2007 DHS consolidated balance sheet and statement of custodial activity. For a complete description of the internal control weaknesses identified in the FY 2007 audit, see OIG-08-12.[7] To determine the status, we compared the

[5] Statement of James L. Taylor, Deputy Inspector General, U.S. Department of Homeland Security, Before the Subcommittee on Management, Investigations, and Oversight, Committee on Homeland Security, U.S. House of Representatives, September 17, 2008; DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.
[6] DOT-OIG, *Significant Internal Control Weaknesses Identified in Audits of FY 1994 and 1995*, R3-CG-6-011, August 1996.
[7] DHS-OIG, *Independent Auditors' Report on DHS' FY 2007 Financial Statements*, OIG-08-12, November 2007.

material weaknesses reported by the independent auditor in FY 2007 with those reported in FY 2008. The scorecard does not include other financial reporting control deficiencies identified in FY 2008 that do not rise to the level of a significant deficiency, as defined by the American Institute of Certified Public Accountants. The ratings show that the department made some progress in FY 2008 toward remediation of the control weaknesses that were identified in FY 2007.

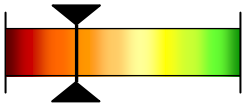
The ratings were based on a four-tiered scale ranging from limited to substantial progress as follows:

- **Limited:** While there may be plans to address internal control weaknesses, few if any have been remediated;
- **Modest:** While some improvements have been made, many of the internal control weaknesses have not yet been remediated;
- **Moderate:** Many of the internal control weaknesses have been remediated; and
- **Substantial:** Most or all of the internal control weaknesses have been remediated.

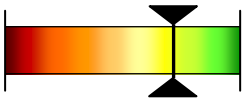
Based on the consolidated result of the seven financial management capability areas, DHS has made "modest" progress overall in the area of Financial Management.

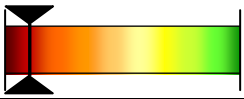
FINANCIAL MANAGEMENT SCORECARD		
Financial Management and Entity Level Control: Entity level controls are the foundation that ensures internal control systems are comprehensively designed to achieve the mission and execute the department's strategy.		
Military	**Modest Progress**	
	The Coast Guard made "modest" progress in addressing its internal control weaknesses related to financial management and entity level controls. In FY 2007, the independent auditor's report (IAR) noted that several conditions related to entity level control weakness also existed in prior years. For example, the Coast Guard did not fully implement a financial management organizational structure that incorporates U.S. generally accepted accounting principles or appropriately supports its financial statement balances. As a result, the Coast Guard could not assert to the completeness, existence (validity), accuracy, valuation, or presentation of its financial data. Although entity level control weaknesses continued to exist at the Coast Guard in FY 2008, some progress has been made. The FY 2008 IAR noted that the Coast Guard updated its Mission Action Plans in FY 2008 and created the *Financial Strategy for Transformation and Audit Remediation* (FSTAR). The FSTAR is a comprehensive plan to identify and correct the root causes of control deficiencies. However, most of the	

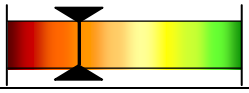
FINANCIAL MANAGEMENT SCORECARD		
	corrective actions outlined in the FSTAR were not scheduled to begin in FY 2008. Consequently, most of the entity level control weaknesses identified during FY 2007 continued to exist during FY 2008. The conditions noted at the Coast Guard contributed to an overall significant deficiency in entity level control at the department for FY 2008.	
Civilian	**Moderate Progress**	
	Overall, DHS has demonstrated "moderate" progress in establishing a financial management organization structure to enforce accountability and institute internal controls into the department's culture. As a result, DHS has remediated the severity of this condition from a material weakness to a significant deficiency with Coast Guard, FEMA, and TSA contributing to this condition. However, while FEMA was the only civilian component that contributed to the material weakness in FY 2007, there is now one additional component (TSA) contributing to a significant deficiency in FY 2008. The department has undertaken and completed several steps designed to strengthen its entity and process level internal controls, thereby improving the reliability of financial reporting. These steps are documented in the DHS FY 2008 *Internal Control Playbook*, released in March 2008, and in component level Mission Action Plans finalized in FY 2008. During FY 2007, a number of internal control weaknesses related to financial management and entity level controls at FEMA rose to a material weakness at the DHS consolidated financial statement level. Among other conditions, the independent auditors noted that FEMA had not established a financial management organization structure with clear oversight and supervisory review functions that support the development and implementation of effective policies, procedures, and internal controls over financial reporting. Such policies, procedures, and controls are needed to ensure that accounting principles are correctly applied and accurate financial data is submitted to the Office of Financial Management for consolidation in a timely manner. FEMA has made "modest" progress toward correcting its entity level control deficiencies. During FY 2008, the independent auditors noted that FEMA developed Mission Action Plans to eliminate account balance qualifications identified in the IAR in FY 2007. However, some entity level control deficiencies identified in previous years continued to exist throughout FY 2008.	

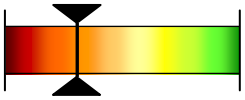
FINANCIAL MANAGEMENT SCORECARD	
	During FY 2008, TSA successfully addressed some account balance discrepancies and control deficiencies that contributed to the disclaimer of opinion on DHS' financial statements. However, during the FY 2008 audit, additional deficiencies that are indicative of weaknesses in entity level controls were identified at TSA.
Financial Reporting: Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period. The Federal Financial Management Improvement Act emphasizes the need for agencies to have systems that can generate timely, reliable, and useful information with which to make informed decisions to ensure ongoing accountability.	
Military	**Limited Progress** 
	The Coast Guard has demonstrated "limited" progress in remediating the numerous internal control weaknesses identified by the independent auditors during FY 2007. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2007 included: 1) lack of an effective general ledger system; and 2) lack of effective policies, procedures, and controls surrounding the financial reporting process. Although the Coast Guard developed its FSTAR during FY 2008, most of the corrective actions outlined in the document are scheduled to occur after FY 2008. Consequently, the Coast Guard was unable to make substantial progress in correcting the control weaknesses that were reported in prior years, and a material weakness still existed in FY 2008.
Civilian	**Modest Progress** 
	During FY 2008, DHS made "modest" progress in correcting the conditions that contributed to the material weakness in financial reporting in FY 2007**.** In FY 2007, conditions at the Office of Financial Management and FEMA rose to a level of material weakness, and conditions at TSA were considered a significant deficiency. During FY 2008, the Office of Financial Management fully corrected its material weakness over financial reporting, and FEMA made substantial progress toward correcting four material weaknesses that were reported in FY 2007. However, while FEMA has taken positive steps in FY 2008, some control weaknesses related to financial reporting continued to exist throughout FY 2008. These conditions at FEMA in the aggregate are considered a material weakness. In FY 2007, TSA adopted a two-year corrective action plan to address its financial reporting and other

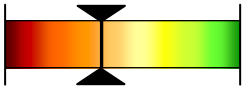
FINANCIAL MANAGEMENT SCORECARD		
	accounting internal control weaknesses. This resulted in TSA making some progress in the development of its core accounting processes throughout FY 2008. However, the independent auditors noted additional and more serious financial reporting control weaknesses, some of which have existed since the agency's inception. As a result, the severity of the condition worsened in FY 2008 and TSA now has a material weakness condition in financial reporting at the department level.	
Financial Systems Security: Financial systems security is essential to achieving effective, reliable reporting of financial and performance data.		
Military	**Limited Progress**	
	The Coast Guard has made "limited" progress in correcting certain information technology (IT) general control weaknesses identified in previous years. During FY 2007 significant control deficiencies included: 1) excessive access to key Coast Guard financial applications, 2) application change control processes that are not adequately designed nor operating effectively, 3) entity-wide security program issues involving personnel background checks, 4) system software weaknesses involving patch management, 5) segregation of duties involving lack of policies and procedures and excessive privilege access issues, and 6) service continuity issues involving the lack of disaster recovery testing . Significant deficiencies in application change control processes are among the principle causes of the Coast Guard's inability to support its financial statement balances. In addition, the Coast Guard was not able to effectively prioritize and implement Corrective Action Plans to remediate the root cause of the IT general control weaknesses in 2007. Many of these weaknesses were inherited from system development activities that did not incorporate strong security controls during the initial implementation of the system over five years ago, and will take several years to fully address. These weaknesses exist in the documentation of processes, the implementation of adequate security controls over processes, and within financial systems. In FY 2008, the Coast Guard remediated approximately 48% of its prior year IT general controls weaknesses. Specifically, the Coast Guard has made progress in remediation of issues in the areas of segregation of duties, systems software, and service continuity. Although there has been an improvement in the remediation effort, significant issues with the Coast Guard's change control process continue to exist for its financial applications.	

FINANCIAL MANAGEMENT SCORECARD		
Civilian	**Moderate Progress**	
	The DHS Office of Chief Financial Officer and Office of Chief Information Officer (OCIO) have demonstrated moderate progress in improving their financial systems security. In FY 2007, two civilian components contributed to the financial systems security material weakness. Significant control deficiencies were noted in the areas of access controls, application change control and service continuity. In FY 2008, these two components continued to contribute to this material weakness although one component did make improvements in the area of service continuity. Overall improvements in the Federal Information System Controls Audit Manual domains for all civilian components resulted in the closing of approximately 43 % of the IT general control findings identified in FY 2007. One component however, continues to show significant weaknesses in the areas of access controls and application change controls for its financial systems. In addition, results of a performance audit conducted in FY 2008 noted that the OCIO's Plan of Action and Milestones process does not contain actionable steps to remediate the issues or address the root cause of the material weakness. In addition, Plans of Action and Milestones are not consistently updated, and there is no correlation between the OCIO's Plan of Action and Milestones and the Office of the Chief Financial Officer's OMB A-123 strategy.	
Fund Balance with Treasury (FBwT): FBwT represents accounts held at Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency's FBwT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of various U.S Government financial reports, and providing a more accurate measurement of budget resources.		
Military	**Limited Progress**	
	The Coast Guard has demonstrated "limited" progress in addressing the material weaknesses noted in this area in FY 2007. Some of the conditions noted in FY 2007 included: 1) lack of adequate supporting documentation that validated the accuracy of all of the Coast Guard FBwT reconciliations; 2) lack of an effective process for accounting for suspense account transactions related to FBwT; 3) the Coast Guard's inability to provide validated military and civilian payroll data to support payroll transactions processed through the Coast Guard's FBwT account.	

FINANCIAL MANAGEMENT SCORECARD		
	In FY 2008, the Coast Guard developed a remediation plan (FSTAR) to address the control deficiencies. However, most of the corrective actions noted in the plan are scheduled to occur after FY 2008, thus, many of the conditions identified in FY 2007 continued to exist throughout FY 2008. These control weaknesses at the Coast Guard resulted in an overall material weakness for the Department in FY 2008, as FBwT at the Coast Guard represented approximately 8.3 % of total DHS FBwT at the end of FY 2008.	
Civilian	**Substantial Progress**	
	No control deficiencies related to FBwT were noted at the civilian components in FY 2007. Corrective actions implemented in previous years continued to be effective throughout FY 2007 and FY 2008.	
Capital Assets and Supplies: DHS capital assets and supplies consist of items such as property, plant and equipment, operating materials, and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.		
Military	**Limited Progress**	
	The Coast Guard has demonstrated "limited" progress in remediating the control deficiencies related to capital assets and supplies in FY 2008. The Coast Guard maintains approximately 60% of all DHS' property, plant, and equipment (PP&E), which includes a large fleet of boat and vessels. Since many of the Coast Guard's assets are constructed over a multi-year period, have long useful lives, and undergo extensive routine servicing that may increase their value or extend their useful lives, comprehensive policies and procedures are necessary to accurately and timely account for these assets. In FY 2007, as in prior years, the independent auditors noted that the Coast Guard has been unable to provide auditable documentation for certain categories of PP&E due to a number of policy, control, and process deficiencies that will require several years to correct. Many of these conditions still existed throughout FY 2008. In FY 2008, the Coast Guard developed corrective action plans (FSTAR) to address the PP&E process and control deficiencies, and began remediation efforts. However, the corrective actions included in the FSTAR are scheduled to occur over a number of years. Consequently, most of the material weakness conditions cited in FY 2007 remained throughout FY 2008.	

FINANCIAL MANAGEMENT SCORECARD		
Civilian	**Modest Progress**	
	Overall, the civilian components demonstrated "modest" progress in addressing the conditions identified in this area in FY 2007. In FY 2007, three civilian components contributed to a material weakness in capital assets and supplies. In FY 2007, conditions reported at FEMA rose to a level of material weakness, and significant deficiency at TSA and US-VISIT. During FY 2008, FEMA and US-VISIT were able to fully remediate the conditions leading to the material weaknesses identified in FY 2007. However, FEMA was unable to assert to the validity of internal use software and as a result, continues to contribute to the capital assets and supplies material weakness at the departmental level. Additionally in response to auditor inquires, TSA initiated various reviews of its capital assets and identified errors in its accounting for equipment used in airports that required a number of restatements to the FY 2007 financial statement balances, and current year corrections. As a result, TSA was unable to assert to the validity of capital assets and supplies and contributes to the qualification of the financial statements and material weaknesses at the department level. Also, new control weaknesses were identified at Customs and Border Protection (CBP) which were considered a significant deficiency. CBP's internal control deficiencies in this area are primarily related to construction of a fence along the border of the United States and Mexico. The FY 2008 IAR noted that CBP had expensed construction cost instead of capitalizing it as construction-in-progress.	
Actuarial and Other Liabilities: Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including accounts and grants payable, and legal and actuarial, and environmental liabilities.		
Military	**Limited Progress**	
	The Coast Guard maintains pension, medical, and postemployment travel benefit programs that require actuarial computations to record related liabilities for financial reporting purposes. Other liabilities include accounts payable, environmental, and legal liabilities. During FY 2008, the Coast Guard made "limited" progress in	

FINANCIAL MANAGEMENT SCORECARD		
	remediating the conditions that contributed to the material weakness in this area. Control deficiencies identified by the independent auditors in FY 2007 and prior years continued to exist in FY 2008. For example, the FY 2008 IAR on DHS financial statements noted that the Coast Guard did not have effective policies, procedures, and controls to ensure the completeness and accuracy of participant, medical cost and other data provided to the actuary for the calculation of related benefit liabilities.	
Civilian	**Modest Progress**	
	Overall, the department demonstrated "modest" progress in this area. During FY 2008, TSA fully corrected the control weaknesses that contributed to a significant deficiency in this area in the prior year. Additionally, conditions at FEMA were reduced to significant deficiency (from material weakness in FY 2007). However, new control weaknesses that rise to the level significant deficiency were identified at three additional civilian components. For FY 2008, the auditors noted that FEMA had not established a reliable method to estimate certain accounts payable for accrual in the financial statements until the end of the fiscal year. Additionally, for FY 2008 the Federal Law Enforcement Training Center, Immigration and Customs Enforcement (ICE), and Science and Technology components did not fully implement policies and standard operating procedures that will allow management to assert that environmental liabilities have been recorded and disclosed in the financial statements in accordance with applicable accounting standards. In the aggregate, the significant deficiencies at the four components and the material weakness at the Coast Guard amount to an overall material weakness for the department.	
Budgetary Accounting: Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded. Since the department received a disclaimer of opinion in FY 07, the audit is limited to the balance sheet and statement of custodial activity. As a result, audit coverage over budgetary accounts is limited to undelivered orders.		
Military	**Limited Progress**	

FINANCIAL MANAGEMENT SCORECARD		
	The Coast Guard has made "limited" progress in this area. Many of the internal control weaknesses that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2007 remained throughout FY 2008. For example, the FY 2007 IAR noted that the policies, procedures, and internal controls over the Coast Guard's process for validation and verification of some account balances are not effective to ensure that recorded amounts are complete, valid, accurate, and that proper approvals and supporting documentation is maintained. This condition also existed during FY 2008. While some issues may take a number of years to be corrected, several of the budgetary control weaknesses can be corrected by process improvements and strengthened policies and internal controls.	
Civilian	**Modest Progress**	
	DHS has demonstrated "modest" progress in remediating internal control weaknesses that were noted in the FY 2007 IAR. During FY 2008, TSA corrected its material weakness in this area. However, DHS' biggest challenge in this area remains at FEMA. In FY 2008, FEMA implemented corrective actions and performed an extensive review of its open obligations, including disaster relief and response mission assignments with other federal agencies. As a result, FEMA was able to deobligate over $1 billion in funds prior to year-end, and make those funds available for FY 2008 disaster relief. FEMA also improved its processes and internal controls over the mission assignment obligation and monitoring process in FY 2008; however, significant control deficiencies remain. As a result, the departmental level material weakness condition remains at FEMA. Additionally, CBP did not enforce its policies and procedures to monitor and deobligate or closeout its obligations in a timely manner. In response to an audit inquiry, CBP initiated a review of open obligations and subsequently deobligated approximately $84 million in open obligations in FY 2008. As a result, CBP has a significant deficiency condition related to budgetary accounting and contributes to the departmental level material weakness.	

INFORMATION TECHNOLOGY MANAGEMENT

Creating a unified IT infrastructure for effective integration and agency-wide management of IT assets and programs remains a challenge for the DHS Chief Information Officer (CIO). In September 2008, we reported that DHS had taken steps to strengthen the CIO's role for

centralized management of IT by providing greater authority and responsibility for overseeing component CIOs' IT acquisitions.[8] As a result, the DHS CIO is better positioned to govern the department's IT investments and resources. However, continued CIO staffing shortages and inconsistent component-level IT budget practices hinder the DHS CIO's ability to fully integrate department-wide IT programs. We recommended that the DHS CIO update the CIO office's staffing plan, ensure that components submit comprehensive budgets, and develop and maintain IT strategic plans and enterprise architectures aligned with DHS' mission.

DHS also faces challenges in meeting OMB's requirement to transition to a new internet protocol, IPv6, which supports an unlimited number of IP addresses and other enhanced capabilities.[9] Although DHS is in the early stages of the transition, the department is unlikely to be positioned to take timely advantage of the enhanced capabilities of IPv6. DHS must also ensure that several key activities, such as establishing a comprehensive inventory of all IPv6 devices, finalizing its IPv6 transition strategy, and engaging its components in IPv6 transition planning and activities, are completed before it can fully transition to IPv6 functionality.

Security of IT Infrastructure

During our FY 2007 *Federal Information Security Management Act*[10] (FISMA) evaluation of the department's intelligence systems, we reported that much progress had been made in establishing an enterprise-wide IT security program that supports the department's intelligence operations and assets. However, procedural and operational issues remained regarding the implementation of the department's intelligence security program and system controls.[11]

We also reviewed Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. The purpose of HSPD-12 is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors. The department is scheduled to complete its HSPD-12 implementation in 2010, two years after OMB's mandated deadline for all agencies.

In September 2008, we reported that components have not implemented appropriate security controls to enforce the department's policies on the acceptable use of portable storage devices.[12] The proliferation and uncontrolled use of portable storage devices (e.g., flash

[8] DHS-OIG, *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain*, OIG-08-91, September 2008.
[9] In August 2005 OMB issued Memorandum 05-22 (M-05-22), *Transition Planning for Internet Protocol Version 6* (IPv6), establishing the goal of transitioning federal agencies' wide area networks to IPv6.
[10] Title III of the 2002 E-Government Act, Public Law 107-347
[11] DHS-OIG, *Challenges Remain in Executing the Department of Homeland Security's Information Technology Program for Its Intelligence Systems*, OIG-08-48, April 2008.
[12] DHS-OIG, *Review of DHS Security Program for Portable Storage Devices*, OIG-08-95, September 2008.

drives, external hard drives, and portable music players) increases the risk of theft and mishandling of sensitive information.

DHS Component IT Management

Although improvements have been made, DHS continues to struggle with agency-wide IT management, planning, and investment, which has resulted in limited system integration and data sharing. For example, in October 2007, we reported that due to a lack of authority and standard policies to govern technology implementation, TSA's CIO faces significant challenges in conducting agency-wide IT planning and investment management. We concluded that TSA's IT management could be strengthened by empowering the CIO with IT budget authority, developing an agency-wide strategic planning approach, implementing an enterprise architecture, establishing guidelines to manage IT development, and increasing staff resources within the IT division.

Similarly, our April 2008 assessment of FEMA's efforts to upgrade its disaster logistics management systems[13] showed that, although the agency has made short-term progress in addressing disaster goods procurement and delivery during disasters, more remains to be done to address long-term planning and systems integration needs. FEMA has taken steps to improve its logistics capabilities by gathering independent evaluations to assess its existing systems, identify IT systems requirements, and select technologies to meet its logistics needs. However, existing systems do not provide complete asset visibility, comprehensive asset management, or integrated logistics information. We recommended that FEMA finalize its logistics strategy and operational plans, develop standard business processes and procedures for logistics activities, evaluate current technologies, and develop a strategy for acquiring IT systems to support the logistics mission.

Privacy

DHS still faces challenges in ensuring that privacy concerns are addressed throughout the lifecycle of each program and information system that contains sensitive personally identifiable information. According to the *E-Government Act of 2002*, federal agencies must conduct a Privacy Impact Assessment (PIA) for each new or substantially changed IT system that collects, uses, maintains, or disseminates personally identifiable information, demonstrating that they have incorporated privacy safeguards throughout the development lifecycle of their programs or systems. Although DHS requires PIAs at the very earliest stage of a project or before beginning a pilot test, DHS officials did not conduct risk assessments in a number of IT system implementations.[14]

In April 2008, we reported that the Intelligence and Analysis' National Applications Office (NAO) had made progress by involving the DHS Privacy Office early in its privacy program planning and development of key organizational documents. However, a revised PIA and a

[13] DHS-OIG, *Logistics Information Systems Need to be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.
[14] DHS Privacy Office, *Privacy Impact Assessment Guidance*, May 2007.

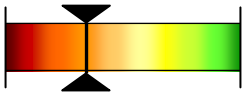
Civil Liberties Impact Assessment reflecting changes in NAO's Charter and proposed operations were also necessary before NAO become operational.[15]

IT Management Scorecard

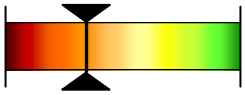
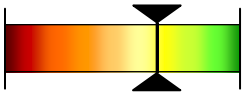
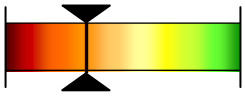
The following scorecard demonstrates where IT management functions of the DHS CIO and the seven largest DHS component-level CIO offices have been strengthened. This high-level assessment identifies progress in six IT management capability areas: IT budget oversight, IT strategic planning, enterprise architecture, portfolio management, capital planning and investment control, and IT security. These six elements were selected based on IT management capabilities required by federal and DHS guidelines for enabling CIOs to manage IT department-wide. The ratings were based on a four-tiered scale ranging from limited to substantial progress:

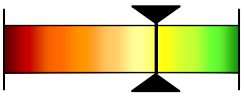
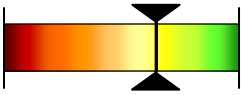
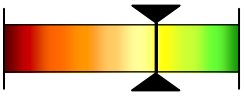
- **Limited:** Plans are in place for this capability, but the capability has not been fully implemented;
- **Modest:** The capability is partially implemented, with limited IT management benefits realized;
- **Moderate:** The capability is implemented with moderate IT management benefits realized; and
- **Substantial:** The capability is implemented with substantial IT management benefits realized.

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

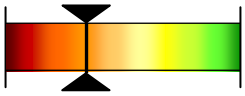
IT MANAGEMENT SCORECARD		
IT Budget Oversight: ensures visibility into IT spending and alignment with the strategic IT direction.		
DHS CIO	**Modest Progress**	
	The DHS CIO has made improvements in managing department-wide IT budgets in accordance with the *Clinger-Cohen Act* and the department's mission and policy guidance. The DHS CIO plans to conduct reviews across the department of all investments that contain IT assets and services. The goals for IT budget reviews are to resolve IT budget issues prior to OMB submission, align IT investments with targets and priorities, and eliminate redundancies. Progress in this area was further evidenced by the FY 2010 IT budget planning guidance, issued in January 2008, on better integrating component IT resource reviews with DHS program and budget reviews. With support of DHS leadership, the	

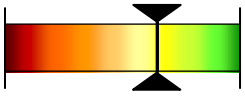
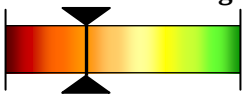
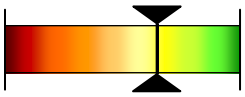
[15] DHS-OIG, *National Applications Office Privacy Stewardship*, OIG-08-35, April 2008.

IT MANAGEMENT SCORECARD		
	DHS OCIO will continue to focus on improving IT budget capabilities.	
Component CIOs	**Modest Progress**	
	Overall, components demonstrated "modest" progress in conducting IT budget planning and programming functions. Although component-level IT budget responsibilities have increased through *DHS Management Directive* 0007.1, more than 70% of DHS component CIOs remain hindered by ineffective, decentralized IT budget practices. Most component CIOs plan to further centralize existing IT budget functions to meet requirements in the management directive to prepare a component IT budget. A number of DHS components are implementing initiatives to increase centralized management of IT investments by restructuring and consolidating IT spending accounts that are currently managed by separate offices throughout the agency.	
IT Strategic Planning: helps align the IT organization to support mission and business priorities.		
DHS CIO	**Moderate Progress**	
	Per OMB Circular A-130, an effective IT strategic plan establishes an approach to align resources and provides a basis for articulating how the IT organization will develop and deliver capabilities to support mission and business priorities. The DHS OCIO has made progress aligning IT with department goals. Although the current IT strategic planning approach does not fully link technology to mission requirements, the OCIO plans to achieve strategic outcomes and stronger IT alignment with the Secretary's goals. The OCIO is currently updating DHS' IT strategic plan and has communicated the plan's goals to the CIO Council.	
Component CIOs	**Modest Progress**	
	As of January 2008, approximately 70% of the component-level CIOs had developed an IT strategic plan as required by *Management Directive* 0007.1. However, not all components can consistently link strategic goals and objectives with IT investments. Further, although some component CIOs said that they had developed an IT strategic plan, not all are up-to-date. Improvements are planned by some component CIOs who are updating their IT strategic plans. However, until the improvements are made, the agency may fall short of its potential to improve business processes and systems.	

IT MANAGEMENT SCORECARD		
Enterprise Architecture: functions as a blueprint to guide IT investments for the organization.		
DHS CIO	**Moderate Progress**	
	The *Clinger-Cohen Act*[16] requires that CIOs develop and implement an integrated IT architecture for the agency to avoid the risk that systems will be duplicative, not well integrated, and limited in optimizing mission performance. The DHS-level enterprise architecture has advanced greatly as an effective tool for reviews and IT management decision-making. Overall, the DHS OCIO has increased its ability to enforce architecture alignment through *Management Directive* 0007.1. Significant progress is due in part to the IT Acquisition Review process, which has helped promote and enforce such alignment. The OCIO plans to mature and optimize the department's architecture through performance-based outcomes and to develop the data architecture further in mission-critical areas.	
Component CIOs	**Moderate Progress**	
	Management Directive 0007.1 requires component CIOs to implement a detailed enterprise architecture specific to the component's mission and in support of DHS' mission. As of January 2008, more than 70% of the component-level CIOs could align IT investments with the department's architecture. Most components have component-level architectures used for some degree of IT investment decision-making. However, architecture products, such as reference models, definitions of current and future state architectures, and transition plans are in varying stages of development or use. A number of components said that their architecture products were out of date or needed to be better defined.	
Portfolio Management: improves leadership's ability to understand interrelationships between IT investments and department priorities and goals.		
DHS CIO	**Moderate Progress**	
	The DHS OCIO has made "moderate" progress in establishing the department's portfolio management capabilities as instructed by OMB Circular A-130.[17] The DHS portfolio management program aims to	

[16] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.
[17] Revision of Office of Management and Budget Circular A-130, Transmittal 4, *Management of Federal Information Resources*, July 1994.

IT MANAGEMENT SCORECARD		
	group related IT investments into defined capability areas to support strategic goals and missions. Portfolio management improves leadership's visibility into relationships among IT assets and department mission and goals across organizational boundaries. The DHS OCIO has a solid plan in place to implement portfolio management capabilities in FY 2008. The OCIO has recently finalized plans, along with the first round of documentation and guidance, for a department-level portfolio management approach. Currently, there are 22 defined portfolio areas, six of which are considered priority areas: infrastructure, geospatial, case management, human resources, screening and credentialing, and finance. In addition, OCIO has created a portfolio management integrated project team to develop transition plans, measure performance, and standardize the portfolio management process. Although progress is being made, the department is not yet realizing management benefits from the portfolio management program. As a result, the department may miss opportunities for system integration and cost savings.	
Component CIOs	**Modest Progress**	
	Overall, DHS components have made "modest" progress in establishing portfolio management capabilities. Full implementation of this capability remains a work in progress, due in part to challenges in creating and aligning component-specific portfolios with DHS' 22 portfolios. Most DHS component-level CIOs have developed a mapping approach to align component IT systems with DHS-level portfolios. Many CIOs said that it is a complicated process to align their unique mission and business processes with multiple DHS-level IT portfolios. For example, Coast Guard officials said that they are working with DHS OCIO officials to determine which portfolios will be associated with each of the systems they identified in the IT budget review. Until this capability is fully implemented, DHS components may continue to invest in systems within organizational silos, limiting opportunities for consolidation and cost savings.	

IT MANAGEMENT SCORECARD		
Capital Planning and Investment Control: improves the allocation of resources to benefit the strategic needs of the department.		
DHS CIO	**Moderate Progress**	
	The *Clinger-Cohen Act* requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning. Through such efforts, in FY 2007, the 94 DHS programs on the management watch list were reduced to 18. In FY 2008, 53 programs are listed. Officials in the OCIO have sought to remove these programs from the list by working with the program managers through the CPIC Administrator's bimonthly meetings.	
Component CIOs	**Modest Progress**	**Modest Progress** 
	Most components have not yet achieved an integrated planning and investment management capability. More than 70% of the major DHS components had limited capital planning processes outside the existing OMB 300 process. However, some component CIOs said that they are creating a CPIC process to integrate with existing governance structures such as the Investment Review Board. For example, the ICE Investment Review Board resembles a CPIC group, incorporating major areas such as security, budget, and enterprise architecture. The ICE CIO said that this process has helped components leverage resources more effectively.	
IT Security: ensures protection that is commensurate with the harm that would result from unauthorized access to information.		
DHS CIO	**Moderate Progress**	
	DHS IT security is rated at "moderate," for progress made during the last 2 years in compliance with FISMA. OMB Circular A-130 requires agencies to provide protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to information and systems assets or their loss, misuse**,** or modification. The DHS CIO has taken an active role in ensuring that components comply with FISMA. In 2007, the CIO requested that components focus on improving areas such as certification and accreditation, annual self-	

IT MANAGEMENT SCORECARD	
	assessments, and plan of action and milestones management. According to the DHS OCIO, additional quality control measures have been implemented manage the certification and accreditation process better. The DHS OCIO also plans to focus on improving disaster recovery and continuity of operations over the coming year.
	(Components were not rated on IT Security)

CATASTROPHIC DISASTER RESPONSE AND RECOVERY

The primary mission of FEMA is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. FEMA does this by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation.

In March 2008, we released a report on FEMA's progress in addressing nine key preparedness areas related to catastrophic disasters.[18] FEMA made moderate progress in five of the nine areas: overall planning, coordination and support, interoperable communications, logistics, and acquisition management. FEMA made modest progress in evacuation, housing, and disaster workforce, and limited progress in mission assignments. (Please see the catastrophic disaster response and recovery scorecard below for a discussion of selected areas.) Our broader recommendations addressed the improvements needed in overall planning, coordination, and communications. FEMA officials said that budget shortfalls, reorganizations, inadequate IT systems, and confusing or limited authorities impeded their progress.

In FY 2009, we will continue to conduct studies regarding FEMA's preparedness, response, and recovery efforts. These studies will allow us to further assess FEMA's progress in transforming itself to be better prepared to lead the federal effort in responding to a catastrophic disaster.

Catastrophic Disaster Response and Recovery Scorecard

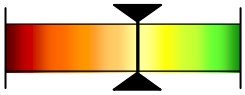
The following scorecard highlights FEMA's progress in six key areas: logistics, evacuations, housing, disaster workforce, mission assignments, and acquisition management. The ratings were based on a four-tiered scale ranging from limited to substantial progress:

- **Limited**: There is an awareness of the critical issues needing to be addressed, but specific corrective actions have not been identified;
- **Modest**: corrective actions have been identified, but implementation is not yet underway;

[18] DHS-OIG, *FEMA's Preparedness for the Next Catastrophic Disaster*, OIG-08-34, March 2008.

- **Moderate**: Implementation of corrective action is underway, but few if any have been completed; and
- **Substantial**: Most or all of the corrective actions have been implemented.

Based on the consolidated result of the six areas, FEMA has made "moderate" progress in the area of catastrophic disaster response and recovery.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD	
Logistics	**Moderate Progress** 

The mission of FEMA's Logistics Management Directorate is to plan, manage, and sustain the national logistics response and recovery operations in support of domestic emergencies. FEMA has made "moderate" progress in meeting its logistics responsibilities such as acquiring, receiving, storing, shipping, tracking, sustaining, and recovering commodities, assets, and property in the event of a catastrophic disaster.

The *Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act)* [19] requires FEMA to develop a logistics system that provides visibility of disaster goods from procurement to delivery. FEMA has not yet met this requirement. FEMA's total asset visibility system is unable to track goods from warehouses to staging areas to distribution sites. Nor can it track goods received from federal and nonfederal partners. FEMA needs to finalize its logistics plans, implement standardized processes and procedures for logistics activities, and develop a strategy for acquiring IT systems to support the logistics mission.[20]

Determining the types and quantities of commodities that FEMA may need in the aftermath of a disaster is a continuing challenge. In 2005, FEMA was criticized for having too few commodities available in the aftermath of Hurricane Katrina. In 2006, FEMA acquired inventory that was not needed during the mild hurricane season, resulting in waste. In-depth analysis of this issue resulted in FEMA's determination that pre-positioning commodities is neither logistically prudent nor an effective use of taxpayer funds. Instead, FEMA plans to rely on public and private sector partners to provide needed items. FEMA appears to have made progress in developing these partnerships, as well as working more closely with states to determine where state shortfalls are likely to occur.

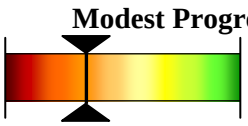
A Distribution Management Strategy Working Group is developing and documenting an integrated national policy and strategy for managing and controlling inventory,

[19] Public Law 109-295, Title VI – National Emergency Management, *Department of Homeland Security Appropriations Act of 2007*.
[20] DHS-OIG, *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

positioning commodities, and distributing critical resources. In the past, FEMA has been prone to drafting strategies, policies, and procedures that were never finalized. FEMA leadership should ensure that this Working Group proposes strategies and policies in a timely manner and that these proposals are promptly reviewed, finalized, and implemented.

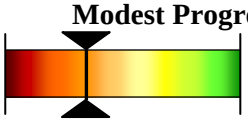
Evacuations



The conduct of evacuation operations is generally a state, tribal, and local responsibility. However, some circumstances exceed the capabilities of those jurisdictions to support mass evacuations. Where federal support is required, FEMA coordinates the support with the affected state, local and tribal governments. Federal support is scaled to the incident level and may be provided in the form of cost reimbursement or direct assistance, for example, providing buses, trains, and air ambulances for evacuation.

FEMA has a number of initiatives underway for improving evacuation management capabilities and published a *Mass Evacuation Incident Annex* describing evacuation functions and agency roles and responsibilities in mass evacuations. However, no single entity within FEMA is responsible for emergency evacuation planning or operations. FEMA has not yet developed a single national system to support multistate, state-managed, or local evacuation operations. Coordinating transportation for evacuees during emergencies, collaborating with states to receive and accommodate the needs of evacuees, and ensuring that dedicated resources are available to support evacuation plans, remain significant challenges.

Housing



Although improvements have been made, disaster housing remains a major challenge, as demonstrated by the results of our recent audits of FEMA housing programs and initiatives. Issues with accountability, management, and disposal of emergency housing units persist. Plans for addressing catastrophic disaster housing needs must be developed and tested. As we have learned from past and recent disasters, not being prepared with a full range of housing options has significant implications for evacuees and the states and communities that host them.

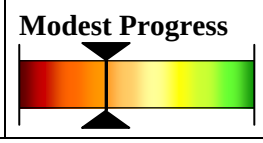
In March 2008, we reported that FEMA had made modest progress in the key preparedness area of housing. While FEMA is striving to improve its disaster housing assistance strategy and coordination, it needs to develop and test innovative catastrophic disaster housing plans to deal with large-scale displacement of citizens for extended periods, where traditional housing programs have been shown to be inefficient, ineffective, and costly.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

In October 2008, we reported that FEMA's strategy for ending its direct housing assistance program is generally sound, and that FEMA has made considerable progress recovering temporary housing units in the Gulf Coast region.[21] However, FEMA's strategy is not complete since FEMA's strategy has not recertified resident eligibility or taken action to recover temporary housing units from ineligible residents. FEMA must implement the recertification of eligibility process to ensure recovery of all temporary housing units by March 1, 2009, which is the ending date of FEMA's direct housing assistance program for hurricanes Katrina and Rita.

The Post-Katrina Act requires FEMA to develop, coordinate, and maintain a National Disaster Housing Strategy (NDHS). FEMA released the draft NDHS for a 60-day public comment period in July 2008. We are currently conducting a review of FEMA's future housing strategies and are reviewing the NDHS as part of this effort. FEMA must move forward with a finalized strategy to guide future disaster housing efforts.

Disaster Workforce



A trained, effective disaster workforce is one of the most effective tools FEMA has to meet its mission. FEMA's disaster workforce consists mainly of reservists who serve temporarily during a disaster, with no employee benefits. During the 2005 Gulf Coast hurricanes, FEMA struggled to provide qualified staff and did not have the automated support to deploy more than 5,000 disaster personnel on short notice. As FEMA evolves, its disaster workforce strategy, structure, and systems need to keep pace.

To date, FEMA has not completed or has not been able to verify the completion of five of nine workforce-related actions required by the *Post-Katrina Act*. The five incomplete or unconfirmed actions are:

- Developing a Strategic Human Capital Plan;
- Establishing career paths;
- Conferring with state, local, and tribal government officials when selecting regional administrators;
- Training regional strike teams as a unit and equipping and staffing these teams; and
- Implementing a surge force capacity plan.

The congressionally mandated due dates for these actions range from March 2007 through July 2007.

[21] DHS-OIG, *FEMA's Exit Strategy for Temporary Housing in the Gulf Coast Region,* OIG-09-02, October 2008.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

Mission Assignments

Limited Progress

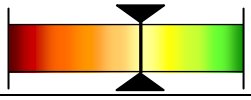
FEMA is responsible for coordinating the urgent, short-term emergency deployment of federal resources to address immediate threats and for stewardship of the associated expenditures from the Disaster Relief Fund. FEMA uses mission assignments to request disaster response support from other federal agencies. Past audits and reviews regarding mission assignments have concluded that FEMA's management controls were generally not adequate to ensure that:

- Deliverables (missions tasked) met requirements;
- Costs were reasonable;
- Invoices were accurate;
- Federal property and equipment were adequately accounted for or managed; and
- FEMA's interests were protected.

FEMA guidelines regarding the mission assignment process, from issuance of an assignment through execution and closeout, have never been fully developed, creating misunderstandings among federal agencies concerning mission assignment operational and fiduciary responsibilities. Implementing Section 693 of the *Post-Katrina Act*, which allows FEMA to designate up to 1% of the funds provided to federal agencies for disaster relief activities as oversight funds, will help ensure effective stewardship and oversight of monies the recipient agencies use for activities conducted under the FEMA reimbursable mission assignment process.

Acquisition Management (Catastrophic Disasters)

Moderate Progress



After a disaster, FEMA's tendency has been to acquire goods and services quickly, but with insufficient attention to costs, definition of requirements, and competition. To balance urgency of needs with good business practices, FEMA's OAM has awarded approximately 27 pre-disaster response contracts and 70 recovery contracts. Planning and negotiating these contracts in advance of a disaster provides more advantageous terms to the government and more opportunity for small and local businesses.

FEMA has found it difficult to recruit experienced acquisition staff. FEMA has increased its acquisition staff from just 35 when Hurricane Katrina struck to about 150 today. FEMA has also increased staffing and training of contracting officer's technical representatives (COTRs), who are responsible for technical contract oversight, inspecting goods, and approving invoices. However, staffing remains a challenge. The new acquisition personnel need training and experience in acquiring goods and services under emergency circumstances. Recent OIG reports recommended increased oversight of contractor actions and reviews of services and invoices by COTRs.

FEMA CATASTROPHIC DISASTER RESPONSE AND RECOVERY SCORECARD

FEMA needs to continue hiring and training acquisition personnel, allocating staff where the need is greatest among Headquarters and the 10 FEMA regional offices, and developing reliable, integrated financial and information systems.

GRANTS MANAGEMENT

Monitoring and documenting the effectiveness of DHS' multitude of grant programs poses an increasingly significant challenge for the department. DHS manages more than 80 disaster and non-disaster grant programs. This challenge is compounded by other federal agencies' grant programs that assist state and local governments in improving their abilities to prepare for, respond to, and recover from acts of terrorism or natural disasters. FEMA has yet to fully implement the April 2007 reorganization directed by the *Post Katrina Emergency Management Reform Act of 2006*. Most states are not sufficiently monitoring subgrantee compliance with grant terms and cannot clearly document critical improvements in preparedness as a result of grant awards.

During FY 2008, we issued audit reports on homeland security preparedness grant management by the states of New Jersey, Ohio, Michigan, Georgia, Florida, Utah, Arizona, and Washington. These states generally did an adequate job of administering the program requirements; however, the most prevalent areas needing improvement concerned the monitoring of subgrantees and controls over personal property and equipment.

We are concluding audits of the effectiveness of grant awards under the State Homeland Security Grant Program in California and Illinois. During the first quarter of FY 2009, we also anticipate issuing an audit mandated by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53) on FEMA's grant management and oversight practices.

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

INFRASTRUCTURE PROTECTION

DHS has direct responsibility for leading, integrating, and coordinating efforts to protect 10 critical infrastructure and key resources (CI/KR) sectors: the chemical industry; commercial

facilities; dams; emergency services; commercial nuclear reactors, materials, and waste; information technology; telecommunications; postal and shipping; transportation systems; and government facilities. In addition, DHS has an oversight role in coordinating the protection of seven sectors for which other federal agencies have primary responsibility.[22] The requirement to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI/KR. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the implementation of protection efforts is a great challenge.

In FY 2007, we reported several opportunities for DHS to improve its engagement of public and private partners and to prioritize resources and activities based on risk.[23] For example, a comprehensive national database that inventories assets is essential to provide a comprehensive picture of the Nation's CI/KR and to enable management and resource allocation decision-making. We are reviewing how DHS uses an asset database to support its risk management framework. We also plan to evaluate how DHS coordinates infrastructure protection with other sectors by reviewing the protection of petroleum and natural gas infrastructure within the energy sector.

Protecting national as well as internal cyber infrastructure continues to be a challenge for DHS. We recently reviewed the department's progress in identifying and prioritizing its internal cyber critical infrastructure in accordance with Homeland Security Presidential Directive 7.[24] This directive established a national policy for the federal government to identify, prioritize, and protect U.S. critical infrastructure, including the internal critical assets used by each department. We found that the department needs to take additional steps to produce a prioritized inventory and to coordinate related efforts to secure these assets. We recommend that the department assign responsibility and provide the resources necessary to determine protection priorities for its internal critical infrastructure, including critical cyber infrastructure. In addition, the department should develop a process to coordinate internal efforts to protect these assets. In FY 2009, we plan to review the National Cyber Security Division's strategy for control systems security and its Computer Emergency Readiness Team.

BORDER SECURITY

A principal DHS challenge is reducing America's vulnerability to terrorism by controlling the borders of the United States. To this end, DHS is implementing the Secure Border Initiative (SBI), a comprehensive multi-year program to secure the borders and reduce illegal immigration. The Coast Guard, U.S. Citizenship and Immigration Services, CBP, and ICE

[22] The seven sectors for which DHS has an oversight role are agriculture and food; the defense industrial base; energy; public health and healthcare; national monuments and icons; banking and finance; and water and water treatment systems.
[23] DHS OIG, *A Review of Homeland Security Activities Along a Segment of the Michigan-Canadian Border*, OIG-07-68, August 2007; *Review of the Buffer Zone Protection Program*, OIG-07-59, July 2007; *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, February 2007.
[24] DHS OIG, *Letter Report: DHS Needs to Prioritize Its Cyber Assets*, OIG-08-31, March 2008.

all have key roles in the SBI program. To ensure SBI success, it is critical that the program be thoroughly planned. DHS also must institute an approach to coordinating the SBI functions and activities of the participating DHS components with the related efforts of other agencies. We are conducting a series of audits to evaluate whether the SBI program initiatives are being accomplished in an economical, efficient, and effective manner.

The technology component of SBI, known as SBInet, involves the acquisition, development, integration, and deployment of surveillance systems. It also involves communications and intelligence technologies. In FY 2006, we recommended that CBP improve the effectiveness of remote surveillance technology to correct the lack of integration between border surveillance cameras and ground sensors, which were plagued by false alarms.[25] CBP has made some progress in improving surveillance and detection technology along the Southwest border via Project 28, which includes enhanced radars, sensors, and cameras. However, delays associated with software integration problems have required CBP to extend the completion dates for implementation from December 2008 to sometime in 2009. Consequently, Border Patrol Agents continue to use technology that predates SBInet and, in the Tucson, Arizona sector, they are still using capabilities from SBInet's prototype system despite previously reported performance shortfalls.[26]

The definition and management of requirements is another significant challenge for the SBI*net* program. According to GAO,[27] the SBI*net* program office issued guidance on the development and acquisition of software and systems that is consistent with recognized leading practices. However, this guidance was not finalized until February 2008, and thus was not used in performing a number of important requirements-related activities. For example, there is a lack of traceability among the different levels of requirements. This limits the program office's ability to determine whether the scope of the contractor's design, development, and testing efforts will produce a system that meets operational needs and performs as intended.

Also, efforts are needed to ensure that ICE can support its detention and removal operations. In our recent reviews of ICE's oversight of immigration detention facilities, we recommended that ICE improve its standards, strengthen its oversight of facilities, and enhance operations.[28] We are completing an audit of ICE's acquisition and management of "bed space" needs to support detention and removal operations.

[25] DHS-OIG, *A Review of Remote Surveillance Technology along U.S. Land Borders*, OIG-06-15, December 2005.
[26] GAO-08-1141T, *SBI Observations on Deployment Challenges*, September 2008.
[27] GAO-08-1086, *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, September 2008.
[28] DHS-OIG, *ICE Policies Related to Detainee Deaths and the Oversight of Immigration Detention Facilities*, OIG-08-52, June 2008; DHS-OIG, *ICE's Compliance with Detention Limits for Aliens with Final Order for Removal from the U.S.*, OIG-07-28, February 2007; DHS-OIG, *U.S. Immigration and Customs Enforcement's Detainee Tracking Process*, OIG-07-08, November 2006; DHS-OIG, *Treatment of Immigration Detainees Housed at Immigration and Customs Enforcement Facilities*, OIG-07-01, December 2006; *Detention and Removal of Illegal Aliens*, OIG-06-33, April 2006.

TRANSPORTATION SECURITY

The Nation's transportation system, which moves millions of passengers and tons of freight every day, is an attractive terrorist target and creates an enormous security challenge due to its size and complexity. TSA was originally created as a part of the Department of Transportation after September 11, 2001, to strengthen the security of the Nation's transportation systems, including aircraft, ships, rail, motor vehicles, airports, seaports, transshipment facilities, roads, railways, bridges, and pipelines. However, since its inception, TSA has focused on aviation.

Checkpoint and Checked Baggage Performance

The *Aviation and Transportation Security Act*[29] requires TSA to screen or inspect all passengers, goods, and property before entry into the sterile areas of an airport. Our undercover audits of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not carried into the sterile areas of heavily used airports and do not enter the checked baggage system. In past testing, we noted four areas that caused most of the test failures: training; equipment and technology; policies and procedures; and management and supervision. TSA agreed with our conclusion that significant improvements in screener performance will be possible only with the introduction of new technology. TSA plans to purchase 300 advanced technology x-rays and 80 passenger imagers. Currently TSA has 700 advanced x-rays and 40 passenger-imaging units deployed at 12 airports. We recently released a classified report on our penetration testing results, specifically at those airports with explosives trace portals and an airport that had a whole body imager, and found that improvements to effectively secure sterile airport areas are still needed.[30]

The OIG will continue to exercise oversight of TSA's performance and processes of checkpoint and checked baggage screening. We are currently in the process of conducting audits of TSA's controls over screener uniforms, badges, and identification cards, as well as the effectiveness of TSA's explosives detection systems on-screen alarm resolution protocol. These reports will be issued later this year.

Employee Workplace Issues

A stable, mature, and experienced TSA workforce is one of the most effective tools to meet the agency's mission. Despite the value of the TSA workforce, employees have expressed their concerns about how the agency operates by historically filing formal complaints at rates higher than other federal agencies of comparable size. Our audit of TSA's efforts to address employee concerns found that low employee morale continues to be an issue at some airports and has contributed to TSA's 17% voluntary attrition rate.[31]

[29] Public Law 107-71, November 19, 2001.
[30] DHS-OIG, *Airport Passenger and Checked Baggage Performance*, OIG-08-25, February 2008.
[31] DHS-OIG, *TSA's Efforts to Proactively Address Employee Concerns*, OIG-08-62, May 2008.

More than half the employees we interviewed described the agency's efforts to educate them on the various initiatives available to address their workplace concerns as "inadequate." We made six recommendations to the Assistant Secretary of TSA to provide employees with sufficient tools, including clear guidance and better communication, on the structures, authorities, and oversight responsibilities of the initiatives we reviewed. TSA fully or partly concurred with five of the recommendations and has taken action to resolve them.

Passenger Air Cargo Security

The vast and multifaceted U.S. air cargo system transports approximately 7,500 tons of cargo on passenger planes each day, making air cargo vulnerable to terrorist threats. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may *only* transport cargo originating from a shipper that is verifiably "known" either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. We are conducting an audit to assess how TSA ensures that cargo from unknown shippers is not being shipped on passenger planes. This report is expected to be issued later this year. During 2009, we also plan to audit TSA's cargo security measures during ground movement.

Rail and Mass Transit

Since the terrorist attacks of September 11, 2001, the London subway bombings, and the Madrid rail bombings, DHS has taken steps to manage risk and strengthen our Nation's rail and transit systems. While most mass transit systems in this country are owned and operated by state and local government or private industry, securing these systems is a shared responsibility among federal, state, and local partners.

DHS operates multiple programs, including several grants, to improve rail and mass transit security. In June 2008, we reported on TSA's efforts to secure mass transit through four major assistance programs: the Surface Transportation Security Inspection Program, Transit Security Grant Program, Visible Intermodal Prevention and Response program, and the deployment of canine explosive detection teams for rail.[32] TSA needs to clarify its transit rail mission, improve interoffice communication and coordination, develop memorandums of understanding with local transit authorities, and develop additional regulations. TSA also needs to understand and address system-specific security requirements better. We are completing mandates to review the effectiveness of the Trucking Industry Security Grant Program and to report further on the Surface Transportation Security Inspection Program.

During emergencies transit agencies must rely on well-designed and regularly practiced drills and exercises to respond and recover rapidly and effectively. Recent events on the rail systems in Washington DC, including a derailment and a fire, have raised questions regarding the mass transit agencies' contingency plans and the ability to handle these basic issues, as well as major emergencies. We will evaluate TSA's efforts to ensure that mass transit agencies are prepared to respond and recover from emergencies on passenger rail systems. We will review TSA's role in security program management and accountability,

[32] DHS-OIG, *TSA's Administration and Coordination of Mass Transit Security Programs*, OIG-08-66, June 2008.

security and emergency response training, drills and exercises, public awareness, and other protective measures for passenger rail systems.

TRADE OPERATIONS AND SECURITY

CBP is primarily responsible for trade operations and security, with the support of the Coast Guard and ICE. Each year, more than 16 million containers arrive in the United States by ship, truck, and rail. CBP typically processes more than 70,000 truck, rail, and sea containers per day, along with the personnel associated with moving this cargo across U.S. borders or to U.S. seaports. Modernizing trade systems, using resources efficiently, and managing and forging partnerships with foreign trade and customs organizations pose significant challenges for CBP and DHS.

CBP works with trade representatives to implement processes and systems to help secure the supply chain and uses targeting systems to identify the highest risk cargo on which to focus its limited resources. Recently, CBP increased its international efforts to secure the cargo supply chain by expanding its work with the Customs-Trade Partnership against Terrorism program and by improving its multi-layered security strategy.

The *Coast Guard and Maritime Transportation Act of 2004* (Public Law 108-293) requires us to evaluate and report annually on the effectiveness of the Automated Targeting System (ATS), which is an intranet-based enforcement and decision support tool used by CBP seaport inspectors to help determine which containers entering the country will undergo inspection. Our annual ATS review in 2008[33] focused on a subsystem of ATS, the Cargo Enforcement Reporting and Tracking System (CERTS), which is designed to gather data on cargo examination findings and report on how efficiently examination equipment is being used. We identified the need for improvements in planning, updating, developing, and implementing CERTS. Specifically, CBP needs to update the project plan to include the scope of work, and a detailed implementation schedule for system design, developing and testing, and cost estimates past phase one. In addition, CBP bypassed key life cycle reviews designed to ensure that end users have a properly working system and have received management's approval to continue the project.

The Coast Guard is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. Our most recent annual review of mission performance[34] revealed that the Coast Guard must make several improvements to implement the *Maritime Transportation Security Act of 2002* (Public Law 107-295) in a timely and effective manner. For example, the Coast Guard needs to balance the resources devoted to the performance of homeland and non-homeland security missions; improve the performance of its homeland security missions; maintain and re-capitalize its Deepwater fleet of aircraft, cutters, and small boats; restore the

[33] DHS-OIG, *Targeting of Cargo Containers 2008: Review of CBP's Cargo Enforcement Reporting and Tracking System*, OIG-08-65, June 2008.
[34] DHS-OIG, *Annual Review of Mission Performance – FY2006*, OIG-08-30, February 2008.

readiness of small boat stations to perform their search and rescue missions; and increase the number and quality of resource hours devoted to non-homeland security missions.

We are reviewing CBP's Account Management Program and National Targeting and Analysis Groups, which aim to improve revenue collection compliance. We are also reviewing DHS' planning, management oversight, and implementation of security measures to protect against small vessel threats.

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Executive Secretariat
Chief of Staff
Deputy Chief of Staff
General Counsel
Under Secretary Management
Assistant Secretary for Public Affairs
Assistant Secretary for Policy
Assistant Secretary for Legislative Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS' OIG Program Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

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

OIG HOTLINE

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

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

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

Management's Response to Major Management Challenges Facing the Department of Homeland Security

The Reports Consolidation Act of 2000 requires that the Department include a statement by the Inspector General that summarizes the most serious management and performance challenges facing the Department and briefly assesses the progress in addressing those challenges. The Office of Inspector General (OIG) considers the most serious management and performance challenges to the Department to be in the following areas:

- Acquisition Management;
- Financial Management;
- Information Technology Management;
- Catastrophic Disaster Response and Recovery;
- Grants Management;
- Infrastructure Protection;
- Border Security;
- Transportation Security; and
- Trade Operations and Security.

In addition to the OIG report on management challenges, the Government Accountability Office (GAO) identifies Federal programs and operations that are high-risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement. GAO periodically publishes updates to their High-Risk Series. In recent years, GAO has also identified high-risk areas to focus on the need for broad-based transformations to address major economy, efficiency, or effectiveness challenges. The areas that fall within the Department's purview and the year the issue was identified are listed below. The GAO maintains these issues in their High-Risk Series until satisfied that acceptable progress has been made to correct the issues.

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

The Department of Homeland Security has steadfastly worked to resolve the challenges identified in the Inspector General's FY 2008 report and the GAO High-Risk Series. The Department will continue to address the unresolved challenges, many of which may require several years to completely address due to the complexity of the challenge.

The following highlights the accomplishments of the Department during FY 2008, and details the future plans to be completed to overcome these significant challenges identified by the OIG. DHS has published their plans to address the GAO High-Risk Series separately and this information can be found at http://www.dhs.gov/xabout/budget/gc_1214229806734.shtm.

FY 2008 Challenge 1: Acquisition Management

The Office of Chief Procurement Officer (OCPO) continues to take leadership responsibility for the Department's efforts to improve its functional capabilities, to utilize sound acquisition practices, and to achieve quality business results as it engages in acquiring the complex and diverse requirements to meet DHS's varied missions. The past year's successes have served to strengthen the acquisition infrastructure and produce:

- Better organizational alignment of acquisition functions;
- Improved acquisition policies and processes;
- Enhanced workforce capabilities; and
- Increased capability to retrieve and report data.

The Department will continue to build upon its successes to improve and strengthen acquisition management to ensure security of the Homeland.

Organizational Alignment and Leadership

In order to establish clear lines of authority and accountability within individual Component acquisition communities and to the Department's Chief Procurement Officer (CPO), the OCPO drafted Management Directive 252-01, Acquisition Line of Business Integration and Management, and Instruction 252-07-001. The directive authorizes the establishment of the position of Component Acquisition Executive to be responsible for all acquisition functions, except for contracting and procurement, within each Component. The Head of Contracting Activity would be responsible for all contracting and procurement functions. The Component Acquisition Executives and the Heads of Contracting Activity would report to their respective Component heads, but would be subject to the policies and oversight of the Acquisition Line of Business Chief.

To provide management oversight in key decision points throughout a program's lifecycle, two new Senior-Executive led divisions were established within the OCPO, the Cost Analysis Division and the Acquisition Program Management Division. The Cost Analysis Division provides cost estimating guidance, oversight of program-generated cost estimates, and addresses systemic issues associated with existing Life Cycle Cost Estimates. The Cost Analysis Division is currently engaged in providing a life cycle cost assessment of all DHS Level I investments prior to that investment being presented to a formal Acquisition Review Board for a development or production decision.

The Acquisition Program Management Division was established to strengthen acquisition program management within the Department by ensuring that program management teams are appropriately staffed and trained, and sound program management principles are applied. The Acquisition Program Management Division worked collaboratively with representatives Department-wide to develop a revised Acquisition Management framework. The framework provides governance to DHS's investment programs and reinstituted the Investment Review Board process with a more rigorous oversight function. The Chief Information Officer's Enterprise Architecture Board and the Chief Administrative Officer's DHS Asset Review Boards provide technical expertise and assistance to the Board where needed. During the period from September 2007 to September 2008, the Acquisition Program Management Division conducted 37 quick-look program reviews of

Level 1 investment programs, two Independent Review Team level program reviews, and eight Investment Review Boards.

To foster collaboration and integration among the Department's acquisition community, the Acquisition Policy and Legislation Branch chairs a monthly OCPO Acquisition Policy Board for the purpose of conveying acquisition related information and exchanging best practices.

Future Actions

- OCPO is working to release two major policy documents that will overhaul the current alignment of the acquisition community;
    - One policy document is the Line of Business Directive that will clarify the lines of authority and the roles and responsibilities of the acquisition community within DHS.
    - A second policy document is a companion to the Line of Business Directive and will furnish implementation instructions.
- OCPO will improve the compatibility for improving cost goals by leading the Department's efforts to standardize cost estimating practices and models, providing up-to-date estimating guidance, and expanding the range of cost estimating support to the Components;
- The Cost Analysis Division will provide Acquisition Review Board assessments and furnish consulting services to the Components to further institute department-wide standardization of good costing principles; and
- OCPO will jointly develop with the Government Accountability Office a Cost Assessment Guide and ensure that DHS's acquisition community is informed of changes.

Policies and Processes

During FY 2008, the OCPO strengthened its policies and processes to further integrate planning, requirements, budgeting, and acquisition decisions and actions. The Acquisition Policy and Legislation Branch revised the Homeland Security Acquisition Regulations and the Homeland Security Acquisition Manual, the primary source of acquisition guidance Department-wide, to incorporate significant policy revisions. Several of these regulatory changes were incorporated into the Federal Acquisition Regulation (FAR). DHS procurement personnel are engaged with various FAR Teams in analyzing complex acquisition related issues and recommending government-wide policy. DHS guidance regarding Interagency Agreements was developed and disseminated with stakeholder cooperation, input, and buy-in that resulted in reduced time and effort required to enter into Interagency Agreements.

To increase acquisition oversight, OCPO published the Acquisition Oversight Program Guidebook to promote sound business processes in financial accountability. Internal controls for our investments were instituted through our Acquisition Oversight Program which was favorably reviewed by the Comptroller General.

OCPO revised the Quarterly Operational Status Report that furnishes metrics that gauge the success of the DHS Components' acquisition programs. These metrics report internal management controls while providing a verification and validation mechanism. The enhanced reporting capability ensures that essential data is obtained for establishing benchmarks to monitor the acquisition processes at each of the Components.

OCPO also completed field work to establish a baseline for each of the Components' procurement practices and operations. These on-site reviews served as a foundation for future oversight reviews by providing: 1) a listing of best practices for distribution and consideration by the Components; 2) a mechanism for identifying systemic issues, recommendations, and action plans; and 3) a basis for conducting assessments and tailoring future review programs to focus on key issues identified in past reviews. These reviews also entailed reviewing Component Heads of Contracting Activity human resources capacity and assessed IT system functionality to facilitate acquisitions and integration with financial systems. Additionally, the Acquisition Oversight Branch has conducted three special reviews of high-risk acquisitions to assess all aspects of the acquisition, provide a risk analysis, and recommending improvements for these acquisitions. This branch has also developed a capability and capacity to monitor and review high-risk contracts for the purposes of managing and mitigating risk and overseeing the awarded contracts. It also recognized the importance of improving the process of evaluating cost and pricing of contracts by conducting training to improve the skills of acquisition professionals with regard to the pricing of contracts whenever cost or pricing principles are to be applied. The training has further assisted with ensuring compliance with Federal laws, policies, and regulations.

The Head of Contracting Activity Desk Officer Branch reviewed more than 100 acquisition-related documents, valued at over $50 million each, provided consulting services and furnished business recommendations to DHS's acquisition professionals including new acquisition initiatives and opportunities. The Desk Officer Branch provided procurement subject matter experts to support the Acquisition Oversight reviews, Acquisition Program Management Division reviews, the Office of Management and Budget (OMB) Exhibit 300 reviews, and participated on the source selection teams for several of DHS's high visibility acquisitions.

To further institutionalize Performance Based Acquisitions (PBA) the OCPO released a memorandum to the Heads of Contracting Activity emphasizing the Chief Procurement Officer's commitment to improving the quality and appropriate application of PBA, and requesting that each Component update its Performance Based Acquisition Management Plan. The Oversight Branch within the OCPO is also taking action to improve the Department's PBA reporting. OCPO conducted procurement management reviews of a sample of performance-based contracts within DHS Components to ascertain whether they include fundamental PBA elements such as performance-based statements of work and corresponding performance metrics, and to ensure that a quality assurance surveillance plan is in place and being used to validate the contract compliance with the contract mandated outcomes. PBA data is reviewed on a quarterly basis with the Department's PBA goals to outcomes; feedback capability is being added to this process this quarter. The GAO determined that the contracts that were reviewed had outcome-oriented requirements. The OCPO continues to work with Program Mangers to provide support and oversight to implement Performance Based Contracting for major, complex acquisitions.

The Acquisition Program Management Division initiated and continues to chair a Program Management Council that meets regularly to discuss policies, procedures, and current issues affecting government acquisition, and completed a rewrite of a management directive that established a new process to be followed by all significant acquisition programs. An Acquisition Program Baseline guide was created to foster meaningful content and strong programmatic documentation of a program's cost, schedule, performance thresholds and objectives with quantifiable metrics from which progress can be measured and assessed. Once a requirement is identified, validated and resourced, the program will be subject to reviews at critical decision points to ensure continued investment in the program is in the best interest of the government.

Future Actions

- OCPO will continue to align the Homeland Security Acquisition Manual and the Homeland Security Acquisition Regulations to meet the Component's acquisition needs and align with the Federal Acquisition Regulation requirements;
- OCPO will develop and disseminate guidance to improve the acquisition communities' knowledge of important aspects of acquisition, such as Intellectual Property, Government Furnished Property, Source Selection and Protests; and
- OCPO will continue to aggressively pursue the development of policies and procedures that are necessitated by legislation, such as the National Defense Authorization Bill of 2009, that has requirements impacting the Federal Acquisition system and its workforce, as well as the need to respond to agendas of the next President's Administration and the next session of Congress, which are both expected to push for acquisition reforms.

Acquisition Workforce

Significant strides have been taken to create an acquisition workforce program that reflects the need to recruit, train, and retain a cadre of acquisition professionals with multiple disciplines. The Acquisition Workforce Branch has focused on four acquisition workforce initiatives:

1) Establishment of the Acquisition Professional Career Program;
2) Certification and training requirements for acquisition functional areas;
3) Creation of a centralized acquisition training fund; and
4) Centralized recruitment and hiring of acquisition personnel.

The OCPO-led recruitment efforts resulted in a net increase of 147 contracting professionals and 49 highly qualified procurement interns hired under the Acquisition Professional Career Program being placed into acquisition offices Department-wide.

The same attention given to the recruitment of staff is being directed to the retention of our existing staff. In this respect, retired acquisition personnel were hired to serve as mentors to our acquisition interns in the training and oversight areas, and a tuition assistance program was instituted by the Head of Contracting Activity of the Office of Procurement Operations. Annual employee satisfaction surveys, an exit survey, and structured rotational and development work assignments were also implemented.

The Department made progress in certifying personnel in the acquisition career fields of Contract Specialists, Program Management, and Contracting Officer Technical Representatives. Four hundred ninety nine contracting professionals Department-wide achieved their Level I, II, or III Federal Acquisition Certification in Contracting; 561 program management professionals achieved certification at Levels I, II, or III; and 2,283 personnel achieved Contracting Officer Technical Representatives certification. The Chief Procurement Officer established revised training, standards, and certification processes for program managers pursuant to Management Directive 782, after analyzing multiple certification systems, including the Defense Department's Defense Acquisition Workforce Improvement Act-based system; the Federal Acquisition Institute's policy, and the Program Management Institute's guidelines.

Acquisition-related training was centralized across the Department to enable all DHS acquisition professionals to receive training promptly. As a result, 711 acquisition professionals were trained in various required courses. The culmination of these activities has yielded an acquisition professional better equipped to support the DHS mission and a DHS workforce with the requisite skills, knowledge, and abilities to accomplish its responsibilities.

Future Actions

- The Acquisition Professional Career Program will be adding an additional 150 contracting interns through FY 2010 and seeking to strengthen program management, including related functions such as cost analysis, logistics, systems engineering, and testing and evaluation;
- OCPO's certification program will continue to establish standards for additional acquisition career fields that will lead to minimizing skill and competency gaps and critical vacancies;
- To aid with succession planning, a mechanism to identify acquisition professionals will be developed to help ensure that acquisition positions are filled by an acquisition professional trained and certified at the appropriate level; and
- Additionally, recruitment efforts will be centralized to improve efficiency and increase the Department's ability to attract and retain quality acquisition professionals.

Knowledge Management and Information Systems

The Acquisition Systems Branch is managing the Enterprise Acquisition System Initiative to consolidate and standardize the Department's contract writing and management systems. The Federal Law Enforcement Training Center was migrated to the enterprise system, and the Federal Emergency Management Agency conducted acceptance testing for compatibility with their financial management system. The enterprise system was rehosted to the DHS-secure environment at Stennis, Mississippi. To address FY 2007 Appropriations Act language authorizing the establishment of a Disaster Response Registry, the Branch headed efforts to incorporate the functions of this registry into the Central Contractor Registry in order to utilize a single government-wide repository for collecting contractor business data.

The Acquisition Program Management Division, in collaboration with the DHS Chief Information Officer (CIO), developed a new internal periodic reporting system for acquisition programs. The system is centered on the parameters established in the Acquisition Program Baseline, and includes other commonly accepted best practice metrics, such as Earned Value Metrics, and a Probability of Program Success assessment technique modeled after similar systems at the Department of Defense, U.S. Coast Guard, and other agencies. The new periodic reporting system provides Components and the Department with a structured approach to produce standardized program cost, schedule, and performance metrics. This system will increase program oversight by senior managers and program managers.

To improve the Department's reporting capabilities and increase the reliability of information posted to the Federal Procurement Data System-Next Generation, a standard report format was developed that meets mandatory requirements. In addition, Heads of Contracting Activity are held accountable for accurately reporting their acquisitions. An improved formal agreement with General Services Administration to expedite posting of National Interest Actions in the Federal Procurement Data System was also implemented.

Future Actions

- Plans for information retrieval and reporting efforts in the short term are going to focus on increasing the integrity and enhancing the reporting of acquisition related data;
- To aid Program Mangers and their leadership with obtaining real time reporting of meaningful information regarding their program, the OCPO, in collaboration with the Chief Information Officer, is leading efforts to pilot a web-based reporting system that provides current metrics, conditions, and issues related to a given program. The principal means of reporting procurement data to interested parties outside the agency is the Federal Procurement Data System-Next Generation;
- OCPO is working closely with the systems program personnel to make improvements that will produce a higher quality system that produces more meaningful results;
- Additionally, OCPO is working to ensure the integrity of the data by certifying that the data input into the system is as current, complete, and accurate as possible; and
- The Department will continue migrating components to the Enterprise System for uniform contract writing.

U.S. Coast Guard Acquisition Processes

During the last year, the U.S. Coast Guard has instituted a more disciplined approach to many aspects of the business processes within acquisition. Having implemented reforms addressing contracting, program management (for cost, schedule and performance), personnel, policies and procedures -- the U.S. Coast Guard has taken a major step toward building capability and capacity, and instituting more effective contract and program management oversight. This response addresses the Inspector General's challenge regarding U.S. Coast Guard's Deepwater acquisition to recapitalize many of its assets.

Blueprint for Acquisition Reform

The *Blueprint for Acquisition Reform* is the U.S. Coast Guard's capstone strategic document for reshaping its acquisition and contracting capabilities. The Blueprint for Acquisition Reform was developed using the GAO's *Framework for Assessing the Acquisition Function at Federal Agencies* (September 2005), and later revised for alignment with Office of Federal Procurement Policy *Guidelines for Assessing the Acquisition Function* (May 2008). It provides the framework for establishing the capacity and capability of the U.S. Coast Guard to organically acquire assets and services in four areas: Organizational Alignment and Leadership, Policies and Processes, Human Capital, and Information Management and Stewardship. Each of these four focus areas are further divided into key elements, each aligned with critical success factors to measure attainment of the key element. The central goal is to enhance the U.S. Coast Guard's mission execution through effective and efficient acquisition and contracting activities.

In July 2008, the Blueprint for Acquisition Reform underwent an annual update to Version 3.0. The document was developed collaboratively between the major offices within the U.S. Coast Guard's Acquisition Directorate (CG-9) and reviewed by senior U.S. Coast Guard leadership. Along with overall strategic direction, it provides a summary of directorate objectives for the next year and a two-year rolling action plan. The revised action plan provides updates and adjustments to the existing action items and adds 62 new actions. Prior to the shift from Version 2.0, the U.S. Coast Guard was "on schedule" with 59 percent of action items completed during the first of two plan

years. To date, the new Version 3.0 has more than 43 percent of the existing (Version 2.0) and new actions completed.

The establishment of a centralized Acquisition Directorate (CG-9) in July 2007 set the stage for fundamental progress in U.S. Coast Guard acquisition reform efforts that continued throughout 2008, including:

- Continued integration of organic technical authority review in acquisition projects, and strengthened partnerships with other directorates including Human Resources (CG-1); Engineering and Logistics (CG-4); Command, Control, Communications, Computers and Information Technology (CG-6); and alignment with the Sponsor, Operations Directorate (CG-7);
- Continued incorporation of independent, third party review of major acquisitions, along with more robust organic and governmental certification programs;
- Continued emphasis on acquisition discipline in documented, transparent and repeatable practices through the development of Standard Operating Procedures, and adherence to the U.S. Coast Guard's *Major Systems Acquisition Manual;*
- Enhancement of the Acquisition Performance Management System to include additional metrics and reporting, a system that integrates input from three U.S. Coast Guard accounting systems into a complete Acquisition, Construction, and Improvement data set;
- Completion of an Alternatives Analysis for the Integrated Deepwater System, a program-wide analysis that included an assessment of the major systems and platforms and validated the Deepwater asset mix;
- Reduction in the involvement of the commercial lead systems integrator (for example, in the recently awarded Fast Response Cutter contract), and initiation of efforts to discontinue the use of Integrated Coast Guard Systems (ICGS) as lead systems integrator beyond the current award term;
- Consolidation of personnel from the Systems Integration Program Office to the Assistant Commandant for Acquisition offices in U.S. Coast Guard Headquarters, Jemal Riverside Building, ending the Government collocation with Integrated U.S. Coast Guard Systems and relocating personnel in proximity to U.S. Coast Guard leadership and the technical authorities;
- Continued building a workforce of approximately 1,000 uniformed, civil service and contractor personnel, which included the hiring of 92 government personnel in FY 2008, and the development of a DHS-approved Human Capital Strategic Plan; and
- Continued efforts to implement an aggressive professional certification process, achieving compliance with DHS requirements for Level I investment program managers being DHS-Level III certified in program management, as well as innovative training approaches, and acquisition intern programs to help grow the workforce in the highly competitive job market.

Future Actions

Acquisition Workforce

- The U.S. Coast Guard has developed a specific human capital plan for its acquisition workforce, while simultaneously transforming its organization and its acquisition approach to develop and apply more government expertise in procurement decisions;

- The U.S. Coast Guard is using a Sustainment/Acquisition Composite Model to forecast required manpower for projects. To date, 12 projects have used this model as part of a DHS pilot program. Further analysis is being conducted to ensure the U.S. Coast Guard has the optimum acquisition workforce;
- Additional resources at all levels of the U.S. Coast Guard have been applied to hiring the most qualified people for the Acquisition Directorate, leading to 92 new government acquisition hires in FY 2008; and
- Following recruitment of new acquisition professionals, the U.S. Coast Guard continues to train its new and current acquisition personnel in the areas of technical management, cost estimating and contracting. Currently, the Level 1 Investment (equivalent to Acquisition Category 1) program managers are DHS-Level III certified in program management. This will position the U.S. Coast Guard in FY 2009 and beyond to become both an effective and efficient DHS acquisition component that delivers the operational assets the U.S. Coast Guard requires.

Major Systems Acquisition Manual Compliance

- The U.S. Coast Guard is in the process of updating the *Major Systems Acquisition Manual* to incorporate many acquisition reform initiatives documented in the *Blueprint for Acquisition Reform*, with release expected in October 2008; and
- Additionally, the U.S. Coast Guard is in the process of bringing all Acquisition Directorate and designated non-major acquisition projects into compliance with the *Major Systems Acquisition Manual*. This will enhance the U.S. Coast Guard's ability to provide oversight into the cost, schedule, and performance of all acquisition projects valued in excess of $20 million or otherwise designated for management.

Non-Major Acquisition Process

- In support of the *Blueprint for Acquisition Reform*, the U.S. Coast Guard has developed a process for the management and oversight of non-major acquisitions. This process has been documented in draft Commandant Instruction 5000.11 "Non-Major Acquisition Process" that is currently in concurrent clearance prior to final approval by the Component Acquisition Executive. The goal of this process is to efficiently acquire assets and systems to meet U.S. Coast Guard mission objectives with an appropriate level of project management and oversight tailored for the effort yet robust enough to address the risks associated with non-major acquisitions.

Lead System Integrator

- Aligning with ongoing efforts to fully assume the role of lead systems integrator, the U.S. Coast Guard's Assistant Commandant for Acquisition has prepared an official memorandum expressing the service's intent to not extend the current contract relationship with the lead systems integration contractor, ICGS, beyond the current award term, which ends on January 25, 2011. This official action is another step in the process toward the U.S. Coast Guard becoming the lead systems integrator for its acquisition projects. The U.S. Coast Guard recognizes it cannot fully accomplish that goal under the current contract structure, which limits the Service's oversight with individual manufacturers. By ending the current contract structure, the U.S. Coast Guard will be better able to manage and oversee first-tier

contractors, ensure best value for the government, and ensure adequate competition for future procurements. Transition plans are in the initial stages of development.

Requirements Generation

- The U.S. Coast Guard expects ongoing acquisition reforms to positively impact requirements generation as they require the Acquisition Directorate to assist the sponsor with initial requirements generation, and to translate those requirements into a quality contract solicitation package. The Acquisition Directorate has significantly refocused the work of the U.S. Coast Guard Research and Development Center (which merged into the Acquisition Directorate during the reorganization) into requirements identification, generation and validation; modeling and simulation; and independent third party studies oversight (e.g. Alternatives Analysis) along with the center's more traditional missions.

- The U.S. Coast Guard plans to ensure this collaboration with its Research and Development Center is formalized and implemented through the following:
    - An update to the U.S. Coast Guard's *Major Systems Acquisition Manual* to better define the requirements development process; manage requirements across the life of the project; consider cost and affordability as a key factor in generating requirements; and validate and update the project requirements prior to each milestone decision point.
    - Early engagement by the Acquisition Directorate in training, supporting, and monitoring requirements development for all projects.
    - Certification that the generated project requirements meet the following criteria:
        - The specific performance parameters stated in the generated requirements are substantiated through analysis.
        - The requirements are clearly stated and are measurable.
    - Coordination by the Acquisition Directorate to independently validate the Life-Cycle Cost Estimate for meeting the generated requirements for each major acquisition project, and conduct Life-Cycle Cost Estimate revisions for changes to requirements.

Fleet Mix Analysis

- The Acquisition Directorate is partnering in a collaborative Fleet Mix Analysis to validate mission targets, design fleet alternatives, analyze fleet performance and costs, and calculate return on investment. The U.S. Coast Guard's Operations Directorate is the sponsor for this effort with collaboration from all directorates and technical authorities, and an upgraded version of the U.S. Coast Guard campaign-level model will be used for the analysis; and
- The U.S. Coast Guard augmented its organic capacity, experience, and expertise through a strategic relationship between the U.S. Coast Guard Research and Development Center and the Johns Hopkins University Applied Physics Laboratory, which is a Navy University Affiliated Research Center acting solely in the government interest. An interim product is expected in July 2009. The final product, a business case for the optimal fleet mix, is scheduled for late December 2009.

FY 2008 Challenge 2: Financial Management

Since the passage of the DHS Financial Accountability Act, the Department has worked collaboratively with Congress, the Government Accountability Office, OMB, DHS Office of the Inspector General, and our independent auditor to ensure that we achieve the Act's intended outcome of strengthening financial management to support the Department's mission. For the second consecutive year financial management at DHS has improved dramatically, as evidenced by the following achievements:

- Throughout the year, Civilian Components reconciled Fund Balance with Treasury with only infrequent reconciling differences, in over half of the year earning the highest OMB rating (Green) on financial management performance indicators;
- Improved the efficiency of transaction processing by paying 96 percent of vendors electronically to save taxpayer dollars, reduce paperwork, and strengthen cash management;
- Maintained current on over 99 percent of travel card balances, and 100 percent current on purchase cards, tied for top- ranked cabinet level agency;
- Established a Workforce Development Program to provide training and tools to support job execution, career path development, and talent management to recruit the next generation of financial management leaders;
- Launched the Financial Management Policy Manual online repository. The Financial Management Policy Manual serves as the single authoritative guide on financial management and the foundation for Department-wide knowledge sharing and standardization;
- Appointed a Performance Improvement Officer to improve Department program performance and finalized the Department's Strategic Plan;
- Strengthened Improper Payments Information Act (IPIA) guidance, training, and oversight; conducted a comprehensive process to assess the risk of programs susceptible to improper payments; and performed sample testing of programs;
- Reduced from 16 to 13, the number of Component conditions that contributed to our material weakness conditions in internal controls over financial reporting.
- FEMA reduced the severity on one half of prior year material weaknesses, including:
    - Corrective actions resulted in $1.8 billion of Mission Assignment deobligations, funding was returned to Disaster Relief Fund for other mission priorities;
    - Conducted inventory counts to be better prepared for the Hurricane Season; and
    - Developed a grant accrual methodology for estimating grant expenses at year-end.
- TSA corrected prior year material weakness conditions related to Other Liabilities and Budgetary Accounting;
- U.S. Coast Guard and FEMA reduced the severity of Departmental Financial Management and Oversight to a reportable condition, a first ever material weakness remediation at U.S. Coast Guard;
- The OCFO and OCIO developed an integrated assessment methodology for strengthening Information Technology General Computer Controls; and
- DHS OCFO sustained FY 2007 progress and for the first time ever, the DHS OCFO does not contribute to a material weakness condition.

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

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

Future Actions

- Conduct a Department-wide Financial Reporting Risk Assessment;
- Provide training for cross cutting financial management challenges, e.g., Internal Use Software and Environmental Liabilities; and
- Update the FY 2009 Internal Control Playbook for FY 2008 Independent Audit and Management Assessment Results.

FY 2008 Challenge 3: Information Technology Management

DHS has completed many activities in FY 2008 to significantly reduce many of the major IT management challenges facing the Department of Homeland Security. There will be ongoing efforts to continually review and update these and other activities based on new technologies, revised management practices and guidance.

Information Security Controls

DHS has taken efforts to ensure effective information security controls and address IT risks and vulnerabilities. In Fiscal Year (FY) 2005, the Chief Information Security Officer (CISO) for the Department of Homeland Security (DHS) outlined a five-year strategic plan to improve its security posture and achieve compliance with the Federal Information Security Management Act (FISMA) of 2002. In FY 2008, the Department completed the next phase, "Achieving Excellence," by enhancing its information security compliance requirements and improving security operations through the development of a robust Network Operations Center/Security Operations Center to enhance network situational awareness and incident response.

The Department continued to show improvements in FISMA compliance for the 591 operational systems in use in the Department, particularly in the areas of security controls testing, Plans-of-Action and Milestones management, and focused security operations.

The Department partnered with Components to improve four key process areas: Certification and Accreditation, weakness remediation, annual testing and validation, and program management. In addition, the Department performed formalized data verification at the Component level and updated the DHS FY 2008 Information Security Performance Plan to further improve the quality of the Certification and Accreditation process. The DHS updated the Security Policy and Architecture Guidance to address new operational requirements and advancing technology. The update also revised methods to identify, report, and remediate known and new cyber threats, as well as adapting new information security best practices.

The implementation of the DHS Security Operations Center has significantly improved efforts to improve information security controls. By bringing the Components under a single Security Operations Center, DHS now has the ability to monitor network activity 24/7 and standardize information security controls. The DHS Security Operations Center centralized security related information to provide an enterprise view of risks and issues. In support of the DHS FY 2009 Information Security Performance Plan, the Security Operation Center has established measures to

monitor vulnerabilities that facilitate an enterprise-wide Vulnerability Assessment. In addition, establishing a remote access infrastructure at one of DHS's data centers provides an enterprise-wide remote access solution for all Components.

The United States Computer Emergency Readiness Team (US-CERT) serves as a partnership between DHS and public and private sectors. This partnership allows State, local, tribal, and territorial governments access to the US-CERT Secure portal designed to provide incident response teams across the world a common access portal for information sharing, secure messaging and security alerts, as well as coordinating defense against and responses to cyber attacks across the nation. The Protected Critical Infrastructure Information Program is an information protection program that enhances information sharing between the private sector and the government. DHS and other Federal, State, local, tribal, and territorial analysts use Protected Critical Infrastructure Information to analyze and secure critical infrastructure and protected systems, identify vulnerabilities, develop risk assessments, and enhance recovery preparedness measures.

Future Actions

- During FY 2009, the Department intends to complete the fifth phase of its strategic plan, "Maintaining Excellence," by continually improving all information security processes as well as process measurement;
- The Department will continue its review of all systems to ensure FISMA compliance; and
- The Security Operations Center will implement its FY 2009 Information Security Performance Plan to monitor DHS systems.

IT Infrastructure Integration

In an effort to acquire and implement systems and other technologies to streamline operations within DHS Component organizations, DHS consolidated operations in two Enterprise Data Centers. These centers are secure, geographically diverse to enable disaster recovery, and engineered for redundancy and interoperability, permitting ample redundancy (backup) in the event of a disaster or other service disruption. As a core IT infrastructure service, enterprise data center services enable information sharing across Components while meeting critical mission requirements for the "One DHS Enterprise Architecture", minimizing infrastructure costs and enhancing the disaster recovery posture of the Department.

DHS established a Trusted Internet Connection at each Enterprise Data Center thereby reducing the number of internet access points. The Trusted Internet Connection effort simplifies management standardization of information security controls across the DHS infrastructure, reducing multiple points of vulnerability, improving response, enhancing forensics capabilities, and reducing cost. This is a major step in the DHS wide area network consolidation called OneNet and demonstrates significant progress towards OMB's Trusted Internet Connection goals. Six major area networks (U.S. Secret Service, Office of Inspector General, DHS Headquarters, U.S. Citizenship and Immigration Services, Immigration and Customs Enforcement, and the Federal Law Enforcement Training Center) have been moved to the Trusted Internet Connection and EINSTEIN was deployed.

DHS established a Federal Desktop Core Configuration (FDCC) working group to align the department to FDCC guidelines. To date, the working group has identified variances and

established a baseline. The working group is now in the process of developing a strategy for aligning DHS with FDCC requirements and tracking progress. Desktop standardization will strengthen DHS IT security by reducing opportunities for hackers to access and exploit government computer systems.

The DHS OCIO updates the Enterprise Architecture on a continual basis to ensure standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (service components) are current. The National Information Exchange Model will continue to develop as the standard for information exchange internal and external to the Department supporting law enforcement, intelligence and emergency management missions at all levels of government. This will enable agile enterprise-wide communications with capabilities for alerts, messaging, video conferencing, online learning, collaboration, and secure application of customer oriented information services. Additionally, in FY 2008, DHS assumed leadership as the Acting National Information Exchange Model Executive Director, reflecting DHS's significant growth in the utilization of standards and data sharing consistent with the President's National Strategy for Information Sharing.

Future Actions

- The remaining DHS components are expected to be migrated to OneNet Trusted Internet Connection in FY 2009;
- DHS intends to continue streamlining operations by completing the transition of five legacy wide-area networks to a single integrated network and designing and deploying an enterprise email solution that will replace the existing 12 Component email systems;
- Efforts to consolidate enterprise communications and common operational picture activities are also planned for FY 2009; and
- DHS will continue the development of the Geospatial Enterprise Segment Architecture to support situational awareness and interoperability of spatial data and analysis throughout the homeland security community.

Information Sharing with Partners

DHS strives to support effective information sharing with State, local, tribal, and territorial governments, the private sector, and the public. To this end, the Department invested more than $254 million over a period of several years to assist State and local governments with establishing 58 fusion centers to share information within their jurisdictions as well as with the Federal Government. The DHS Office of Intelligence and Analysis currently provides more than 30 DHS intelligence and analysis professionals to the fusion centers. The Department also established the Control Systems Security Program to reduce control system risks across all critical infrastructure sectors by coordinating efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors.

DHS provides communications systems capable of delivering to States and major urban areas real-time interactive connectivity with the National Operations Center. The Homeland Secure Data Network enables the Federal Government to move information and intelligence to the States at the Secret level and is deployed at 23 fusion centers. Through the Homeland Secure Data Network, fusion center staff can access the National Counterterrorism Center's (NCTC) classified portal of the most current terrorism-related information, NCTC Online. The Homeland Security Information

Network enables all States and major urban areas to collect and disseminate information between Federal, State, and local agencies involved in combating terrorism.

Future Actions

- The Department plans to continue its commitment to information sharing with State and local governments by providing more than 10 additional intelligence and analysis professionals to the fusion centers in 2009.

Privacy Concerns

DHS's efforts to address privacy concerns while integrating its myriad systems and infrastructures demonstrate that privacy and information security are closely linked, and strong practices in one area typically supports the other. In fact, security is one of the Fair Information Practice Principles. To that end, the Chief Information Security Officer works closely with the Privacy Office to monitor the privacy requirements under the Federal Information Security Management Act (FISMA).

The DHS FY 2008 Information Security Performance Plan was updated to further improve the quality of the DHS Certification and Accreditation process and included the addition of Privacy as one of the key process areas. The FISMA scorecard was updated to include a status of systems requiring privacy related Privacy Impact Assessments and/or System of Records Notice (SORN) records. The privacy metrics are designed to provide the status of completed Privacy Impact Assessments or SORNs for those systems requiring such information. The metric is not applied to systems other than those identified by the Chief Privacy Officer as designated privacy systems.

On a quarterly and annual basis, DHS reports to OMB its progress in conducting PIAs and issuing SORNs for IT systems that are required to go through the FISMA Certification and Accreditation. At the end of the FY 2007 reporting period, October 1, 2007, DHS conducted Privacy Impact Assessments on 26 percent of the IT systems that required Privacy Impact Assessments and 66 percent of the IT systems were covered by a SORN. By July 1, 2008, DHS improved its FISMA privacy numbers to 40 percent for Privacy Impact Assessments and 84 percent for SORNs.

One of the requirements for protecting privacy sensitive systems is the process of authorizing, approving, and tracking personal identifiable information extracts from DHS systems. In response to this requirement and the need for standard operating procedures to supplement Attachment S, the DHS Privacy Office established a Data Extracts Working Group. The group, made up of privacy personnel from various components, is developing a set of Standard Operating Procedures to establish uniform practices throughout the Department for authorizing, approving, and tracking data extracts.

Future Actions

- In FY 2009, DHS plans to continue efforts to ensure electronic information and data are fully accessible to members of the public and employees with disabilities.

Budget Oversight/Capital Planning and Investment Control

Management Directive 0007.1 requires that the DHS CIO within the Office of the Chief Information Officer approve any Information Technology (IT) acquisition of $2.5 million and greater. The acquisition actions that require review include, but are not limited to contracts, task orders, and delivery orders, Interagency Agreements, reimbursable agreements, modifications, exercise of options, Military Interdepartmental Procurement Requests, commodity purchases and any other contractual activity that includes an obligation of $2.5 million and above. This includes any IT element(s) of $2.5 million or greater that may be contained within a "non-IT" acquisition. To facilitate the reviews, the OCIO implemented a process, which must be followed for IT acquisitions. The OCIO established an email address for handling communications on the review process to include acquisition request submittals.

The IT Acquisition Review process has resulted in a 50 percent increase in the number of programs reviewed by the Enterprise Review Board to validate alignment to the Homeland Security Enterprise Architecture improved security and accessibility requirements through introduction of specific, contractually binding language; the improved progress of the Wide Area Network consolidation into DHS OneNet, and accelerated transition to the DHS's consolidated Data Centers. Planned accomplishment for FY 2008 support the Secretary's priorities, are consistent with the direction expressed in OCIO Strategic Plan for FYs 2007 – 2011 and align with DHS mission priorities.

The OMB Watch List shows 16 DHS programs on the Management Watch List for President's FY 2009 Budget, down from 53.

Future Actions

- For FY 2009, the CIO plans to actively manage the IT portions of the Watch List programs through the IT Acquisition Review process.

FY 2008 Challenge 4: Catastrophic Disaster Response and Recovery

Since Hurricane Katrina in 2005, major improvements have been made within FEMA and in our ability to work effectively with our partners to improve preparedness and develop a comprehensive emergency management system across the Nation. The pace of improvement at FEMA has been steady and we have strived to use our resources wisely to address the many requirements that have been identified. We believe FEMA's response to Hurricanes Gustav and Ike this hurricane season has shown that while there is still work to be done, FEMA is an agency much improved since the 2005 hurricane season.

In March 2008, the Office of Inspector General identified major management challenges in nine key areas of concern. Following is an assessment of our progress in six of the key areas identified in the report: 1) Logistics; 2) Evacuation; 3) Housing; 4) Disaster Workforce; 5) Mission Assignments; and 6) Acquisitions. For each area we have described the issue and identified accomplishments, challenges, and further actions.

Under a Needs Analysis Initiative rolled out in the Spring of 2007, a Gap Analysis Tool was developed in coordination with the State of New York Emergency Management Office/New York City Office of Emergency Management and has been implemented to provide FEMA and its partners at both the State and local levels in the hurricane prone regions of the country a snapshot of asset gaps at the local, State and National levels. Seven critical areas are incorporated for review in the tool: debris removal, commodity distribution, evacuation, sheltering, interim housing, medical needs, and fuel capacity along evacuation routes. The FEMA regions and corresponding hurricane prone States, territories and local communities have been conducting meetings to discuss capabilities and gaps for responding to hurricane disasters:

- Region I: Connecticut, Rhode Island, Maine, Massachusetts, New Hampshire;
- Region II: New York, New Jersey, Puerto Rico, Virgin Islands;
- Region III: Maryland, Delaware, Virginia, District of Columbia;
- Region IV: Mississippi, Florida, North Carolina, South Carolina, Alabama, Georgia; and
- Region VI: Louisiana, Texas

Logistics

FEMA is responsible for coordinating the delivery of commodities, equipment, personnel, and other resources to support emergency or disaster response efforts, and therefore, FEMA's ability to track resources is key to fulfilling its mission. Logistics plans must move the agency beyond simply providing commodities (e.g., meals, water, and tarps) but toward a holistic management approach that is sufficiently flexible and efficient to meet requirements, and leverages the private sector and 21st Century advances in supply chain management.

FEMA established the Logistics Management Directorate to effectively plan, manage, and sustain the national logistics response and recovery operations, in support of domestic emergencies and special events. The Directorate is responsible for logistics policy, guidance, standards, execution, and governance of logistics support, services, and operations. The Directorate has issued several key operational documents reflecting new processes for testing and validation: 1) Logistics Operations Manual – describes how DHS/FEMA and its public and private sector partners provide logistics support during domestics emergencies and special events; 2) National Logistics Staging Area Concept of Operations – provides a framework for the establishment, operation, and demobilization of the National Logistics Staging Areas which are designated sites where personnel and material are temporarily received, pre-positioned, and shipped for further distribution and deployment; 3) Direct Housing Support Concept of Operations – outlines the logistics support provided to the Disaster Assistance, Individual Assistance Program through the stockage, maintenance, and deployment of temporary housing units; and, 4) FEMA Logistics Transportation Users Guide – prescribes the procedures for acquiring multi-modal transportation, covers mission previously executed by the Department of Transportation Emergency Transportation Center. These documents will be reviewed and updated to reflect lessons-learned from the past hurricane season. Recent responses to the Midwest Floods and Hurricanes Gustav and Ike have helped to validate these processes.

Several of the concepts tested in FY 2008 are as follows: the National Logistics Coordinator concept; Emergency Support Function 7 co-lead with Government Services Agency; Emergency transportation management, (formerly a Department of Transportation role in Emergency Support

Function 1); Distribution Management strategies; Evacuation support through Logistics-based contracts; and the National Logistics Staging Area concept.

FEMA also developed and implemented new internal management controls, and improved total asset visibility and pre-positioning of commodities. Based upon gap-analysis data, FEMA Logistics pre-positioned critical life-saving and life-sustaining disaster commodities throughout the hurricane-prone regions in Florida, Alabama, Mississippi, Louisiana, Texas, and New York, hence were able to significantly enhance the first 72 hour response capability. Total Asset Visibility in-transit extended to all ten regions, Total Asset Visibility specialist cadre developed and trained for rapid deployment. The Logistics Management Directorate established an Internal Management Control program beginning with formalized training of a Program Lead. Logistics played pivotal role in the rewrite of the Property Management Manual 6150-1, following through with the accurate accounting of disaster accountable property and conducting wall-to-wall inventories for 100 percent accountability.

Future Actions

- FEMA intends to engage the private sector and incorporate industry best practices to include incorporating a third party logistics structure into the Logistics Management Directorate where appropriate. During FY 2009, the Directorate will concentrate on four strategic cornerstones: People, Customers, Processes, and Systems, in that order. The focus is to institutionalize command and coordination of strategic logistics planning, operations and management while pushing operational control and execution down to the most effective level of execution. More specifically, to develop National Level collaboration while continuing to improve internal operations and capability such as further developing the Single-Integrator concept and National Supply chain strategy. The Logistics Management Transformation Initiative is the overarching program to help transform the Directorate into a more effective, responsive organization with improved readiness and response capability. A Transformation Management Office was established in FY 2008 to drive transformation. The Transformation Management Office will provide the governance structure to assist in galvanizing the transformation process. Third-party logistics opportunities are continuously explored and analyzed as future integrated supply chain options; and
- FEMA will implement Logistics Management capabilities similar to the Department of Defense's well-recognized logistics (J4) system and organization. The National Logistics Coordinator concept promotes FEMA Logistics Management as the Single-Integrator for strategic planning, operational, and tactical logistics support. The National Logistics Coordinator will coordinate domestic emergency logistics planning, management and sustainment capabilities, and promote the strategic and tactical logistics collaboration among public, private and non-governmental organization partners. The National Logistics Coordinator concept somewhat mirrors the role J4 plays in the Military Service.

Evacuation

FEMA made improvement in its plans and capabilities for managing mass evacuations and the resulting displaced populations, including additional State and local plans and development and expansion of evacuee tracking systems. FEMA is working closely with States to ensure that evacuation plans are in place, and completed five state hosting plans for large numbers of evacuees, including refined evacuee hosting guidance. While the Department of Transportation has retained

responsibility for some transportation functions, FEMA has taken over the standby contracts for air/bus/rail support to ensure available evacuation transport when State and local governments cannot handle the evacuation process.

Enhancements were made to the National Shelter System and enhancements were made to the National Shelter System and the Aidmatrix Network which is a national disaster relief coordination system funded by FEMA, The UPS Foundation, Accenture, and the Aidmatrix Foundation, Inc. to better manage unsolicited donations and volunteers. This network connects State and local governments with donors, State Voluntary Organizations Active in Disaster, National Voluntary Organizations Active in Disaster, and FEMA through web-based tools to reduce paperwork and allow for easy information sharing. No software, hardware or additional IT staff is required with this hosted solution, and training is minimal. FEMA also produced an annual report to Congress, per Homeland Security Act of 2002, Section 882, and quarterly reports on the status of National Capital Region, West Virginia, and Pennsylvania evacuation planning.

Future Actions

- Refine evacuee hosting guidance and complete five State hosting plans for large numbers of evacuees in FY 2009 and FY 2010; and
- Complete enhancements to the National Shelter System and Aidmatrix system to improve system security and user interface, and continue to provide technical assistance and training to users nationwide.

Housing

Possibly the largest problem FEMA faced in the aftermath of Hurricane Katrina was providing financial assistance, sheltering, and housing to evacuees. Because FEMA lacked a catastrophic disaster housing strategy and had never before been faced with meeting the short- and long-term housing needs of hundreds of thousands of disaster victims, it relied on shelters, hotels, motels, cruise ships, and tents, as well as any other available housing resources to meet sheltering and housing needs.

To address short and long-term disaster housing, FEMA developed the draft National Disaster Housing Strategy that describes how the Nation provides housing to those affected by disasters and charts a new direction to better meet the needs of disaster victims and communities. This draft Strategy is available for public comment and is being reviewed by key partners. The Strategy provides the overarching vision, goals, and principles for a national disaster housing effort. A 2008 Disaster Housing Plan was also issued which compliments the draft Strategy and describes the specific actions that FEMA will take this year to support State and local officials in meeting the housing needs for disaster victims. Additionally, FEMA staff completed a compendium of potential alternative housing solutions with ratings and guidelines for best application of particular units given disaster conditions through the Joint Housing Solutions Group.

Future Actions

- FEMA will develop and implement priority elements of the National Disaster Housing Strategy;

- They will continue to make strides in interagency planning and coordination to assist communities with long-term recovery, to address contaminated debris, debris volume estimation, and streamlining the Public Assistance Program processing for very large events through planning, training, and technology improvements; and
- FEMA must continue to improve and test/exercise FEMA's capabilities for all of its Individual Assistance functions (mass care, emergency assistance, housing, and human services).

Disaster Workforce

Section 624 of the Post-Katrina Emergency Management Reform Act of 2006 requires that a plan for a Surge Capacity Force be submitted to Congress not later than 6 months after enactment. The Surge Capacity Force is an external resource which supplements FEMA when a disaster exceeds the Agency's internal capabilities to respond. The plan therefore must include procedures on how to designate sufficient numbers of trained, credentialed employees for disaster missions from DHS and other Federal agencies. Since Disaster Reservists account for 70 percent or more of all FEMA employees who deploy to each disaster, a viable plan for the Surge Capacity Force must first be premised on a stronger Disaster Reserve Workforce.

A comprehensive assessment of the Disaster Reserve Workforce was initiated in 2007, and completed in September 2007. Based in part on the results of this assessment, the Disaster Reserve Workforce Division (DRWD) was established within the Management Directorate in March 2008. The new Division grew out of a small staff located within the Disaster Operations Directorate, and is now led by a career Senior Executive and several experienced reserve managers. DRWD is the Agency's single accountable program manager for transforming the legacy Disaster Assistance Employee program into an all-hazard Disaster Reserve Workforce. This Division also coordinates the deployment, tracking and FEMA-specific credentialing of all FEMA employees for disaster response and recovery. Increased expectations for performance, balanced with improved benefits for qualifying Disaster Reservists, are essential to creating a professional, national, all-hazards workforce.

Working with FEMA's Emergency Management Institute, DRWD is co-sponsoring an 18-month initiative to produce a standardized, National Incident Management System (NIMS) compliant credentialing process applicable to all 23 disaster specialties ("cadres") and 230 disaster job titles found at Joint Field Offices. Completion of this project will be subject to the availability of funding. FEMA recently released interim policies to pay Disaster Reservists for administrative absences and designated Federal holidays when the Joint Field Office or assigned work site is closed and the Reservist does not work.

Future Actions

- FEMA will complete the standardized credentialing plan project for all 230 disaster job titles staffed by FEMA disaster workers. With the completion of the credentialing project, the Agency will have completed an important step towards a consistently credentialed, more professional disaster workforce standardized across all cadres;
- FEMA will improve deployment systems by finalizing and deploying a web-enabled upgrade to the Agency's Automated Deployment Database system. Future actions also include formalizing interim policies regarding administrative absence and designated

Federal holiday pay, as well as developing policies for sick leave, telework, and prospective legislation that address benefits or training for Disaster Reservists;

- DRWD will work with planners and cadre managers at the Headquarters and Regional levels to determine the number and composition of skilled Disaster Reservists required for response and recovery; and
- A more robust, more professional Disaster Reserve Workforce will minimize the size and composition of *Post-Katrina Emergency Management Reform Act* Surge Capacity Force required for catastrophic events and major disasters. However, to comply with Section 624 of the *Post-Katrina Emergency Management Reform Act*, FEMA worked with DHS component agencies in spring 2008 to identify criteria in selection of prospective selectees for the Surge Capacity Force. In September 2008, this initial effort was augmented by the establishment of an ad hoc working group of selected DHS agencies to develop a Concept of Operations (CONOPS) for this Surge Capacity Force. This CONOPS will describe the process for selection, training, deployment, and reimbursement of the Surge Capacity Force. A completed, approved CONOPS for the Surge Capacity Force is anticipated by summer 2009.

Mission Assignments

Mission Assignments (MAs) are a critical component of the Federal Government's response to an incident and require significant Federal funds and resources. Other Federal departments and agencies have considerable resources and expertise that can prove effective in life-saving circumstances and provide major support to the response and recovery process. FEMA uses MAs to coordinate the urgent, short-term emergency deployment of federal resources to address immediate threats, and is responsible for stewardship of the associated expenditures from the Disaster Relief Fund. The issuance and execution of MAs touch virtually every functional area in a response, and requires coordination with many, if not all of those areas, such as operations, recovery programs, planning, acquisitions, logistics, finance, administration, and information technology.

FEMA has expanded the use of pre-scripted mission assignments. In 2006, FEMA had only 44 pre-scripted mission assignments with two Federal agencies. In 2007, FEMA had 224 pre-scripted mission assignments in coordination with 31 Federal departments and agencies, and in 2008 FEMA had 236 pre-scripted mission assignments with 33 Federal departments and agencies.

Future Actions

- Continue to build on the number of pre-scripted mission assignments and enhance the requisite coordination with Federal departments and agencies. Increased capabilities and resources in this arena will ensure fewer errors and greater programmatic control and consistency.

Acquisitions

In the aftermath of Hurricane Katrina, FEMA was not prepared to provide the scope and nature of acquisition support needed for a catastrophic disaster. Challenges included acquisition planning and preparation for the large number of acquisitions needed immediately after a disaster; clearly

communicated acquisition responsibilities; and sufficient numbers of acquisition personnel to manage and oversee contracts. Pursuant to the Post-Katrina Act, FEMA has undergone significant reorganization to improve this function.

FEMA has established a strategic roadmap for the Office of Acquisition Management (OAM) that outlines goals, objectives and strategies to build a world-class acquisition organization. They have also provided technical support and training for the ProTrac and ProDoc systems, which provides contract management, tracking, and document generation capability. In addition, Acquisition staff created a robust program to support and provide on-the-job guidance to Contracting Officer's Technical Representatives. Finally, they developed and coordinated the addition of an Acquisition Advisor to the Federal Coordinating Officer under the Incident Command System structure to include improving the quality of business advice and expertise during major disasters and emergencies.

Future Actions

- FEMA will continue to implement and refine the Office of Acquisition Management strategic roadmap and improve the office's ability to meet customer needs;
- They will also sustain and improve business processes by leveraging e-business technologies such as ProTrac, ProDoc, FedBid and other systems;
- Acquisition will build upon the Contracting Officer's Technical Representative program by establishing a tiered Contracting Officer's Technical Representative development program that provides greater levels of training based on the level of contract management required for a particular program or contract; and
- Finally, Acquisition Management must continue to provide a full range of acquisition services that support the procurement and contract management programs' policies, procedures, operations, contract planning, awards, administration, and closeouts.

FY 2008 Challenge 5: Grants Management

To meet its mission and to ensure fulfillment of Congressional requirements, the DHS Headquarters' Office of Grant Policy and Oversight (GPO) continues to develop policies that address grants management administrative requirements. This will ensure standardization of processes for grant-making components and offices, including FEMA. Grant management policies will be issued through the DHS Headquarters Office of the Chief Financial Officer's (OCFO) *Financial Management Policy Manual.*

Reorganization

The FY 2008 Challenge addresses FEMA's reorganization as well as other components' grants management processes. In FY 2009 the DHS Headquarters grants management policy and oversight function was transferred from the Office of the Chief Procurement Officer (OCPO) to the Office of the Chief Financial Officer (OCFO). Under this transfer, *Single Audit Act* process, currently administered by the DHS Office of General Inspector (OIG), will also be transferred to and implemented by the Headquarters OCFO, GPO. Monitoring associated with the receipt, review, and resolution of audits/findings will provide administrative management insight for the stewardship of DHS assistance awards. Timely review of audits will provide information related to

the management and expenditure of awards from the sub-recipient to the DHS component levels. As a result of this monitoring DHS will provide guidance and technical assistance to the components regarding audit findings, which in turn should be provided to primary recipients of assistance awards.

An implementation plan for the transfer and expansion of the grant management function to the CFO/GPO will be completed in early 2009. The plan will include a timetable for the transfer of the *Single Audit Act* function from the OIG, and enhancement for the organization and staffing. This move will enhance statutory authority compliance and provide resources for a more vigorous oversight capability as it relates to accountability of funds, internal controls and audit processing/oversight of assistance awards.

The transfer and expansion will also address the concerns identified in the OIG Management Challenge regarding the transfer of Grants and Training and Preparedness Offices into FEMA. Not only will the expanded OCFO/GPO oversight ensure compliance, but it will identify redundant planning, effective management gaps, identification of duplicate program efforts/initiatives/funding and lack of monitoring within the components. The goal of this initiative is to support and complement objective by providing a comprehensive DHS oversight for grants management requirements that also meets the needs of individual assistance programs.

Future Actions

- CFO to develop implementation plan for the transfer and expansion of the grant management function to be completed in early 2009; and
- Transfer DHS Headquarters grants management policy and oversight function from OCPO to the OCFO in FY 2009.

Oversight and Internal Controls

The DHS Grants Management Challenge for 2008 states, in part, "DHS needs to ensure that internal controls are in place and adhered to, and grants are sufficiently monitored to achieve successful outcomes."

As part of internal controls oversight, the GPO will analyze all DHS assistance programs to identify programs that: 1) may duplicate other programs; 2) are similar to other programs; or 3) complement other programs. Once the analysis is completed, GPO will coordinate the results with other DHS oversight offices and components with applicable programs. The analysis and report will be completed by September 30, 2009 in order to capture all programs that have been announced for assistance funding opportunities. The report will be submitted to the DHS Policy Office for follow up to determine if the program needs to be redirected to address duplication of efforts. GPO will provide a similar report annually and provide recommendations for combining programs when appropriate.

GPO is also currently reviewing all the Terms and Conditions of assistance awards in conjunction with the other Headquarters oversight offices, (e.g., Office of General Counsel, Office of Chief Information Officer, Privacy Office, etc.) and program offices to determine validity, compliance, and consistency within DHS. The terms and conditions will be tied to the compliance requirements, risk assessment, and internal controls associated with the appropriate program(s). This task is to be

completed in 2009, as copies of FY 2009 Award Terms and Conditions are submitted to GPO for review.

Internal control development for DHS grants management processes will continue to be developed through policy development and implementation, monitoring and oversight, through coordination with the OCFO internal controls management action plans. This will ensure effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. It is anticipated that the internal control infrastructure will be in place by the end of 2009.

Future Actions

- GPO will analyze all DHS assistance programs to identify programs that: 1) may duplicate other programs; 2) are similar to other programs; or 3) complement other programs in FY 2009;
- GPO to review contractual Terms and Conditions of assistance awards to determine validity, compliance, and consistency within DHS; and
- Internal controls Mission Action Plans to be developed to address monitoring and oversight functions.

Standardization/Streamlining

FY 2008 Grants Management Challenge discusses the development of two Grants Management Line of Business life-cycle grants management systems. To address that challenge, and to further standardize and streamline grants management processes, DHS through FEMA is developing two life-cycle electronic grants management systems; one for disaster and one for non-disaster grants. It is anticipated that by FY 2011, all DHS assistance awards should be executed and managed through one of the systems. Once activated, the systems will provide consistent internal controls over data entry, transaction processing and reporting for all DHS assistance programs. Because of the volume and urgency of the disaster award processing, it is not anticipated that the systems will be fully integrated. DHS will develop an interface between the two systems that will provide joint capability for payment processing, data generation, reporting, and other functional requirements.

Future Actions

Interim Action Items:	**Target Date:**
- Under Secretary for Management delegation to CFO	11/30/2008
- Post Vacancies and Recruit Staff	11/30/2008
- OIG/CFO Memorandum of Understanding to transfer A-133 Audit Function	12/31/2008
- Develop A-133 Audit Strategy/Implementation Plan	12/31/2008
- Complete Policies	03/31/2009
- Transfer A-133 Audit Function	04/01/2009

- **Long-Term Action Items:**
  - Analyze DHS assistance programs to determine possible duplicate programs 09/30/2009
  - In coordination with OGC, develop "Standard Terms and Conditions Template" for assistance awards 09/30/2009
  - FEMA development of two life-cycle electronic grants management systems to be operational FY 2011

FY 2008 Challenge 6: Infrastructure Protection

Coordination of Critical Infrastructure and Key Resources (CIKR)

In the management challenges report, the Inspector General notes that, "*the requirement to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CIKR. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the effective implementation of protection efforts is a great challenge."* The Office of Infrastructure Protection within the National Protection and Programs Directorate (NPPD) recognizes the challenge of ensuring protection in a voluntary environment, and continues to be proactive in leading the coordination of a national Critical Infrastructure and Key Resources (CIKR) risk management program. As part of this program, Infrastructure Protection is required to prepare and submit to Congress the National CIKR Protection Annual Report (NAR).

The CIKR Sector Partnership Framework, as outlined in Chapter 4 of the National Infrastructure Protection Plan (NIPP), is the core enabling component of the CIKR risk and performance management efforts. The Framework includes Government Coordinating Councils and the Sector Coordinating Councils for each of the 18 CIKR sectors. Infrastructure Protection ensures that the NIPP and the Sector Specific Plans are fully implemented, that they remain aligned with long-term strategies, and that the sectors achieve the milestones set out in these documents. The Sectors are responsible for submitting their Sector Annual Report each year to provide updates on how the sector is implementing the NIPP and their Sector Specific Plans. The Sector Annual Reports are then consolidated into the NAR.

Future Actions

- Revise metrics chapter of the National Annual Report to emphasize an outcome-focused view on CIKR performance management across all sectors; and
- Develop outcome-oriented scorecards across all sectors in order for DHS to effectively identify security gaps and progress, regardless of whether it is DHS, other Federal agencies, State, local, tribal, and territorial entities, or the private sector leading the CIKR security efforts.

Incident Management

During crises, Infrastructure Protection uses the NIPP and the National Response Framework to guide its response activities with federal partners and the private sector. Through the Infrastructure Protection Incident Management Cell, the Infrastructure Protection Assistant Secretary, CIKR

owners and operators, the 18 SSAs, and other security partners work collaboratively to monitor an incident, develop impact assessments, and coordinate and facilitate prevention, response, and recovery activities. Infrastructure Protection's efforts during recent Hurricanes Ike and Gustav illustrate this coordination. Before the storm hit landfall the National Infrastructure Coordinating Center, National Infrastructure Simulation and Analysis Center, and the deployed Protective Security Advisors were working with stakeholders to provide up-to-date information based on hurricane models.

NPPD's Office of Cybersecurity and Communications (CS&C), also plays a significant role in addressing infrastructure protection issues associated with cybersecurity across the public and private sectors. Specifically, DHS's national response mechanism, the National Cyber Security Division's (NCSD) United States Computer Emergency Readiness Team (US-CERT), provides stakeholders with alerts and actionable information, such as Critical Infrastructure Information Notices and Federal Information Notices, needed to protect information systems.

Future Actions

- US-CERT is working with NCSD's Outreach and Awareness Program and other cross-sector working groups to increase awareness through communication channels such as the Homeland Security Information Network for Critical Sectors, the National Cyber Alert System, various information sharing and analysis centers, the US-CERT Portal, the Government Forum of Incident Response and Security Teams Portal and the US-CERT Public Website. These channels allow for ongoing information exchange with public and private sector stakeholders to distribute alerts and warnings in the event of a cyber incident.

Infrastructure Data Warehouse

The Inspector General states that, "*a comprehensive, national database that inventories assets is essential to provide a comprehensive picture of the nation's CIKR and to enable management and resource allocation decision-making. Their office is currently reviewing how DHS uses an asset database to support its risk management framework.*" Infrastructure Protection is currently developing the Infrastructure Data Warehouse to maintain a national database of CIKR systems and assets. The Infrastructure Data Warehouse is a federated data architecture that provides a single virtual view of one or more infrastructure data sources. In addition, Infrastructure Protection produces the annual prioritized lists of systems and assets critical to the Nation (The Tier 1/Tier 2 and Critical Foreign Dependencies Lists). The Tier 1/Tier 2 program, which develops the Tier 1/Tier 2 list each year, is a joint effort between the Sector Specific Agencies, the States, Infrastructure Protection, and other entities. This list informs grant programs such as the Buffer Zone Protection Program and the Homeland Security Grant Program. During the 2008 Fiscal Year, Infrastructure Protection conducted 395 vulnerability assessments and 743 Energy Conversation Investment Program (ECIP) Assessments, of which 40 assessments were part of the California Water System Comprehensive Review which utilized extensive National Infrastructure Simulation and Analysis Center modeling.

Future Actions

- The Infrastructure Data Warehouse plans to have initial operating capability by Spring 2009 of a national database of CIKR systems and assets;

- In FY 2009, Infrastructure Protection will increase functionality of the Tier 1/Tier 2 program to more efficiently and effectively conduct analysis of high priority critical infrastructure and key resource assets and facilitate information exchange, verification, and maintenance with State and sector partners; and
- In FY 2009 Fiscal Year, Infrastructure Protection plans to conduct over 300 vulnerability assessments and over 1,000 ECIP Assessments, which will include a multi-asset/system-based Comprehensive Review, on Tier 1 and Tier 2 Facilities and 12 New Nuclear Reactor Security Consultations.

Securing Critical Infrastructure and Key Resources

On September 17, 2008, DHS created the Office of the Chief Administrative Officer, Office of Business Continuity and Emergency Preparedness in response to the Inspector General's assertion that, "*protecting national as well as internal cyber infrastructure continues to be a challenge for DHS. We recently reviewed the department's progress in identifying and prioritizing its internal cyber critical infrastructure in accordance with Homeland Security Presidential Directive 7…we found the department needs to complete additional steps to produce a prioritized inventory and to coordinate related efforts to secure these assets, and the recommendation to designate a specific office to determine protection priorities for its internal cyber critical infrastructure*." Under Secretary for Management designated Business Continuity and Emergency Preparedness to manage the DHS-internal CIKR program, including the determination of protection priorities for its internal critical cyber infrastructure. Established in 2006, Business Continuity and Emergency Preparedness provides DHS with an office for central management and coordination of the Department's internal continuity of operations and emergency preparedness programs. The two programs are interrelated with CIKR as well as other internal Department protection and preparedness programs.

Future Actions

- Business Continuity and Emergency Preparedness will apply an integrated "mission assurance" approach by leveraging capabilities and analysis within interrelated programs to identify and protect CIKR resources.

Mission Essential Functions and Primary Mission Essential Functions

The Inspector General also suggested, "*the department should develop a process to coordinate internal efforts to protect these assets"*. During FY 2008 a major focus of the COOP program was the identification and analysis of the Department's Mission Essential Functions (MEF) and Primary Mission Essential Functions (PMEF) and how those functions support the National Essential Functions. The MEF/PMEF process is detailed in the FEMA developed Federal Continuity Directive – 2, "Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification Process," dated February 2008. Analysis of DHS MEF/PMEF includes identification through a detailed Business Process Analysis of key resources required to perform the MEF/PMEF. The Business Process Analysis results will serve as a new baseline for the CIKR program including determination of internal critical cyber infrastructure and the priority of asset protection and recovery based on the asset's impact on Department MEF/PMEF and business functions.

In addition, the National Cybersecurity Initiative, formalized by National Security Presidential Directive 54/Homeland Security Presidential Directive-23, enables NCSD—and the Department as a whole—to expand its current activities which contribute to its mission. The National Cybersecurity Initiative is a series of continuous efforts designed to further safeguard Federal Government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats.

Future Actions

- NCSD is working with other Departmental and Interagency components to develop the strategic analysis of the Nation's critical cyber infrastructure, integrating all relevant and appropriate sources of information to support predictive analysis;
- NCSD is seeking to engage stakeholders in other Federal and non-Federal agencies to provide them with actionable information based on this predictive analysis; and
- The National Communications System will provide the Director of the Office of Science and Technology Policy and DOD with an implementation plan for a comprehensive Continuity Communications Architecture. The implementation plan will include the minimum requirements necessary to finalize selection of a secure communications system by DOD.

FY 2008 Challenge 7: Border Security

Along with the successes enjoyed by U.S. Customs and Border Protection (CBP) in FY 2008, CBP acknowledges that there will be challenges in the coming fiscal year in order to secure the borders against all threats. The following are the top challenges for FY 2009 and plans to address and resolve them.

Secure Border Initiative (SBI)

As of September 30, 2008, U.S. Customs and Border Protection, through the Secure Border Initiative (SBI), has constructed 204 miles of pedestrian fence and 154 miles of vehicle fence to further secure the border. CBP has other miles that are currently under construction, 66.3 miles of pedestrian fence and 33.3 of vehicle fence, but CBP is not counting those miles as completed until all elements of construction have been undertaken. In addition, 74.9 miles of pedestrian fence and 116.2 miles of vehicle fence are currently under contract. All remaining mileage will be awarded prior to the end of the calendar year. CBP remains committed to achieving the goal of 661 miles of fencing in the areas that the border patrol has identified as operational priorities. By the end of the calendar year, CBP believes that it can get close to the goal in terms of miles that are actually finished, under construction, or in some cases under contract.

Successful execution of the SBI mission requires the establishment and sustainment of a well-trained and coordinated team of acquisition professionals. To accomplish this, an SBI Acquisition Workforce Development, Sustainment, and Training Working Group was established in January 2008, consisting of members from the SBI Acquisition Office and SBI Program Executive Office. SBI policies and procedures were and continue to be established to standardize the execution of acquisition functions, and an SBI Joint Policy Board, consisting of members from the SBI Program Executive Office, and the SBI Acquisition Office, was established. Continuing into FY 2009, a comprehensive set of acquisition and procurement policies and procedures are being

implemented to establish expectations and govern the planning, execution and oversight of all SBI procurement and acquisition activities to assure that intended results are achieved. In FY 2009, CBP will finalize the policy that defines functional roles and responsibilities of all acquisition positions within the SBI Acquisition Office and SBI Program Executive Office. In addition, to ensure that sound acquisition practices are being developed and adhered to, an SBI Acquisition Management and Customer Support Division was established during FY 2008.

In the past, tactical infrastructure maintenance and repair was accomplished on an ad hoc basis by either Border Patrol employees (uniformed or civilian) or the military (Operation Jump Start or other military units on a rotational, short term basis). This has not been an efficient use of resources and a more permanent solution is under development. The SBI Tactical Infrastructure Program Management Office is taking steps to award a Comprehensive Tactical Infrastructure Maintenance and Repair contract in the July 2009 time frame. This contract will cover maintenance and repair of all types of tactical infrastructure, including fencing, and will provide coverage to all nine Southwest Border Patrol Sectors. In FY 2009, a set of metrics will be developed and utilized to eliminate redundancies, identify potential process improvements, identify strategic sourcing opportunities, provide for internal control monitoring, aid in workload management, and track status of SBI procurements.

Future Actions

- SBI Tactical Infrastructure will coordinate Real Estate acquisition support for SBI*net* in FY 2009 to obtain the numerous real estate tracts required to support the number of tower sites through a partnership with the U.S. Army Corps of Engineers. Prospective sites are identified at the outset, which requires engaging more landowners for Rights of Entry than will ultimately be needed for acquisition, with new sites identified as the project progresses. In FY 2009, these acquisitions will be negotiated toward purchase to the fullest extent possible, but they may require Department of Justice involvement to enter into the condemnation process;
- The SBI Tactical Infrastructure Program Management Office is taking steps to award a Comprehensive Tactical Infrastructure Maintenance and Repair contract in the July 2009 time frame. This contract will cover maintenance and repair of all types of Tactical Infrastructure, including fencing, and will provide coverage to all nine Southwest Border Patrol Sectors;
- In FY 2009, CBP will finalize the policy that defines functional roles and responsibilities of all acquisition positions within the SBI Acquisition Office and SBI Program Executive Office; and
- In FY 2009, a set of metrics will be developed and utilized to eliminate redundancies, identify potential process improvements, identify strategic sourcing opportunities, provide for internal control monitoring, aid in workload management, and track status of SBI procurements.

SBI*net*

SBI*net* is employing a "spiral" approach of iterative design-prototype-test-learn cycles. This spiral development approach provides for an initial definition of requirements (under formal configuration control), and then a period of development and testing to gain user feedback and engineering confidence with initial (sometimes draft) designs. Final requirements, as well as final designs, are

worked together and often in parallel. The initial test spirals also help to complete detailed test plans and procedures needed for qualification and acceptance testing. Activity to accomplish this includes revising or developing the Mission Need Statement, the Operations Requirements Document, the Acquisition Program Baseline, and the Test and Evaluation Master Plan. Additionally, to track progress being made by SBI contractors, increased utilization of earned value management principles is being emphasized.

Future Actions

- In 2009, SBI*net* will continue to follow a disciplined set of activities for planning, executing, and reporting SBI*net* program testing; and
- SBI will include in the SBI*net* Block 1 Acquisition Program Baseline a revised SBI*net* life cycle management approach, including a Systems Engineering Plan, and Test and Evaluation Master Plan that highlights specific testing roles and responsibilities, and those parties accountable for the revised test.

Border Patrol Workforce

CBP is continually challenged to maintain and expand the gains we have achieved in securing operational control of our borders. As CBP improvises and adapts to the tactics of human and narcotics smugglers, the same criminal organizations move to adapt to the tactics of CBP. To counteract this in FY 2009, CBP will continue to rely on and implement intelligence driven operations, as well as maintain a well trained and flexible work force of agents. CBP will also continue to upgrade and enhance its Special Operations Groups of Border Patrol Tactical Units, Border Patrol Search, Trauma, and Rescue, and Special Response Team units. As a highly mobile, rapid-response tool, the Special Operations Group personnel will significantly improve CBP's ability to respond operationally to specific terrorist threats and incidents, as well as support the traditional Border Patrol mission. Additionally, a consequence of the very successful Border Patrol agent recruiting program was that there has not been a commensurate number of Mission Support Specialists brought on board to support the Agents. Mission Support Specialists perform non-law enforcement functions that allow agents to focus their efforts on safeguarding the borders. CBP relies on these very important positions to allow them to conduct the important business of safeguarding the borders of the United States.

Future Actions

- CBP will conduct a strong recruiting and hiring campaign in FY 2009 for these Mission Support positions, similar to the recruiting and hiring campaign for Border Patrol agents;
- CBP will conduct a series of training exercises and classes in FY 2009 to include advanced weapons training, explosive handler courses, primary marksman courses, high-risk operations and special response team training;
- A series of exercises in coordination with other Federal and State agencies addressing airlift and search and rescue operations will be conducted in FY 2009; and
- Additionally, the Office of Border Patrol intends to train 690 First Responders in FY 2009.

Integration of Border Activities

A number of actions taken in 2008 and current initiatives emphasize the vital role of integration and capitalizing on efforts of multiple organizations to successfully secure the border. CBP and the U.S. Coast Guard are operating a Joint Program Office for unmanned aircraft systems to link requirements and test maritime variants. A joint maritime advanced concept and technology demonstration occurred in March 2008. DHS is using a unified command structure in select locations such as the San Diego Sector where U.S. Coast Guard, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection employ maritime response protocol integration in interagency efforts. Project Seahawk in Charleston, South Carolina, is a prime example of a successful multi-jurisdictional task force comprised of Federal, State, and local law enforcement agencies charged with preventing or disrupting illicit activity. Department leadership concluded an acquisition review of Border Security, Fencing, Infrastructure and Technology investment in September 2008 and underscored the importance of a common operational picture with a more open architecture to readily adapt to changes in sensor types, technologies, and an integrated concept of operations.

Also in FY 2008, CBP and ICE jointly hosted the Human Trafficking Symposium which raised awareness and discussed best practices in the fight against human trafficking. CBP also sponsored the 2008 Joint Agency Agriculture Stakeholders Conference that strengthened existing partnerships (CBP-Agriculture Plant Health Inspection Service, CBP-States and CBP-Industry), and provided a forum for State Governments and private industry to offer ideas for fulfilling our agricultural mission.

Future Actions

- CBP will form a focus group using the recently completed Massachusetts Institute of Technology Lincoln Laboratory Architecture Trade Study as a starting point to make recommendations to leadership by January, 2009; and
- The Department is also beginning a cross-Component analytical effort to assist in resource allocation across programs and Components and to measure effectiveness of inter-Component DHS efforts on the border.

Detention and Removal

U.S. Immigration and Customs Enforcement (ICE) introduced new Performance-Based Detention Standards to ensure that safe, secure and humane conditions of confinement exist for ICE's detained alien population. These new and improved standards are based upon the performance-based format now endorsed by the American Correctional Association and focus on the results and outcomes that daily performance expectations should accomplish. Also, the Performance-Based Detention Standards provide enhanced transparency at ICE facilities and to the public, to non-governmental organizations and to third-party oversight groups.

Further, oversight of the ICE detention assets was strengthened by the establishing of a Detention Facilities Inspection Group (DFIG) within the Office of Professional Responsibility. The DFIG provides ICE with an independent inspection arm dedicated to oversight of ICE's Detention and Removal Operations (DRO) program. The DFIG conducts independent Quality Assurance Reviews, and Special Assessment Reviews requested by the Assistant Secretary. The DFIG

conducts independent reviews of critical incidents involving ICE detainees in concert with ICE DRO headquarters personnel. The DFIG prepares executive summaries and final reports for the Assistant Secretary, ICE Executive Leadership and for DRO management. The group monitors the progress being made by DRO to correct any non-complying condition.

Additionally, ICE has contracted with private companies to provide on-site compliance verification of the Performance-Based National Detention Standards at all ICE detention facilities. These personnel are posted full time at ICE's 40 largest facilities to monitor both the detention standards and quality of life issues at all Service Processing Centers, Contract Detention Facilities, and the larger State, local and county jails that house ICE detainees via Intergovernmental Service Agreements. In addition, ICE now uses a contracted service that performs annual inspections of all detention facilities that house ICE detainees. These inspections are performed by detention subject-matter experts who specialize in Health Services, Security, Safety and Food Service. More than 200 facility reviews have already been completed.

Border Enforcement Security Task Force

In 2006, DHS Secretary Michael Chertoff adopted the Border Enforcement Security Task Force (BEST) initiative to leverage Federal, State, local and foreign law enforcement resources in an effort to identify, disrupt, and dismantle organizations that seek to exploit vulnerabilities in the border and threaten the overall safety and security of the American public. The task forces are designed to increase information sharing and collaboration among the agencies combating this threat on both sides of the border.

During 2005, the Laredo, Texas and Nuevo Laredo, Mexico areas experienced a significant increase in violent crimes, specifically murder and kidnappings. These crimes were often associated with the underlying criminal activities, primarily drug smuggling, human smuggling, arms trafficking, bulk cash smuggling, and money laundering. In response to the increased violence in this geographical area and other areas along the Southwest border with Mexico, the U.S. Immigration and Customs Enforcement (ICE) in partnership with various Federal, State, foreign, and local law enforcement officials expanded its ongoing Border Crimes Initiative by creating a multi-agency operation called the Border Enforcement and Security Task Force, or BEST.

BESTs utilize a comprehensive approach toward dismantling the cross-border criminal organizations that exploit vulnerabilities of the United States border, while also developing information useful toward eliminating the top leadership and the supporting infrastructure that sustains these often-violent organizations. BESTs includes personnel from ICE, CBP, the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Federal Bureau of Investigation, the U.S. Coast Guard, and the U.S. Attorney's Office, along with other key Federal, State, tribal, local, and foreign law enforcement agencies.

BESTs leverage Federal, State, tribal, local, and foreign law enforcement and intelligence resources to achieve the goals of the BEST. These goals are to:

- Gather and analyze intelligence;
- Identify, disrupt, dismantle and prosecute cross-border smuggling and trafficking organizations; and
- Interdict contraband, weapons, money and persons entering the U.S. illegally.

In furtherance of the BEST mission, U.S. law enforcement agencies coordinate intelligence sharing and investigative leads with representatives from the governments of Mexico and Canada. This coordination better enables the United States Government's ability to attack organizations in a more-coordinated way on both sides of the border. Participating in BEST on the Southwest border is the Mexican law enforcement agency Secretaria de Seguridad Publica. For the Northern border, participating Canadian law enforcement agencies include the Canada Border Services Agency, the Royal Canadian Mounted Police, the Ontario Provincial Police, the Niagara Regional Police Service, and the Toronto Police Service.

The BEST concept was first implemented in Laredo, Texas in January 2006. BESTs were subsequently established in: 1) Tucson, Arizona in March 2006; 2) El Paso, Texas in October 2006; 3) San Diego, California in November 2006; and 4) Rio Grande Valley (Harlingen, Brownsville, and McAllen, Texas) in March 2007.

On February 4, 2008, the first Northern border BEST initiated operations in Blaine, Washington. A second Northern border BEST was subsequently launched in Buffalo, New York on March 4, 2008.

In FY 2008, BESTs were established in three additional locations along the Southwest border. BESTs were established in Phoenix, Arizona in March 2008, in Yuma, Arizona during March 2008, and in Imperial Valley, California in June 2008.

Preliminary results for FY 2008 show that, BESTs were responsible for 918 criminal arrests, 1,229 administrative arrests, 342 indictments, and 320 convictions and has seized 1,599.44 pounds of cocaine, 55,560.71 pounds of marijuana, 120.84 pounds of methamphetamine, 5.47 pounds of crystal methamphetamine, 50.88 pounds of heroin, seized 414 weapons, 288 vehicles, and approximately $8.1 million in United States currency and monetary instruments.

FY 2008 Challenge 8: Transportation Security

The security of the Nation's aviation system is a collaboration of public and private sector elements working together to provide effective protection for travelers and the flow of goods. This coordinated effort to protect the aviation system is designed to defeat threats, reduce vulnerabilities, minimize the consequences of, and expedite the recovery from attacks that might occur. Transportation Security Administration (TSA) screening of persons and property continues to be a vital and successful element of the overall aviation security system. The effectiveness of TSA screening is due to the layered approach to aviation security, greater emphasis on unpredictable screening methods, and systematic improvements implemented in the screening process.

To address the challenge of improvements needed in training; equipment and technology; policy and procedures; and management and supervision, TSA has completed the following:

Checkpoint and Checked Baggage Performance

In support of Office of Security Operations review of options to relieve Supervisory Transportation Security Officers and Lead Transportation Security Officers of as much ancillary administrative responsibilities as possible, a Working Group of Supervisory and lead Transportation Security

Officers and Lead Transportation Security Officers was recently convened. The Working Group's recommendations have been further studied, impacts determined, and vetted with Senior Leadership. At this time, senior leadership decisions are moving through the Office of Security Operations requiring near term alteration of program administrative practices and associated systems.

A standard operating procedure change has been made that allows for more than two passes through the Walk-Through Metal Detector in an attempt to induce divestiture of substantial amounts of metal. Following completion of Hand Held Metal Detector and sensitive area pat-down screening, Transportation Security Officers may now re-process the individual through the Walk-Through Metal Detector to confirm that Walk-Through Metal Detector metal alarms were resolved as a result of additional screening. Additional random pat-downs have also been included in the recent change.

In FY 2008, TSA purchased an additional 117 advanced technology systems and a procurement of an additional 133 systems is pending with plans to procure an additional 332 systems later in the year. The current advanced technology contract is capped at 500 systems per vendor, so a new procurement solicitation has been initiated to be awarded in FY 2009. To date, TSA has deployed 280 systems to 13 airports.

TSA continues to explore options for more effective sensitive area pat-downs, while weighing security concerns with social expectations. Although a new sensitive area pat-down was recently designed, the increased level of intrusiveness inherent in the proposed procedure requires additional field study and a more comprehensive understanding of the impact it will have on the flying public. Toward that end, a pilot is currently underway at several airports that will test alternative sensitive area pat-down procedures. TSA is still in the process of conducting field suitability and effectiveness testing of x-ray backscatter and millimeter wave whole body imaging technologies in operational environments. In addition, TSA continues to work closely with the vendors to ensure our ability to take full advantage of the effectiveness of the imaging, while continuing to afford appropriate protections for the traveling public.

Also in FY 2008, as a result of recently conducted pilots, TSA implemented a change to the alternative bag search protocol which will require all bags to be opened at non-Explosive Detection System checked baggage screening locations.

Future Actions

- Completing Checkpoint Evolution training for over 50,000 employees;
- Continuation of advanced security solutions at the checkpoint;
- Utilizing advanced communication systems for Transportation Security Officers throughout the airport;
- Continuing testing to determine appropriate staffing levels for new technology;
- Utilizing Security Transportation Inspectors for re-certification training. By eliminating contractor support and performing this essential function with Transportation Security Officers, TSA will be able to focus its training resources more directly on Transportation Security Officers; and
- Developing and conducting improvised explosive device Exercise Drills and Kits for checked baggage and checkpoint Transportation Security Officers.

Employee Workplace Issues

TSA has taken proactive steps by establishing the Office of the Ombudsman, the Integrated Conflict Management System, and the National Advisory Council to help identify and address its employees' workplace concerns and to meet the challenges of providing employees with sufficient tools, guidance and communication on the structure, authorities, and oversight responsibilities. As stated in our previous response to OIG, TSA is taking a systems approach that includes skills, structures, and support to build a values based culture, which encompasses conflict management competency, innovation, communication, collaboration, and employee engagement.

TSA issued the Ombudsman Management Directive which clearly identifies the role of the Office of the Ombudsman to plan and execute all necessary activities, including site visits, free from interference; suggest corrective actions to airports and Area Directors as a result of its activities; and follow-up with TSA officials responsible for airport operations to ensure that corrective actions are implemented.

The Office of Ombudsman converted data collected prior to the implementation of the Inquiry Management System to a Microsoft Access database and created a selection of reports that permit more ready extraction and analysis of data. Additional summary reporting formats that will give Federal Security Directors and other senior leadership official's information on the volume, nature and type of contacts received by the Office of the Ombudsman from its first year of operation in 2003 are under development. This report format will list the volume of contacts by type received each quarter. From this data, historical trends and comparisons will be more readily made. A page on the Office of the Ombudsman's SharePoint site is being created that will be populated with the summary reports described above. Summary reports for the first three quarters of FY 2008 were posted to this site by September 2008. Historical quarterly data reports will be made available through this site by the end of the second quarter of FY 2009.

TSA's senior leadership established the National Advisory Council to bridge the gap between field personnel and headquarters. The National Advisory Council has built a communications network across the field by establishing a point of contact at every airport. The points of contact work to foster effective communication between the front-line workforce and headquarters. The National Advisory Council developed many important initiatives including: dual-function bonus; changes to PASS; development of the Voluntary Leave Transfer Program; as well as provided field input to changes in Standard Operating Procedures, technology, safety and training. The National Advisory Council serves as an advisory board that provides direct, unfiltered feedback to the TSA Administrator, Deputy Administrator and Senior Leadership Team. TSA's National Advisory Council is composed of 34 members from among the Transportation Security Officers, Lead Transportation Security Officers, Supervisory Transportation Security Officers, and Behavioral Detection Officers from airports nationwide and 27 members drawn from the Assistant Federal Security Director-Screening and Transportation Security Manager ranks.

Future Actions

- Develop internal practitioners to continue the development of core competencies in conflict management and cooperative problem solving;
- Expand the influence and span of the National Advisory Council by fully engaging the National Advisory Council Network in the gathering of ideas and sharing information;

- Implementation of revised Mid-Level Development Program with defined program components, and accomplished of needs assessment for purposed of program right-sizing and development of new learning tools;
- Complete all program development activities for Senior Leadership Development Program 2 and most activities for Senior Leadership Development Program 3;
- Development of needs analysis and proposal for a new Executive Leadership Development course; and
- Initial selection and development participants for the TSA Career Resident Program and planning for possible nationwide rollout in FY 2010.

Passenger Air Cargo Security

TSA's conducts many programs to ensure the security of air cargo. Some of the programs conducted include the Indirect Air Carrier Standard Security Program, the Aircraft Operator Standard Security Program, Model Security Program, Airport Security Program, Security Threat Assessments, Access Control, Secure Movement of Air Cargo, and Cargo Security Training and Air cargo screening. During FY 2008, TSA completed its deployment of the Transportation Security Inspectors Cargo K9 Handlers and conducted 25 "cargo strike" surges.

Transportation Security Inspectors also conduct "known shipper" inspections of regulated entities that transport cargo on aircraft against various standard security programs and security directives. These programs and directives indicate the baseline requirements necessary to establish a shipper as being known and in compliance with baseline requirements. Known Shippers, or "vetted shipper", status allows entities that have routine business dealings with freight forwarders or air carriers to move cargo onto a passenger aircraft. In contrast, unknown shippers are entities that have conducted limited or no prior business with a freight forwarder or air carrier, and are not considered vetted. Regulated entities can also prove known shipper status through Customer Record, Business History, Contract and Site Visit Verification. The Known Shipper Management System uses commercial databases to verify the legitimacy of shippers. Through FY 2008, more than 1.3 million shippers in the U.S. have been vetted by TSA and approximately 184,351 security threat assessments were completed by freight forwarders and air carriers. The Office of Inspector General is conducting an audit of the Air Cargo Security - Known Shipper Program. TSA anticipates a draft report from the Office of Inspector General in the very near future and benefiting from the recommendations made.

In FY 2008, TSA Implementation of the Certified Cargo Shipper Program in an effort to achieve 50 percent screening air cargo originating in the U.S. transported on passenger aircraft by February 2009 and 100 percent screening by August 2010.

Future Actions

- The TSA will address recommendations from the Office of Inspector General Known Shipper Program audit in FY 2009;
- Publish the Certified Cargo Screening Program Interim Final Rule to implement 9/11 Act mandates to screening 50 percent of air cargo originating in the U.S. and transported on passenger aircraft by February 2009 and 100 percent by August 2010;
- Develop and implement the Air Cargo Data Management Systems – critical to full deployment of the Certified Cargo Security Program;

- Complete deployment of 85 canine teams to the larger airports to support the 100 percent cargo screening mandate of the 9/11 Commission Act; and
- Complete the remaining 14 vulnerability assessments for the 27 Category X airports.

Rail and Mass Transit

The report of the DHS Inspector General on TSA's mass transit security programs cited challenges in four areas:

1. Clarity of the role of TSA Surface Transportation Security Inspectors (STSIs) in the transit security mission;
2. Internal communication and coordination with the STSIs and with access to results of Baseline Assessment for Security Enhancement (BASE) program results the STSIs produce;
3. Coordination with mass transit and passenger rail security partners on Visible Intermodal Prevention and Response (VIPR) operations, with the recommended action that TSA complete Memorandums of Understanding with each security partner; and
4. The lack of security regulations in mass transit and passenger rail.

TSA STSIs play an integral role in the implementation of the mass transit security strategy. Their assessment work advances the strategic priority of elevating the security baseline. The assessment results inform the setting of security priorities and the development and implementation of programs and resource allocations to achieve them, including the Transit Security Grant Program.

In communicating STSIs mission to security partners, TSA has made this connection clear - whether at meetings of the Sector Coordinating Council (SCC), monthly teleconferences with the Peer Advisory Group (PAG), the semi-annual Transit Security Roundtables, and the periodic meetings of Regional Transit Security Working Groups (RTSWG).

To enhance internal communications, Transportation Security Network Management (TSNM) Mass Transit engages with the Surface Transportation Security Inspection Program (STSIP) consistent participation in the bi-weekly STSIP national teleconference, daily coordination with the program director, and briefings at the STSIP annual meetings. This proactive engagement aims to ensure timely awareness and thorough understanding of developments in mass transit and passenger rail security programs and initiatives. An area needing improvement is consistency in ensuring STSIs are aware of meetings involving security partners in their respective areas.

On providing accesses to assessment results, TSNM Mass Transit and the STSIP have set a clear policy of limiting access to those with a need to know to execute security responsibilities pertaining to mass transit and passenger rail. In addition to the STSIs, this group includes members of the Mass Transit Division, officials with responsibilities for the Transit Security Grant Program in Transportation Sector Network Management, and others reviewed on a case-by-case basis as dictated by their security responsibilities. This policy specifically aims to restrict distribution of the results to avoid breaches of information security.

With respect to the VIPR program, TSA has completed an agreement with the mass transit and passenger rail community, as represented by the PAG, on operating guidelines for the deployment of TSA resources to augment security in mass transit and passenger rail. The agreement provides a framework for effective planning, coordination, preparation, execution, and after action review of

VIPR deployments. TSA has distributed the VIPR operating guidelines to the law enforcement chiefs and security directors of the largest 50 mass transit and passenger rail agencies, to the SCC, and to Federal Security Directors and Federal Air Marshal Special Agents in Charge. To enhance the deployment of the various TSA components in VIPR teams, TSA also produced a supporting product that explains the role and capabilities of each VIPR element and provides recommendations on effective deployment of these resources in mass transit and passenger rail. The VIPR operating guidelines and guidance on roles, capabilities, and tactical employment provide the foundation for effective conduct of VIPR operations. Therefore, Memorandums of Understanding with each mass transit and passenger rail agency that could participate in a VIPR deployment are not necessary.

TSA recently issued regulations aimed at strengthening the security of the nation's freight and passenger rail systems and reducing the risk associated with the transportation of security-sensitive materials. The Rail Security final rule will require freight and passenger rail carriers to designate rail security coordinators and report significant security concerns to the TSA. The rule also will codify TSA's broad inspection authority. For freight rail, the rule will ensure the positive handoff of security-sensitive materials as well as establish security protocols for custody transfers for security-sensitive material rail cars between receivers of these materials that are located in high threat urban area, shippers of these materials, and rail carriers. To raise the level of security in the freight rail transportation sector ahead of the final rule, both TSA and the U.S. Department of Transportation developed security action items, along with the freight rail industry, to reduce the risk associated with the transportation of Poisonous by Inhalation (PIH) materials. These measures have resulted in an overall risk reduction of more than 60 percent, well above the target reduction of 50%. PIH materials are potentially harmful and include essential chemicals like chlorine and anhydrous ammonia. PIH materials represent less than one percent of all hazardous materials rail shipments.

Under the BASE program, STSIs have now completed 88 assessments, vastly expanding TSA's domain awareness, understanding of security enhancement needs, and abilities to advance effective security programs and resource allocations. The assessments results have enabled TSA to identify the priorities requiring attention and build consensus in such forums as the Government Coordinating Councils, SCC, PAG, and RTSWGs for collaborative risk mitigation efforts. Through such products as the Smart Security Practices compilation, TSA is fostering networking among security partners to expand adoption of the most effective programs, measures, and activities.

TSA recognizes the value that performance-based requirements can yield in security enhancement. Consistent with the requirements of the Implementing Recommendations of the 9/11 Act, TSA has initiated consultation and coordination with security partners for development of regulations on security plans, assessments, and training programs. The results of this outreach, further informed by the continuing assessment results, are being applied in the concerted TSNM effort to produce the required regulations during FY 2009.

Future Actions

- Maintain consistency on TSA's mission and security priorities in all engagements with security partners. Expand involvement of the STSIP in outreach forums such as the SCC, PAG, RTSWG, and Transit Security Roundtable meetings, to ensure understanding of the integrated role STSIs play in the implementation of TSA's security strategy in mass transit and passenger rail;

- Establish primary and alternate internal liaison representatives between TSNM Mass Transit and the STSIP to ensure timely communication and coordination of upcoming meetings and related matters with security partners, whether as individual agencies or in group forums such as the SCC and RTSWG;
- Complete and distribute the VIPR Operations Kit for mass transit and passenger rail security partners and Federal Security Directors and Federal Air Marshal Special Agents in Charge. The kit includes the operating guidelines and guidance on roles, capabilities, and tactical employment. TSA projects distribution of this product will commence in early 2009; and
- Update the summaries of the developing concepts for the pending rulemakings on security training programs and security plans and assessments. Complete consultations with security partners on these updated summaries by the end of 2008. Complete draft for notices of proposed rulemakings in each area in the first quarter of FY 2009.

FY 2008 Challenge 9: Trade Operations and Security

U.S. Customs and Border Protection (CBP) will facilitate about $2 trillion in legitimate trade this year while enforcing U.S. trade laws that protect the economy, health, and safety of the American people. The Office of Inspector General report states, "Modernizing trade systems, using resources efficiently, and managing and forging partnerships with foreign trade and customs organizations pose significant challenges for CBP and DHS. Finding the right balance to fulfilling CBP's mission to secure the Nation's borders and to facilitate the free flow of international trade is a challenge that requires CBP to consistently monitor and evaluate the processes and systems the agency employs to screen and clear the millions of import ocean cargo containers and millions of entries that cross our ports of entry every year. We accomplish this through close partnerships with the trade community, other government agencies, and foreign governments. The following is an update to CBP's trade operations.

The Container Security Initiative

The Container Security Initiative (CSI) enables CBP, in working with host government Customs Services, to examine high-risk maritime containerized cargo at foreign seaports before they are loaded on board vessels destined for the United States. Almost 32,000 seagoing containers arrive and are off loaded at United States seaports each day. The goal is for CBP's overseas CSI teams to review all the manifests before containers are loaded on vessels destined for the United States. Today, CSI has partnered with 32 countries and is operational in 58 ports worldwide in North, South, and Central America; Asia; Europe; South Africa; the Middle East; and the Caribbean.

Future Actions

- There are no current plans to expand CSI further than to the 58 ports they are operating in.

Secure Freight Initiative

The Secure Freight Initiative (SFI) integrated scanning pilot project consists of Radiation Portal Monitors provided by Department of Energy and non-intrusive inspection imaging systems provided by CBP or the host nation, that are used to scan containers as they move through foreign ports. DHS CBP created SFI in partnership with the Secretaries of Energy and State on

December 7, 2006 in order to meet Congressional scanning requirements. SFI is currently operating in four foreign ports scanning 100 percent of all cargo using non-intrusive inspection imaging systems.

Future Actions

- DHS/CBP is finalizing a strategy focused on high-risk trade corridors that entails expanding the concept into new areas, adding more complexity to the challenges noted in DHS's report to Congress on the pilot implementations.

Customs and Trade Partnership Against Terrorism

CBP's Customs Trade Partnership Against Terrorism (C-TPAT) is an integral part of the CBP multi-layered strategy through which CBP works in partnership with the trade community to better secure goods moving through the international supply chain. C-TPAT now has more than 8,700 members and accounts for almost half of all imports into this country. CBP conducted more than 9,690 validations of C-TPAT members since its inception which more than 1,893 were re-validations.

Future Actions

- By the end of calendar year 2008 C-TPAT will complete 3,200 validations, meeting the SAFE Port Act requirements to validate new members within one year of the date of certification and conduct revalidations within 3 years of the date of initial validation; and
- C-TPAT projects that it will complete approximately 3,000 validations in calendar year 2009 and 2010 to meet the SAFE Port Act requirements. Continued membership growth will require CBP to re-examine program resources.

10+2 Security Filing

CBP recognizes the critical need to fully incorporate additional advance trade data information into the targeting environment. In pursuing this objective, CBP is currently in the process of requiring additional supply chain information, which includes critical entry type data, to improve automated targeting capabilities. This new requirement, known officially as the 'Importer Security Filing and Additional Carrier Requirements' or simply "10+2" will significantly increase the scope and accuracy of information gathered on the goods, conveyances and entities involved in the shipment of cargo arriving by vessel into the United States. CBP worked with the trade community through the Departmental Advisory Committee on Commercial Operations to create a new Security Filing in an effort to obtain additional advanced cargo information and enhance our ability to perform risk-based targeting prior to cargo being laden on a vessel overseas. CBP's close partnership with the trade community is the key reason why the "10+2" Security Filing proposal was developed in a smooth and timely fashion. Stakeholder input during the consultative process as well as its participation in the Advance Trade Data Initiative has been instrumental in the successful crafting of the proposal. Additionally, earlier this year, the Committee on Commercial Operations made almost 40 recommendations to CBP on how to implement the security filing or "10+2 Security Filing initiative". CBP carefully studied and considered the Committee on Commercial Operations recommendations and agreed in full and/or in part to a majority of the recommendations.

Future Actions

- There will be no comments on the rule in progress.

Mutual Recognition Partnerships

An important effort to note is the potential mutual recognition of other countries' customs-to-business partnership programs. Creating an international network to exchange information about trusted traders and knowing that those participants are observing specified security standards in the secure handling of goods and relevant information is a win-win for both government and business. In June 2007, CBP signed its first mutual recognition arrangement with New Zealand. In June 2008, CBP signed two additional arrangements, one with Canada and the other one with Jordan.

Future Actions

- CTPAT projects two additional mutual recognition arrangements in FY 2009; and
- While dependent upon the ability of those administrations which have communicated interest to CBP in creating their own industry supply chain security program in accordance with CTPAT, the trend of signing one or two Mutual Recognition Arrangements is expected to continue over the next few years.

Participation in World Trade and World Customs Organizations

CBP provided guidance to the Office of the U.S. Trade Representative on World Trade Organization matters including the Chinese Auto Parts dispute; the Trade Facilitation Negotiating Group; World Trade Organization Accessions for Russia; Yemen, Montenegro, Serbia, and Kuwait; the Anti-Counterfeiting Trade Agreement; and the complaint against China for ineffective intellectual property rights enforcement. In addition, CBP represented the U.S. at the World Customs Organization's 40th and 41st session of the Harmonized System Committee, 36th and 37th Session of the Harmonized System Review Sub-Committee, Technical Committee on Customs Value, and Technical Committee on Rules of Origin. CBP also participated in the development of the Standards Employed by Customs for Uniform Rights Enforcement.

Future Actions

- CBP will continue to support the World Trade Organization in FY 2009 and beyond by providing appropriate trade expertise as needed.

Cargo Security

The Office of Inspector General report states, "Our annual Automatic Targeting System (ATS) review in 2008 focused on a subsystem of ATS, the Cargo Enforcement Reporting and Tracking System (CERTS), which is designed to gather data on cargo examination findings and report on how efficiently examination equipment is being used. We identified the need for improvements in planning, updating, developing and implementing the CERTS system. CBP needs to update the project plan to include the scope of work, and a detailed implementation schedule for system

design, developing and testing, and cost estimates past phase one. In addition, CBP bypassed key life cycle reviews designed to ensure end-users have a properly working system and have received management's approval to continue the project." CBP has developed, implemented and is monitoring the updating of CERTS. CBP realigned the key life cycle reviews and updated the Production Readiness Review and the Operational Readiness Review as discussed with the Office of Inspector General. In addition, the latest quality assurance testing was also conducted. Remaining CERTS funding was re-appropriated by DHS and remains an open item as the amount of the appropriation is only projected to last until May 2009.

Future Actions

CBP anticipates the CERTS Project Plan Actions through Phase II cited below will be completed by May 1, 2009. A funding stream has not been identified for Phase III development.

Phase II – Iteration V

- Support for Automated Commercial Environment Post Release Entry Summary, Accounts and Revenue (ESAR 2.2)
- Pre-work/recertification of Initial Decision Point
- Planned released to all users November 11, 2008

Phase II – Iteration VI

- User Interface modifications to support Entry Summary, Accounts and Revenue events
- Initial Decision Point
- Based on recertification of definition/business requirements
- Planned release to all users January 11, 2009

Phase II – Iteration VII

- Support Laboratories and Scientific Services notification
- Integrate CERTS events with ATS Find Queries
- Correct Seal Logic
- Pre-work for In-process/Pending events
- Planned release to all users February 18, 2009

Phase II – Iteration VIII

- In-process/Pending events
- Planned release to all users April 1, 2009

Closeout Phase II activities

- Technology Readiness Review – April 17, 2009
- Production Readiness Review – May 1, 2009

Implementing the World Customs Organization Framework

The World Customs Organization Framework, developed by the World Customs Organization, represents an extraordinary implementation challenge for the customs administration of any country, particularly for one that may not have the resources or subject matter expertise readily available to implement the practices identified in the Framework.

The Framework is a set of standards to secure and facilitate global trade and provides a new avenue in which customs administrations can operate. The Framework will enhance CBP's ability to strengthen the entirety of the global supply chain by assisting countries in strengthening their customs operations. It will also help CBP synchronize its own operations with other trusted customs administrations to meet the challenges of the global economy. This is because the Framework provides standards that, if adopted universally, would provide continuity, consistency, and stability to the customs process.

- In FY 2009, CBP will work with the World Customs Organization to align the Framework with CBP's major strategic goals, including:
  - Harmonizing data requirements of the Framework with those found in the World Customs Organization Data Model;
  - Continuing to develop the Single Window concept;
  - Solidifying relationships with other customs administrations through the negotiation of Mutual Recognition Arrangements; and,
  - Continuing development of a World Customs Organization Trade Recovery Program. This program addresses what steps countries need to take should there be a significant disruption to trade.

Maintaining a Safe and Secure Food Supply

As the value and complexity of our food imports grow, CBP's challenge is to maintain a safe and secure food supply. As with our approach to anti-terrorism, CBP has taken a multi-layered approach to protect the safety of America's food imports. In its newly published CBP Trade Strategy, Objective 3.1 calls for CBP to "Protect U.S. consumers through the secure and trusted import of safe agriculture and goods." CBP will accomplish this by helping to build a prevention-focused model to monitor the entire import lifecycle, while working to expand partnerships and integrating import safety verifications. CBP will continue to leverage its trade expertise, including the use of laboratory services to analyze and verify the health, safety, and admissibility of products prior to release.

Future Actions

- Continuing in FY 2009, CBP is partnering with other Federal agencies to refine our targeting skills, monitor for compliance, and prevent contaminated products from entering the U.S.; and
- CBP is also training its personnel to further identify safety concerns, including food-related threats.

Protecting Against Unfair Trade Practices, Illicit Commercial Enterprises and Unsafe Imports

With the growth of U.S. imports and the risk associated with international trade, CBP must direct an effective trade facilitation and enforcement approach to protect our Nation's economy and people from unfair trade practices, illicit commercial enterprises and unsafe imports.

Future Actions

- In FY 2009 CBP will continue to focus its actions and resources around priority trade issues (antidumping and countervailing duty, agriculture, import safety, intellectual property rights, penalties, revenue, and textile and wearing apparel) that pose a significant risk to the U.S. economy, consumers and stakeholders; and
- CBP will work closely with international partners, including the European Union to carry out Intellectual Property Rights initiatives focused on goods that also present health and safety concerns.

Commercial Trade Fraud Investigations

CBP is primarily responsible for trade operations and security with the support of the U.S. Coast Guard, while ICE leads trade enforcement investigations for DHS. ICE conducts commercial trade fraud investigations, a key element of the overall DHS trade enforcement strategy, and also focuses on priority programs aimed at stopping predatory and unfair trade practices that threaten the United States' economic stability, restrict the competitiveness of U.S. industry in world markets, and places the public health and safety of the U.S. public at risk. Successful cases have produced significant seizures, civil penalties, and criminal prosecutions.

Acronym List

The ***Appendix*** contains a list of acronyms.

Acronym List

AFG – Assistance to Firefighters Grants
A&O – Analysis and Operations
ARTF – Aquatic Resources Trust Fund
ATS – Automated Targeting Systems
BASE – Baseline Assessment for Security Enhancement
BEST – Border Enforcement Security Task Force
BPD – Bureau of Public Debt
B&SA – Bureau & Statistical Analysis
C&A – Certification and Accreditation
CBP – U.S. Customs and Border Protection
CDL – Community Disaster Loan
CERTS – Cargo Enforcement Reporting and Tracking System
CFO – Chief Financial Officer
C.F.R. – Code of Federal Regulations
CGC – Coast Guard Cutter
CIKR – Critical Infrastructure and Key Resources
CIO – Chief Information Officer
COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985
COE – U.S. Army Corps of Engineers
CONOPS – Concept of Operations
COTR – Contract Officer's Technical Representative
COTS – Commercial Off-the-Shelf
CPIC – Capital Planning and Investment Control
CS&C – Cybersecurity and Communications
CSI – Container Security Initiative
CSRS – Civil Service Retirement System
C-TPAT – Customs-Trade Partnership Against Terrorism
CY – Current Year
DADLP – Disaster Assistance Direct Loan Program
DFIG – Detention Facilities Inspection Group
DHS – Department of Homeland Security
DHS FAA – Department of Homeland Security Financial Accountability Act
DNDO – Domestic Nuclear Detection Office
DOC – Department of Commerce
DOD – Department of Defense
DOI – Department of Interior
DOL – Department of Labor
DRO – Detention and Removal Operations
DRWD – Disaster Reserve Workforce Division

ECIP – Energy Conversation Investment Program
FAR – Federal Acquisition Regulation
FASAB – Federal Accounting Standards Advisory Board
FBwT – Fund Balance with the Treasury
FCRA – Federal Credit Reform Act of 1990
FECA – Federal Employees Compensation Act
FEGLI – Federal Employees Group Life Insurance Program
FEHB – Federal Employees Health Benefits Program
FEMA – Federal Emergency Management Agency
FERS – Federal Employees Retirement System
FFMIA – Federal Financial Managers' Financial Integrity Act
FIRA – Flood Insurance Reform Act
FISMA – Federal Information Security Management Act
FLETC – Federal Law Enforcement Training Center
FMA – Flood Mitigation Assistance
FMFIA – Federal Managers' Financial Integrity Act
FPS – Federal Protective Service
FSIO – Financial Systems Integration Office
FY – Fiscal Year
FYHSP – Future Years Homeland Security Program
GAAP – U.S. Generally Accepted Accounting Principles
GAO – Government Accountability Office
GPO – Grants Policy Oversight
GSA – General Services Administration
HHS – Health and Human Services
HSDN – Homeland Security Data Network
HSGP – Homeland Security Grant Program
HSIN – Homeland Security Information Network
HSPD – Homeland Security Presidential Directive
HS SLIC – Homeland Security State and Local Intelligence Community of Interest
ICCB – Internal Control Coordination Board
ICE – U.S. Immigration and Customs Enforcement
ICGS – Integrated Coast Guard Systems
IDI – Injured Domestic Industries
IEFA – Immigration Examination Fee Account
IHP – Individuals and Household Programs
INA – Immigration Nationality Act
IP – Improper Payment
IPIA – Improper Payments Information Act of 2002
IPP – Infrastructure Protection Program
ISSM – Information System Security Managers

IT – Information Technology
MA – Mission Assignment
MD&A – Management's Discussion and Analysis
MEF – Mission Essential Functions
MERHCF – Medicare-Eligible Retiree Health Care Fund
MGMT – Management Directorate
MRS – Military Retirement System
NAO – National Applications Office
NAR – National CIKR Protection Annual Report
NCSD – National Cyber Security Division
NCTC – National Counterterrorism Center
NDHS – National Disaster Housing Strategy
NEMIS – National Emergency Management Information System
NFIP – National Flood Insurance Program
NIMS – National Incident Management System
NIPP – National Infrastructure Protection Plan
NPPD – National Protection and Programs Directorate
NSC – National Security Cutter
OAM – Office of Acquisition Management
OCFO – Office of the Chief Financial Officer
OCHCO – Office of the Chief Human Capital Officer
OCPO – Office of the Chief Procurement Officer
OHA – Office of Health Affairs
OIG – Office of Inspector General
OMB – Office of Management and Budget
OM&S – Operating Materials and Supplies
OPEB Other Post Retirement Benefits
OPM – Office of Personnel Management
ORB – Other Retirement Benefits
OSLTF – Oil Spill Liability Trust Fund
PA – Public Assistance
PA&E – Program Analysis and Evaluation
PAG – Peer Advisory Group
PART – Program Assessment Rating Tool
PBA – Performance Based Acquisitions
PIA – Privacy Impact Assessment
PKEMRA – Post-Katrina Emergency Management Response Act of 2006
P.L. – Public Law
PMA – President's Management Agenda
PMEF – Primary Mission Essential Functions
POA&M – Plan of Action and Milestones

PPBE – Planning, Programming, Budgeting, and Execution
PP&E – Property, Plant, and Equipment
PY – Prior Year
QHSR – Quadrennial Homeland Security Review
RSI – Required Supplementary Information
RSSI – Required Supplementary Stewardship Information
RTSWG – Regional Transit Security Working Groups
SAT – Senior Assessment Team
SBI – Secure Border Initiative
SBR – Statement of Budgetary Resources
SCC – Sector Coordinating Council
SFFAF – Statement of Federal Financial Accounting Standards
SFI – Secure Freight Initiative
SLFC – State and Local Fusion Center
SMC – Senior Management Council
SFRBTF – Sport Fish Restoration Boating Trust Fund
SORN – System of Records Notice
S&T – Science and Technology Directorate
STSI – Surface Transportation Security Inspectors
STSIP – Surface Transportation Security Inspection Program
TAFS – Treasury Account Fund Symbol
TSA – Transportation Security Administration
TSI – Transportation Security Inspector
TSNM – Transportation Security Network Management
UAS – Unmanned Aerial System
U.S. – United States
U.S.C. – United States Code
US-CERT - United States Computer Emergency Readiness Team
USCG – U.S. Coast Guard
USCIS – U. S. Citizenship and Immigration Services
USSGL – United States Standard General Ledger
USSS – U.S. Secret Service
US-VISIT – U.S. Visitor and Immigrant Status Indicator Technology
VIPR – Visible Intermodal Prevention and Response
WHTI – Western Hemisphere Travel Initiative
WMSL – Maritime Security Cutter, Large
WYO – Write Your Own

The Department of Homeland Security's FY 2008 Annual Financial Report is available at the following website:
http://www.dhs.gov/xabout/budget/editorial_0430.shtm

For more information or to obtain additional copies, contact:

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

par@dhs.gov
(202) 447-0333

Homeland
Security