Other Accompanying Information

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

Tax Burden/Tax Gap

Revenue Gap

The Entry Summary Compliance Measurement (ESCM) program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations, and agreements, and is used to produce a dollar amount for Estimated Net Undercollections and a percent of Revenue Gap. The Revenue Gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and trade agreements using a statistically valid sample of the revenue losses and overpayments detected during ESCM entry summary reviews conducted throughout the year. For FY 2009 and 2008, the Revenue Gap was $285 million and $396 million, respectively. CBP calculated the preliminary FY 2010 Revenue Gap to be $91 million. As a percentage, the preliminary Revenue Gap for FY 2010 represents less than 0.28 percent of all collectible revenue for the year, the lowest it has been in over five years. The estimated over collection and under collection amounts due to noncompliance for FY 2010 were $51 million and $142 million, respectively. The overall trade compliance rate for FY 2009 and FY 2008 is 98.2 and 97.6 percent, respectively. The preliminary overall compliance rate for FY 2010 is 99 percent.

The final overall trade compliance rate and estimated revenue gap for FY 2010 will be issued in February 2011.

Summary of Financial Statement Audit and Management Assurances

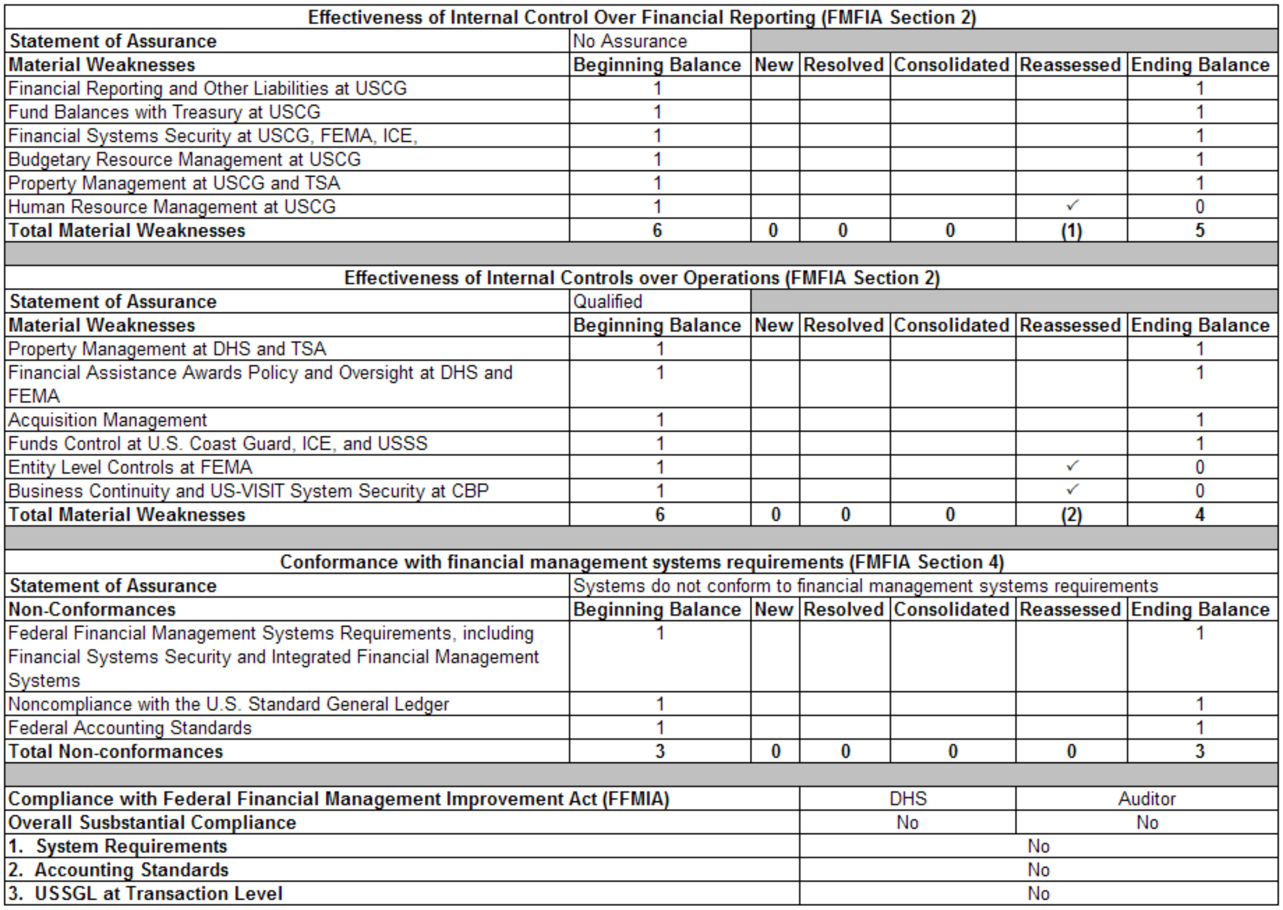
Table 1 and Table 2 below provide a summary of the financial statement audit and management assurances for FY 2010.

Table 1. FY 2010 Summary of the Financial Statement Audit

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

In FY 2010, the Independent Auditor's integrated financial statement and internal control report identified six material weakness conditions at the Department level; however, portions of prior year material weakness conditions were reduced in severity. For example, CBP implemented corrective actions to reduce the severity of Property, Plant, and Equipment deficiencies. CBP, FEMA, and TSA implemented corrective actions to reduce the severity of Financial Management and Reporting conditions. Finally, USCIS, ICE, TSA, and NPPD corrected several significant deficiencies at the consolidated level.

Table 2. FY 2010 Summary of Management Assurances



Effectiveness of Internal Control Over Financial Reporting (FMFIA Section 2)						
Statement of Assurance	No Assurance					
Material Weaknesses	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Financial Reporting and Other Liabilities at USCG	1					1
Fund Balances with Treasury at USCG	1					1
Financial Systems Security at USCG, FEMA, ICE,	1					1
Budgetary Resource Management at USCG	1					1
Property Management at USCG and TSA	1					1
Human Resource Management at USCG	1				✓	0
Total Material Weaknesses	**6**	**0**	**0**	**0**	**(1)**	**5**
Effectiveness of Internal Controls over Operations (FMFIA Section 2)						
Statement of Assurance	Qualified					
Material Weaknesses	**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**Ending Balance**
Property Management at DHS and TSA	1					1
Financial Assistance Awards Policy and Oversight at DHS and FEMA	1					1
Acquisition Management	1					1
Funds Control at U.S. Coast Guard, ICE, and USSS	1					1
Entity Level Controls at FEMA	1				✓	0
Business Continuity and US-VISIT System Security at CBP	1				✓	0
Total Material Weaknesses	**6**	**0**	**0**	**0**	**(2)**	**4**
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. Since FY 2005 DHS has reduced audit qualifications from ten to one and material weaknesses by more than half. In addition, the U.S. Coast Guard's Financial Strategy for Transformation and Audit Readiness has allowed us to increase the auditable balance sheet amounts to approximately ninety percent in FY 2010. Finally, in FY 2010, the Department completed a limited scope evaluation of processes that provide internal control over the Statement of Budgetary Resources, Changes in Net Position, and Net Cost.

DHS reported five material weakness conditions at the Department level in FY 2010, one less material weakness than reported on by the independent auditor. The difference between audit and management's conclusion results from reporting timing and classification differences. One example of the differing conclusion results is the independent audit reports on a U.S. Coast Guard Actuarial Liability material weaknesses that existed throughout FY 2010. Management's conclusion of the U.S. Coast Guard Actuarial Liability condition reports on the status and severity of the condition as of September 30, 2010 while considering interim compensating measures in place since June 30, 2010 that enable the Department to clear a $43 billion audit qualification related to U.S. Coast Guard Actuarial Liabilities. U.S. Coast Guard and the Department will work with the independent auditor in early FY 2011 to measure progress through an independent audit. In addition, 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, based on Federal Financial Systems Requirements (FFSR). The FFSR process definitions used by management aid corrective actions and facilitate development of standard controls and business processes.

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

Table 3. FY 2010 Internal Control Over Financial Reporting Corrective Actions

Material Weaknesses in Internal Controls Over Financial Reporting	Year Identified	DHS Component	Corrective Actions	Target Correction Date
Financial Management and Reporting: U.S. Coast Guard has 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	The DHS OCFO will continue efforts to support U.S. Coast Guard in implementing corrective actions to address staffing shortfalls and develop policies and procedures to establish effective financial reporting control activities.	FY 2012
IT Controls and System Functionality: The Department's Independent Public Auditor had identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to inherited control deficiencies surrounding general computer and application controls. The *Federal Information Security Management Act* mandates that Federal Agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance.	FY 2003	U.S. Coast Guard, FEMA, and ICE	The DHS OCFO and OCIO will support the U.S. Coast Guard, FEMA, and ICE to design and implement internal controls in accordance with *DHS 4300A Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Financial Systems.*	FY 2012
Fund Balance with Treasury: U.S. Coast Guard did not implement effective internal controls to accurately clear suspense transactions in order to perform accurate and timely reconciliations of Fund Balance with Treasury (FBWT) accounts.	FY 2004	U.S. Coast Guard	In FY 2010, U.S. Coast Guard made progress in reconciling FBWT payroll activity and will continue efforts to develop short-term compensating controls for non payroll FBWT activity, while longer-term corrective actions are implemented.	FY 2012
Property, Plant, and Equipment: The controls and related processes surrounding U.S. Coast Guard and TSA Property, Plant, and Equipment (PPE) to accurately and consistently record activity are either not in place or contain errors and omissions.	FY 2003	U.S. Coast Guard and TSA	CBP implemented corrective actions to reduce the severity of portions of the PPE material weakness. In addition, U.S. Coast Guard implemented corrective actions to correct Operating Materials and Supplies conditions. TSA made progress towards implementing policies and procedures to identify and account for software capitalization in accordance with Statement of Federal Financial Accounting Standard (SFFAS) No. 10, *Accounting for Internal Use Software* . U.S. Coast Guard will implement policies and procedures to support completeness, existence, and valuation assertions for PPE. The DHS OCFO will continue efforts to support U.S. Coast Guard and TSA implementing corrective actions to address capital asset conditions and develop policies and procedures to establish effective financial reporting control activities.	FY 2012
Budgetary Accounting: Policies and procedures over obligations, disbursements, and validation and verification of undelivered orders for accurate recording of accounts payable were not effective.	FY 2004	U.S. Coast Guard	U.S. Coast Guard developed corrective actions to improve budgetary accounting. However, corrective actions may extend beyond FY 2011 due to resource constraints and magnitude of other corrective actions.	FY 2012
Actuarial and Other Liabilities: U.S. Coast Guard has not completely implemented policies and procedures to account for actuarial liabilities. In addition, internal control weaknesses exist in developing estimates for accounts payable and environmental liabilities at U.S. Coast Guard.	FY 2006	U.S. Coast Guard	U.S. Coast Guard implemented corrective actions in FY 2010 to provide management representations and clear a $43 billion audit qualification related to actuarial liabilities. Progress was made in developing accounts payable estimates, however additional actions will be implemented in FY 2011 to refine estimates. Corrective actions for environmental liabilities will be taken in coordination with PPE corrective actions to develop a complete population of locations where environmental liabilities exists.	FY 2011

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 fourth consecutive year, we have made tremendous progress in strengthening Department-wide internal controls over operations, as evidenced by the following FY 2010 achievements:

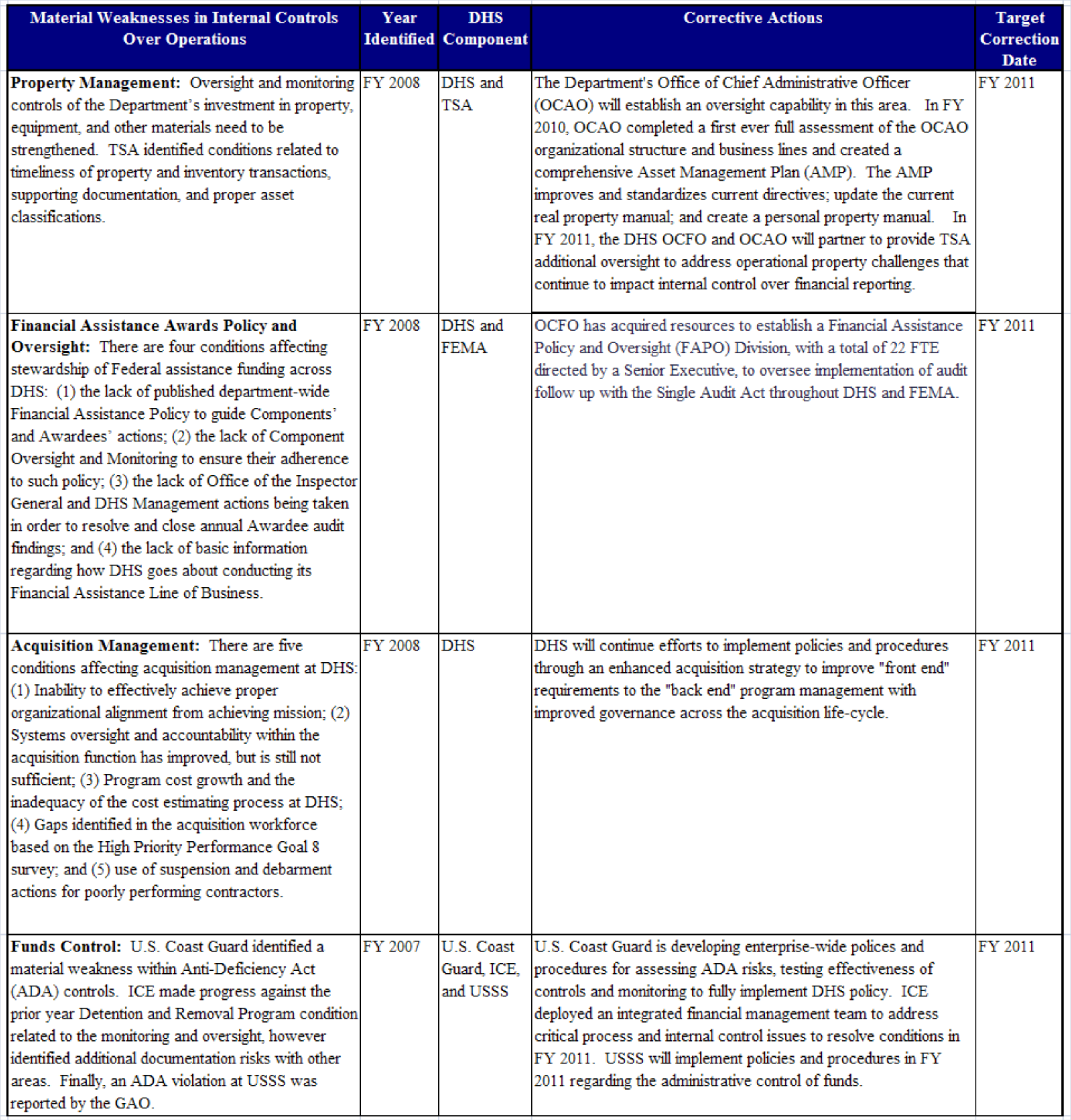
- Transformed relations with the U.S. Government Accountability Office (GAO) through issuance of DHS/GAO Protocols and established an audit follow up governance process to improve the efficiency and effectiveness of operations.
- Developed the first-ever DHS Secretary's Workforce Strategy. The Office of the Chief Information Officer was selected as the Pilot Program for the DHS Balanced Workforce Initiative and has successfully implemented Human Resource and Career Development Strategies.
- Received a grade of "A" from the Small Business Administration for success in contract awards. Increased competition rate from 74 percent to 86 percent between FY 2009 and FY 2010. Implemented a Quarterly Operational Assessment measuring specified metrics. Conducted oversight reviews at three Components as well as five DHS-wide reviews, resulting in numerous recommendations for improvement and identification of best practices. Updated the Homeland Security Acquisition Manual to reflect new regulatory and policy requirements.
- The Acquisition Professional Career Program continues to build momentum with 200 participants on-board by September 30, 2010. Professional certification programs have been created for contract specialists, contracting officer's technical representatives, program managers, and test and evaluators. The Office of the Chief Procurement Officer has developed ethics training geared specifically for those individuals who have responsibility for participating in the procurement process.
- Directive 102-01 and a new revision of the Systems Engineering Life Cycle were signed out. Ten Portfolio-based Reviews were conducted this fiscal year. Eight Component Acquisition Executives have been designated. Governance through Executive Steering Committees (ESCs) has been established over high-priority programs such as Transformation and Systems Consolidation (TASC).
- Execution of planned FY 2010 Data Center Consolidation is on track for ICE, USCIS, FEMA, NPPD, and TSA. OneNet Network transitions are ahead of schedule where 95 percent of all transition items are on the GSA contract. A Common Operating Environment has been established with development and test capabilities to be migrated to this rapid provisioning environment.
- Completed a first ever full assessment of the Office of the Chief Acquisition Officer organizational structure and business lines. The purpose of the full assessment is to provide an organizational roadmap and playbook for optimizing the efficiencies and effectiveness of administrative business lines.

- Created a comprehensive Asset Management Plan (AMP). The AMP improves and standardizes current directives; update the current real property manual; and create a personal property manual.
- The DHS HSPD-12 Program, under the direction of the Office of the Chief Security Officer, ended FY 2010 with the issuance of 115,546 Personal Identity Verification cards to DHS employees and contractors. Over this same period of time, card issuance workstations were deployed to more than 130 DHS locations. HSPD-12 has fostered greater collaboration and opportunities for improving how DHS handles information related to employees' identification through all business processes. Plans are in progress for ensuring physical and logical access is efficient across the Department.
- Finalized construction on the DHS Headquarters perimeter security design project that began in February 2010. At present, 40 percent of the perimeter fencing is complete; the vehicle screening building is scheduled for completion and turnover in December 2010; and the security command center is scheduled for completion in April 2011. Its completion and use will be a major milestone in establishing an effective emergency and crisis-response capability.
- The Office of the Chief Security Officer (OCSO) coordinated with State, local, tribal and private sector partners to conduct 51 on-site Fusion Center visits. These trips consisted of pre-construction meetings and post-construction/certification surveys for Fusion Center secure rooms, security training, and attendance at regional Fusion Center conferences. Safeguarding National Security Information training and specialized training was presented at 13 sites. The OCSO certified 18 Fusion Center Secure Rooms to support the Intelligence and Analysis sponsored Homeland Security Data Network deployment to State Fusion Centers.

To address challenges to internal control over operations, the Department's Under Secretary for Management conducts weekly Senior Management Council Oversight meetings.

Table 4 summarizes material weaknesses in internal control over operations as well as planned corrective actions with estimated target correction dates.

Table 4. FY 2010 Internal Control Over Operations Corrective Actions



Material Weaknesses in Internal Controls Over Operations	Year Identified	DHS Component	Corrective Actions	Target Correction Date
Property Management: Oversight and monitoring controls of the Department's investment in property, equipment, and other materials need to be strengthened. TSA identified conditions related to timeliness of property and inventory transactions, supporting documentation, and proper asset classifications.	FY 2008	DHS and TSA	The Department's Office of Chief Administrative Officer (OCAO) will establish an oversight capability in this area. In FY 2010, OCAO completed a first ever full assessment of the OCAO organizational structure and business lines and created a comprehensive Asset Management Plan (AMP). The AMP improves and standardizes current directives; update the current real property manual; and create a personal property manual. In FY 2011, the DHS OCFO and OCAO will partner to provide TSA additional oversight to address operational property challenges that continue to impact internal control over financial reporting.	FY 2011
Financial Assistance Awards Policy and Oversight: There are four conditions affecting stewardship of Federal assistance funding across DHS: (1) the lack of published department-wide Financial Assistance Policy to guide Components' and Awardees' actions; (2) the lack of Component Oversight and Monitoring to ensure their adherence to such policy; (3) the lack of Office of the Inspector General and DHS Management actions being taken in order to resolve and close annual Awardee audit findings; and (4) the lack of basic information regarding how DHS goes about conducting its Financial Assistance Line of Business.	FY 2008	DHS and FEMA	OCFO has acquired resources to establish a Financial Assistance Policy and Oversight (FAPO) Division, with a total of 22 FTE directed by a Senior Executive, to oversee implementation of audit follow up with the Single Audit Act throughout DHS and FEMA.	FY 2011
Acquisition Management: There are five conditions affecting acquisition management at DHS: (1) Inability to effectively achieve proper organizational alignment from achieving mission; (2) Systems oversight and accountability within the acquisition function has improved, but is still not sufficient; (3) Program cost growth and the inadequacy of the cost estimating process at DHS; (4) Gaps identified in the acquisition workforce based on the High Priority Performance Goal 8 survey; and (5) use of suspension and debarment actions for poorly performing contractors.	FY 2008	DHS	DHS will continue efforts to implement policies and procedures through an enhanced acquisition strategy to improve "front end" requirements to the "back end" program management with improved governance across the acquisition life-cycle.	FY 2011
Funds Control: U.S. Coast Guard identified a material weakness within Anti-Deficiency Act (ADA) controls. ICE made progress against the prior year Detention and Removal Program condition related to the monitoring and oversight, however identified additional documentation risks with other areas. Finally, an ADA violation at USSS was reported by the GAO.	FY 2007	U.S. Coast Guard, ICE, and USSS	U.S. Coast Guard is developing enterprise-wide polices and procedures for assessing ADA risks, testing effectiveness of controls and monitoring to fully implement DHS policy. ICE deployed an integrated financial management team to address critical process and internal control issues to resolve conditions in FY 2011. USSS will implement policies and procedures in FY 2011 regarding the administrative control of funds.	FY 2011

Federal Financial Management Improvement Act

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

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

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

Financial Management Systems – Transformation and Systems Consolidation (TASC)

The mission support systems inherited in the stand up of the Department of Homeland Security had serious limitations, based on an assessment conducted in 2003. Specifically, financial systems failed to meet Government standards for accounting, internal controls, and reporting. Significant portions of the DHS financial reports are manually populated with financial data that reside in multiple and varying acquisition and asset systems. DHS faces enormous manual reconciliation tasks and time-consuming complexities of recording accurate, consistent, and timely obligations.

To start to address these deficiencies in DHS financial reporting accuracy and timeliness, the Department is preparing to award the TASC contract, which will enable the Department to move forward with the standardization of business processes and fiscal reporting capabilities.

DHS is seeking approval for the TASC program to award the Indefinite Delivery Indefinite Quantity (IDIQ) contract and initial task orders. Upon award of the contract, the Department has determined, based on business need and factors for successful implementation, that FEMA will be the first Component to migrate to the TASC solution. Once the successful implementation of the initial migration is completed, the TASC Program Management Office will request OMB approval to begin migrating additional Components based on business need and risk factors.

Federal Information Security Management Act (FISMA)

The *E-Government Act of 2002* (Pub. L. 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 2010 Federal Information Security Management Act Report and Privacy Management Report consolidates reports from three DHS offices:

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

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, the OIG in FY 2010 identified progress the Department has made on the following ten key areas of DHS's information system security program:

- System Inventory;
- Certification and Accreditation Process;
- Plan of Action and Milestones;
- Incident Response and Reporting;
- Security Training;
- Remote Access;
- Account and Identity Management;
- Continuous Monitoring;
- Contingency Planning Program; and
- Privacy.

The Department continues to improve and strengthen its security program. The OIG report, "Evaluation of DHS' Information Security Program for Fiscal Year 2010," identified seven recommendations for information security improvements. DHS plans to update the DHS Information Security Performance Plan with enhanced metrics further improving compliance in these areas.

Improper Payments Information Act

The *Improper Payments Information Act* (IPIA) *of 2002* (Pub. L. 107-300) requires agencies to review their programs and activities to identify those susceptible to significant improper payments. In addition, Section 831 of the FY 2002 *Defense Authorization Act* (Pub. L. 107-107) established the requirement for Government agencies to carry out cost-effective programs for identifying and recovering overpayments made to contractors, also known as "Recovery Auditing." The OMB has established specific reporting requirements for agencies with programs that possess a significant risk of improper payments and for reporting on the results of recovery auditing activities.

The IPIA was amended on July 22, 2010 by the *Improper Payments Elimination and Recovery Act* (IPERA) of 2010 (Pub. L. 111-204). IPERA reporting requirements for the Annual Financial Report will not go into effect until FY 2011.

I. Risk Assessments

In FY 2010, risk assessments were conducted on 99 DHS programs, totaling $57 billion in FY 2009 disbursements. Assessments were not conducted on programs with total disbursements less than $10 million. All payment types were assessed except for Federal intra-governmental payments which were excluded after consultation and concurrence with OMB and OIG.

Improper payment estimates in this section are based on statistical estimates for FY 2009. These estimates are then projected for FY 2010 and beyond based on improvements expected from completing corrective actions.

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

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

- Operating Environment – Existence of factors which necessitate or allow for loosening of financial controls. Any known instances of fraud. Management's experience with designing and implementing compensating controls.
- Additional Grant Programs Factors – Federal Audit Clearinghouse information on quality of controls within grant recipients. Identification of deficiencies or history of improper payments within recipients. Type and size of program recipients and sub-recipients. Maturity of recipients' financial infrastructure, experience with administering Federal payments, number of vendors being paid, and number of layers of sub-grantees.

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

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

Table 5. Programs at High-Risk for Improper Payments Based on FY 2010 Risk Assessments and Prior Year Payment Sample Testing[1]

Component	Program Name	Disbursements ($ Millions)
CBP	Border Security Fencing	$638
	Custodial – Refund & Drawback	$1,436
FEMA	Disaster Relief Program – Individuals and Households Program (IHP)	$848
	Disaster Relief Program – Vendor Payments	$1,382
	Insurance – National Flood Insurance Program (NFIP)	$3,287
	Grants – Public Assistance Programs (PA)	$5,070
	Grants – Homeland Security Grant Program (HSGP)	$1,300
	Grants – Assistance to Firefighters Grants (AFG)	$429
	Grants – Transit Security Grants Program (TSGP)	$119
ICE[2]	Detention and Removal Operations (DRO)	$1,320
	Federal Protective Service (FPS)	$760
TSA	Aviation Security – Payroll	$2,383
USCG	Active Duty Military Payroll (ADMP)	$2,766
Total Disbursements		**$21,738.00738**

Notes:

1. In FY 2009, OMB granted relief from measuring and reporting annual improper payment information for four programs that DHS tested and reported estimated error amounts below $10 million. These programs were: (1) At CBP – Continued Dumping & Subsidy Offset Act & Payments to Wool Manufacturers, (2) At ICE – Investigations, (3) At USCG – Contract payments for Acquisition, Construction & Improvements and (4) At USCG – Contract payments for Operating Expenses (OE). The next year that DHS will report on these four programs will be in its FY 2013 Annual Financial Report.
2. Only the non-payroll portion of ICE programs was found to be high-risk. Disbursement figures are for non-payroll disbursements.

II. Statistical Sampling Process

For FY 2010 reporting, a stratified sampling design was used to test payments based on FY 2009 disbursement amounts and the assessed risk of the program. The design of the statistical sample plans and the extrapolation of sample errors across the payment populations were completed by a statistician under contract.

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

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

The following procedure describes the sample selection process:

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

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

DHS sample test results are listed in Table 6.

Table 6. DHS Sample Test Results

Component	Program	FY 2009 Payment Population ($millions)	FY 2009 Sample Size ($millions)	Est. Error Amount ($millions)	Est. Error Percentage (%)
CBP	Border Security Fencing	$638	$527	$0	0.03%
	Refund & Drawback	$1,436	$237	$3	0.20%
FEMA	Disaster Relief Program – Individuals and Households Program (IHP)	$848	$4	$23	2.72%
	Disaster Relief Program – Vendor Payments	$1,382	$506	$46	3.32%
	Insurance – National Flood Insurance Program (NFIP)	$3,287	$42	$73	2.22%
	Grants – Public Assistance Programs (PA)[1]	$706	$566	$1	0.21%
	Grants – Homeland Security Grant Program (HSGP)[2]	$115	$92	$2	2.20%
	Grants – Assistance to Firefighters Grants (AFG)	$429	$50	$27	6.32%
	Grants – Transit Security Grants Program (TSGP)[3]	$16	$16	$0	0.09%
	Grants – Emergency Food and Shelter Program (EFSP), ARRA Payments	$86	$17	$5	6.18%
ICE	Detention and Removal Operations[4]	$1,320	$254	$7	0.53%
	Federal Protective Service[4]	$760	$127	$1	0.10%
TSA	Aviation Security – Payroll	$2,383	$2	$0	0.00%
USCG	Operating Expenses - Active Duty Military Payroll	$2,766	$3	$4	0.13%
DHS	**All Programs[5]**	**$16,172**	**$2,443**	**$192**	**1.19%**
DHS	**High-Risk Programs (Est. Error Amount >$10 Million)**	**$5,946**	**$602**	**$169**	**2.84%**

Notes:

1. Sample testing of the Public Assistance Program was done in two stages covering six states (AR, IL, IN, LA, OH, and TX). The six states paid out $3,006 million out of a national total of $5,070 million. The totals in the table are the stage two payment populations for the six states tested. See the Outlook projection table for the national estimated error of $11 million.
2. Sample testing of the Homeland Security Grant Program was done in two stages covering eight states (CO, FL, MI, MO, NV, OH, PA, WA) and Washington, DC. These regions paid out $312 million out of a national total of $1,300 million. The totals in the table are the stage two payment populations for the nine regions. See the Outlook projection table for the national estimated error of $29 million.
3. Sample testing of the Transit Security Grant Program was done in two stages covering eight states (CO, FL, MI, MO, NV, OH, PA, WA) and Washington, DC. These regions paid out $20 million out of a national total of $119 million. The totals in the table are the stage two payment populations for the nine regions. See the Outlook projection table for the national estimated error of $0 million.
4. The estimated error total for Detention and Removal Operations includes $341,829 of duplicate payments which were issued on two Treasury schedules that were paid twice in FY 2009. Federal Protective Service duplicate payments on the same Treasury schedules totaled $13,217.
5. Program total of $16,172 in this table differs from $21,738 total in Improper Payment Reduction Outlook Table for several reasons. For State Administered Grant Programs, the table above lists the population totals for the States tested while the Improper Payment Reduction Outlook Table lists the national payment populations. FEMA's EFSP ARRA Payments are listed above as they were sample tested to meet the improper payment objectives listed in the Recovery Act. They are not listed in the Improper Payment Reduction Outlook Table due to the non-recurring nature of this funding.

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.

Based on the results of sample testing, corrective action plans are required for the following six programs due to estimated error amounts above $10 million: FEMA’s Assistance to Firefighters Grants, FEMA’s Disaster Relief Program - Vendor Payments, FEMA’s Homeland Security Grant Program, FEMA’s Individuals and Households Program, FEMA’s National Flood Insurance Program, and FEMA’s Public Assistance Program.

III. Corrective Action Plans for High-Risk Programs

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

FEMA Assistance to Firefighter Grants Program

Table 7. Completed Assistance to Firefighters Grants Program Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Insufficient Supporting Documentation		
1. Missing invoice.	1. Provide applicants with examples of proper supporting documentation when award is granted.	February 2010
Category of Error: Purchases Outside Allowable Timeframe		
2. Purchases before or after the period of performance.	1. If an advance payment is requested, ask applicants whether arrangements have been made to purchase the goods within 30 days of receipt of funding.	January 2010

Table 8. Planned Assistance to Firefighter Grants Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Supporting Documentation		
1. Grantee was unable to provide supporting documentation relevant to grant payments.	1. Guidance – Develop and distribute to all Grantees a "Grantee Supporting Documentation Retention Strategy" detailing the types of supporting documentation Grantees should retain at each phase of the grant life cycle.	May 2011
	2. Training – Require each grantee to complete the AFG Grant Management Tutorial.	May 2011 (and ongoing)
Category of Error: Purchase Outside Allowable Timeframe		
2. Invoices for purchases from sub-grantees fell outside of the period of performance.	1. System Enhancements – Develop and deploy a modification email notification to be sent to Grantees through AFG System towards the end of the period of performance (at nine months and eleven months) alerting Grantees to make purchases before the deadline.	May 2011
	2. Training – Require each grantee to complete the AFG Grant Management Tutorial	May 2011 (and ongoing)
Category of Error: Drawdown Outside Allowable Timeframe		
3. Grantee received funds beyond 90 days following expiration of the period of performance.	1. System Enhancements – Develop and deploy a modification email notification to be sent to Grantees through AFG System towards the end of the period of performance (at nine months and eleven months) alerting Grantees to make purchases before the deadline.	May 2011
	2. Training – Require each grantee to complete the AFG Grant Management Tutorial.	May 2011 (and ongoing)
Category of Error: Vehicle Down Payment Exceeds 25% of Federal Share		
4. Grantee received and used grant funds that in excess of 25% of the Federal Share.	1. Process Improvement – Implement a quality control process in which vehicle acquisition related payments requests are reviewed by at least two AFG Program specialists.	May 2011
	2. Training – Require each grantee to complete the AFG Grant Management Tutorial.	May 2011 (and ongoing)

FEMA Disaster Relief Program - Vendor Payments

Table 9. Completed Disaster Relief Program Vendor Payments Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Contract Administration		
1. Payment made outside period of performance.	1. Grant access to Pro Trac for appropriate staff.	March 2010
2. Unauthorized staff approved invoices.	2. Document the delegation of authority	March 2010
Category of Error: Payment Errors		
1. Improper invoice.	1. Require that specific information be provided on each invoice.	March 2010
	2. Provide access to supporting documentation in Pro Trac to verify invoice adjustments.	March 2010
2. Missing documents.	3. Require authorized officials to provide supporting documentation with payment requests.	March 2010

Table 10. Planned Disaster Relief Program Vendor Payments Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Contract Administration		
1. Improper Authorization of responsibilities to individuals and unauthorized sign off of payments.	1. Guidance – Revise Acquisition Manual to include a chapter on OCPO roles and responsibilities for contract payments.	May 2011
	2. Process Improvement – Evaluate the ability to upload COTR appointment letter to Pro Trac.	February 2011
	3. Training – Institute mandatory refresher training for contracting officers, contracting officer technical representatives and accounting technicians.	May 2011 (and ongoing)
Category of Error: Payment Errors		
2. Proper invoices not submitted in accordance with contract terms.	1. Guidance – Revise Acquisition Manual to include a chapter on OCPO roles and responsibilities for contract payments.	May 2011
	2. Guidance – Revise contracting officer technical representative handbook to include standard procedures for reviewing invoices.	May 2011
	3. Training – Institute mandatory refresher training for contracting officers, contracting officer technical representatives and accounting technicians.	May 2011 (and ongoing)

FEMA Homeland Security Grant Program

Table 11. Completed Homeland Security Grant Program Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Insufficient Supporting Documentation		
1. Sub-grantees could not provide documentation to support payment requests.	1. Incorporate compliance with external documentation requests as a key metric to be taken into account when evaluating future grant applications.	February 2010
	2. Establish responsiveness and timeliness standards to assess compliance with documentation requests throughout the grant process.	March 2010
	3. Develop a standardized document retention protocol and provide training.	March 2010
	4. Require a certification statement from sub-grantee that all funds will be applied to transactions occurring within the period of performance.	April 2010

Table 12. Planned Homeland Security Grant Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Noncompliance with Allowable Cost Guidelines		
1. Exceeding of $1,000,000 construction cost limitation without approval; changes to allowable cost items from one fiscal year to the next not followed by grantees.	1. Guidance – Modify guidance to expand on the requirements related to construction costs. Disallow reimbursement for construction costs which lack proper documentation.	February 2011
	2. Training – Develop a standardized construction cost training program. Provide classroom and electronic training.	March 2011
	3. Process Improvement – Require Grantees and Sub-Grantees to provide additional documentation with the invoices to confirm that expenditures are within allowable cost guidelines.	January 2011
	4. State Oversight – Identify best practices across States and promote nationally.	March 2011

FEMA Individuals and Households Program

Table 13. Planned Individuals and Households Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Case Processing Errors		
1. Applicants received payments without supplying necessary documentation; misinterpreting submitted insurance documents.	1. Guidance – Improve caseworker guidance for high risk payment types.	May 2011
	2. System Enhancements – Continue development of NEMIS Help Text including tips and relevant disaster specific guidance.	May 2011 (and ongoing)
	3. Training – Provide caseworker training focusing on new guidance and insurance coverage policies and processing procedures.	May 2011 (and ongoing)
Category of Error: Calculation Errors		
2. Incorrect calculations or applications of Fair Market Rent; valid claims from second inspection were unpaid.	1. System Enhancements - Improve NEMIS or Infoview report platform to ensure accurate processing of awards generated by multiple inspections.	May 2011 (and ongoing)
	2. Guidance – Improve caseworker guidance for use of Fair Market Rent.	May 2011 (and ongoing)
Category of Error: Overlapping Assistance		
3. Transient Sheltering Assistance overlapping with rental assistance due to timing issues.	1. Guidance – Improve caseworker guidance on overlapping assistance risks.	May 2011
	2. System Enhancements – Continue development of NEMIS Help Text including tips and relevant disaster specific guidance.	May 2011 (and ongoing)
Category of Error: Duplication of Benefits		
4. Second inspection resulted in repayment of same line item.	1. Guidance – Improve caseworker guidance on second review risk issues.	May 2011
	2. System Enhancements – Continue development of NEMIS Help Text on second review risks.	May 2011 (and ongoing)

FEMA National Flood Insurance Program

Table 14. Completed National Flood Insurance Program Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Incorrect Payment Calculations and Payment Processing Errors		
1. Misapplied profit costs and fees; improper determination of scope; incorrect application of coverage; insufficient itemization on estimates and inventories; incorrect application of special coverage limits.	1. Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	June 2010
Category of Error: Insufficient Damage Documentation		
1. Lack of invoices, inventories, and estimates.	1. Conduct educational workshops at the annual National Flood Conference and other industry national and regional conferences.	June 2010
2. No direct physical damage documentation.	2. Emphasize damage documentation requirements in the adjuster claims manual when it is updated.	May 2010

Table 15. Planned National Flood Insurance Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Insufficient Damage Documentation		
1. Lack of invoices, inventories, estimates and other supporting documentation.	1. Training – Conduct educational workshops at the annual National Flood Conference and other industry and regional conferences.	May 2011
	2. Process Improvement – Document improvements coming from IPIA findings and incorporate into Claims Operation Review procedures.	June 2011
Category of Error: Payment Processing Errors		
2. Incorrect or lacking mortgagee or other lienholder information on payment.	1. Training – Conduct educational workshops at the annual National Flood Conference and other industry and regional conferences.	May 2011
	2. Process Improvement – Document improvements coming from IPIA findings and incorporate into Claims Operation Review procedures.	June 2011

Risk Factors	Corrective Actions	Target Completion Date
	3. System Enhancements – Develop a Claims Operation Review Data Capture Tool to be utilized by NFIP management that records findings and tracks progress on identified errors.	July 2011
Category of Error: Incorrect Estimate/Worksheet Calculation		
3. Incorrect application of coverage, depreciation not applied correctly, and inadequate management controls.	1. Training – Conduct educational workshops at the annual National Flood Conference and other industry and regional conferences.	May 2011
	2. Process Improvement – Document improvements coming from IPIA findings and incorporate into Claims Operation Review procedures.	June 2011
	3. System Enhancements – Develop a Claims Operation Review Data Capture Tool to be utilized by NFIP management that records findings and tracks progress on identified errors.	July 2011

FEMA Public Assistance Program

Note: FEMA's Public Assistance Program had a very low estimated error rate of 0.21%. The risk factors below were seldom encountered but were responsible for a national estimated error amount greater than $10 million.

Table 16. Completed Public Assistance Program Corrective Actions

Risk Factors	Corrective Actions	Completed Date
Category of Error: Insufficient Costs Documentation		
1. Insufficient supporting documentation.	1. Standardize record keeping.	March 2010
	2. Provide record keeping guidance and training.	April 2010
Category of Error: Out-of-Scope Payments		
2. Payments were made outside the period of performance.	1. Provide documentation review guidance to grantees.	April 2010
	2. Provide guidance and training for Category Z project worksheets.	April 2010
Category of Error: Unmet Work Completion Deadline		
3. Documentation was not obtained and/or retained to substantiate valid work extensions.	1. Develop documentation review checklists.	February 2010
	2. Provide guidance and training to grantees on correct invoice review policies.	March 2010
	3. Develop guidance to store work extension documentation with project worksheet in system of record.	February 2010

Risk Factors	Corrective Actions	Completed Date
	4. Modify standard operating procedures to include record keeping guidance.	February 2010
Category of Error: Missing Payment Verification Documentation		
4. Documentation was not obtained and/or retained to substantiate that the correct sub-grantee was paid	1. Develop documentation retention policies.	April 2010

Table 17. Planned Public Assistance Program Corrective Actions

Risk Factors	Corrective Actions	Target Completion Date
Category of Error: Incorrect SMARTLINK Drawdown		
1. Drawdown taken from an incorrect disaster.	1. Process Improvement – Implement additional internal controls for Grantees with more than one open disaster to ensure project costs are linked to correct disaster.	November 2010
	2. System Enhancements – Encourage States to implement automated controls.	November 2010
Category of Error: Missing Payment Verification Documentation		
2. Lack of payment verification documentation which demonstrates correct Sub-grantee was paid.	1. Process Improvement – Improve Grantee retention and access to payment verification documentation.	November 2010
	2. Monitoring – Increase FEMA's monitoring of Grantee distribution of funds to Sub-grantees.	November 2010 (and ongoing)

IV. Program Improper Payment Reporting

Table 18 summarizes improper payment amounts for DHS high-risk programs and projects future year improvements based on completing corrective actions. Improper payment percent (IP%) and improper payment dollar (IP$) figures are based on statistical estimates for FY 2009. These estimates are then projected for FY 2010 and beyond based on improvements expected from completing corrective actions.

Table 18. Improper Payment Reduction Outlook

Improper Payment Reduction Outlook
($ in millions)

Program	FY 2009 Outlays	FY 2009 IP%	FY 2009 IP$	FY 2010 Outlays	FY 2010 Est. IP%	FY 2010 Est. IP$	FY 2011 Est. Outlays	FY 2011 Est. IP%	FY 2011 Est. IP$	FY 2012 Est. Outlays	FY 2012 Est. IP%	FY 2012 Est. IP$
Border Security Fencing (CBP)	$638	0.03%	$0	$562	0.01%	$0	$600	0.00%	$0	$600	0.00%	$0
Refund & Drawback (CBP)	$1,436	0.20%	$3	$1,198	0.20%	$2	$1,350	0.07%	$1	$1,350	0.07%	$1
IHP (FEMA)	$848	2.72%	$23	$845	1.25%	$11	$845	1.00%	$8	$845	0.75%	$6
Disaster Relief Program Vendor Payments (FEMA)	$1,382	3.32%	$46	$1,396	3.00%	$42	$1,410	2.50%	$35	$1,424	2.00%	$28
NFIP (FEMA)	$3,287	2.22%	$73	$3,287	2.00%	$66	$3,287	1.75%	$58	$3,287	1.50%	$49
PA (FEMA)	$5,070	0.21%	$11	$5,070	0.19%	$10	$5,070	0.17%	$9	$5,070	0.15%	$8
HSGP (FEMA)	$1,300	2.20%	$29	$1,430	2.00%	$29	$1,573	1.75%	$28	$1,730	1.50%	$26
AFG (FEMA)	$429	6.32%	$27	$438	4.25%	$19	$446	4.00%	$18	$455	3.50%	$16
TSGP (FEMA)	$119	0.09%	$0	$122	0.09%	$0	$125	0.09%	$0	$127	0.09%	$0
DRO (ICE)	$1,320	0.53%	$7	$1,414	0.25%	$4	$1,442	0.12%	$2	$1,471	0.06%	$1
FPS (ICE)	$760	0.10%	$1	$785	0.10%	$1	$809	0.10%	$1	$833	0.10%	$1
Aviation Security – Payroll (TSA)	$2,383	0.00%	$0	$2,518	0.00%	$0	$2,793	0.00%	$0	$2,999	0.00%	$0
ADMP (USCG)	$2,766	0.13%	$4	$2,927	0.13%	$4	$3,006	0.13%	$4	$3,068	0.13%	$4
All Programs	**$21,738**	**1.02%**	**$223**	**$21,992**	**0.84%**	**$186**	**$22,756**	**0.72%**	**$163**	**$23,259**	**0.60%**	**$140**

Note: For the three FEMA programs which were not tested nationally—HSGP, Public Assistance (PA) and TSGP—the error rate from the state(s) tested was applied to the national payment population to produce the estimated error amounts listed above.

Recovery of Improper Payments

ICE paid two Treasury schedules twice on June 15 and 16, 2009. Total duplicate payments were $1,789,764 for USCIS and $11,545,347 for ICE. All duplicate payments were recovered within 180 days.

V. Recovery Auditing Reporting

DHS completed recovery audit work for FY 2009 disbursements and continued collection activities for errors identified in prior year recovery audits. Work was completed at ICE, U.S. Coast Guard, and the Components they cross-service. Work was also completed at CBP and FEMA. In Table 19 which follows, current year (CY) equals FY 2009 disbursements and prior year (PY) covers FY 2005–FY 2008 for DNDO, TSA, and U.S. Coast Guard; FY 2004–FY 2008 for CBP, ICE, MGMT, NPPD, S&T, and USCIS; and FY 2009 for FEMA. Total Amounts Recovered PYs ($000) were adjusted from $292 to $245 at CBP, from $1,730 to $1,724 at ICE, and from $905 to $897 at USCIS to reflect items previously identified for recovery that were subsequently determined to be invalid.

Table 19. Recovery Audit Results

DHS Component	Amount Subject to Review for CY Reporting ($ Millions)	Actual Amount Reviewed and Reported CY ($ Millions)	Amounts Identified for Recovery CY ($000)	Amounts Recovered CY ($000)	Amounts Identified for Recovery PYs ($000)	Amounts Recovered PYs ($000)	Cumulative Amounts Identified for Recovery (CY + PYs) ($000)	Cumulative Amounts Recovered (CY + PYs) ($000)
CBP	$2,397	$2,397	$5	$14	$245	$231	$250	$245
DNDO	$206	$206	$0	$1	$1	$0	$1	$1
FEMA	$1,549	$1,549	$0	$0	$178	$0	$178	$0
ICE	$2,698	$2,698	$24	$30	$1,724	$1,557	$1,748	$1,587
MGMT	$465	$465	$2	$16	$172	$153	$174	$169
NPPD	$478	$478	$0	$0	$190	$190	$190	$190
S&T	$373	$373	$0	$0	$54	$54	$54	$54
TSA	$2,478	$2,478	$0	$0	$722	$722	$722	$722
USCG	$2,970	$2,970	$0	$9	$107	$82	$107	$91
USCIS	$1,105	$1,105	$7	$11	$897	$866	$904	$877
Totals	**$14,719**	**$14,719**	**$38**	**$81**	**$4,290**	**$3,855**	**$4,328**	**$3,936**

VI. Ensuring Management Accountability

The goals and requirements of Presidential Executive Order 13520, "Reducing Improper Payments and Eliminating Waste in Federal Programs (November 20, 2009)" were communicated repeatedly to all levels of staff throughout the Offices of the Chief Financial Officer and to relevant program office and procurement staff. Further, presentations and summary papers were circulated on OMB and Treasury Implementing Guidance on Executive Order 13520, the High-Dollar Overpayments Report, IPERA, the Presidential Memorandum on Recapturing Improper Payments, the DHS "Do Not Pay List" Plan, and the improper payments goals listed in the *American Recovery and Reinvestment Act*.

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

VII. Agency Information Systems and Other Infrastructure

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

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

VIII. Statutory or Regulatory Barriers

None.

IX. Overall Agency Efforts

The Department focused its FY 2010 efforts on supporting Presidential Executive Order 13520, sustaining compliance with the *Improper Payments Information Act* (first achieved in FY 2009), and supporting FEMA's efforts to expand improper payments testing of grant programs. The Department took an active role in several Government-wide groups looking at issues related to reducing improper payments to deepen our knowledge base and to remain alert to emerging requirements.

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 0.004 percent and 0.013 percent for the period of October 2009 through September 2010, with an annual average of 0.007 percent   (Note: MTS statistics are reported with at least a six week lag).

Debt Collection Improvement Act (DCIA)

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

FY 2009 Biennial User Charges Review

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

To ensure compliance with this biennial requirement, each DHS Component is required to compile and furnish individual summaries for each type of user fee by addressing the key points for each user fee, in sufficient detail, to facilitate a review by the OCFO. For FY 2009, six DHS Components were responsible for collecting user fees covering various services provided to the traveling public and trade community. The following is a detailed analysis of the fee collections and costs of the related services:

- ***U.S. Customs and Border Protection (CBP)*** – CBP collects user fees for services provided in connection with the processing of commercial air and commercial vessel passengers and loaded or partially loaded railroad cars carrying passengers or commercial flights arriving into the customs territory. CBP inspection user fee collections in FY 2009 totaled approximately $1.3 billion (14 percent of CBP's budget).

Since FY 2008, the amount of fees collected by CBP has trended downward. As a result of the decline in the number of passengers and conveyances entering the United States, revenues from inspection user fees suffered a reduction of approximately 8 percent in FY 2009.

- ***U.S. Citizenship and Immigration Services (USCIS)*** – USCIS is responsible for collecting fees from people requesting immigration benefits and depositing them into the Immigration Examination Fee Account. These fees are used to fund the full cost of processing immigration and naturalization benefit applications and petitions, biometric services, and associated support services. These fees are also used to recover the cost of providing similar services to asylum and refugee applicants and certain other immigrants at no charge. In addition, USCIS collects fees for fraud reporting and nonimmigrant worker benefit applications. These fees generated a total of $2.2 billion in revenues in FY 2009.

  During the latter part of FY 2008, USCIS began to see a downward trend in application volume. Thus, the resulting revenue was below levels anticipated under the 2007 fee rule. This downward trend continued into FY 2009, with revenue ultimately falling more than $345 million below fee rule assumptions. Although actions were taken to reduce spending in the face of this decline, actual spending exceeded revenue received during the year, which necessitated the use of prior-year fee revenue balances within fee accounts totaling about $259 million.

- ***U.S. Immigration and Customs Enforcement (ICE)*** – ICE collects user fees to provide a mechanism for monitoring and providing information on student and exchange visitor status violators through the Student Exchange and Visitor Program. In addition, ICE receives 17.4 percent of the collections from the CBP immigration inspection user fee to cover the costs incurred by ICE in connection with detention, removal, and investigations of "inadmissible" aliens who attempt to enter the United States at airports and seaports. In FY 2009, ICE collected fees totaling $271 million; however, in conjunction with CBP's shortfall, revenues from immigration inspection user fees suffered a reduction of approximately 8 percent in FY 2009.

- ***Transportation Security Administration (TSA)*** – TSA is responsible for collecting a variety of user fees related to the security of the nation's aviation system. These security fees include:
  - Air Cargo Security Fee;
  - Aviation Security Passenger and Infrastructure Fees;
  - Fees for Security Threat Assessments for HAZMAT Drivers;
  - Flight Training for Aliens Fee;
  - Passenger Civil Aviation Security Service Fee;
  - Registered Traveler Fee;
  - Protection of Sensitive Security Information Fee;
  - Transportation Worker Identification Credential Fee; and
  - Ronald Reagan Washington National Airport Enhanced Security Procedures for Certain Operations Fees.

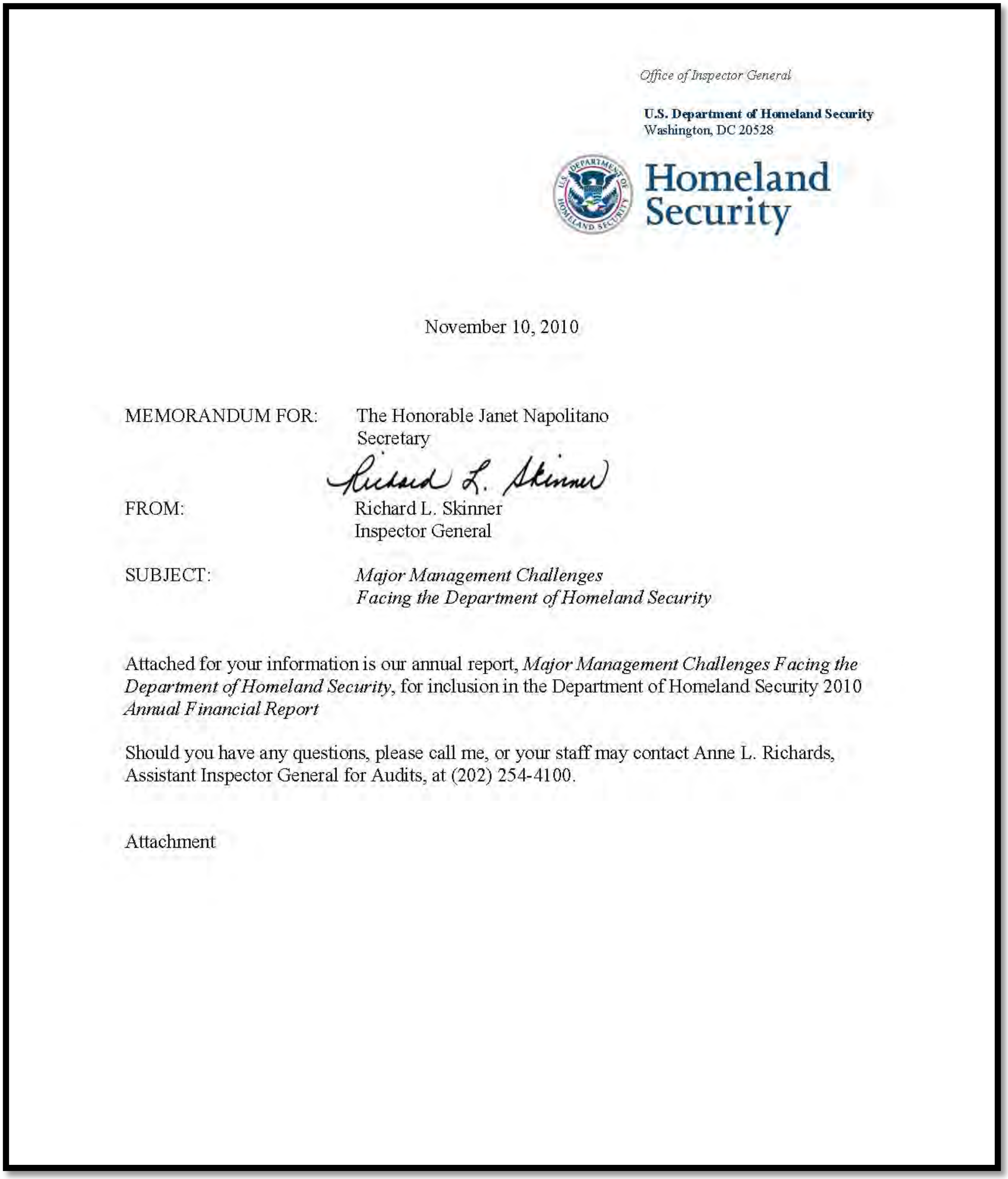
During FY 2009, TSA collected $2.2 billion in user fees. TSA's offsetting fees from the Aviation Security Passenger Fee (which is based on passenger volume) and the Aviation Security Infrastructure Fee totaled $1.9 billion, which reflects 86 percent of TSA's total user fee collections.

- ***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 2009, the fee collections from these services amounted to $24.3 million.

- ***Federal Emergency Management Agency (FEMA)*** – FEMA collects fees for the Radiological Emergency Preparedness Program, which was established to ensure the safety of citizens living near commercial nuclear power plants in case of an accident and to inform the public about radiological emergency preparedness. This program provides site-specific emergency response training to state, local, and tribal governments. In FY 2009, the fees collected for this program totaled $29.6 million.

On October 28, 2009, the *FY 2010 Department of Homeland Security Appropriations Act* (Pub. L. 111-83) and accompanying House report 111-157 was passed, requiring the Department to provide to Congress a quarterly report on actual FY 2009 user fee collections and future projections across all relevant DHS Components. Therefore, to ensure consistency in reporting, the OCFO conducted the above DHS user fee assessment based on the Component's review, validation, and confirmation of actual cash collections and user fee structures, as identified in the Department of Homeland Security User Fees Report to Congress.

Major Management Challenges



Office of Inspector General

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

Homeland Security

November 10, 2010

MEMORANDUM FOR: The Honorable Janet Napolitano
Secretary

Richard L. Skinner

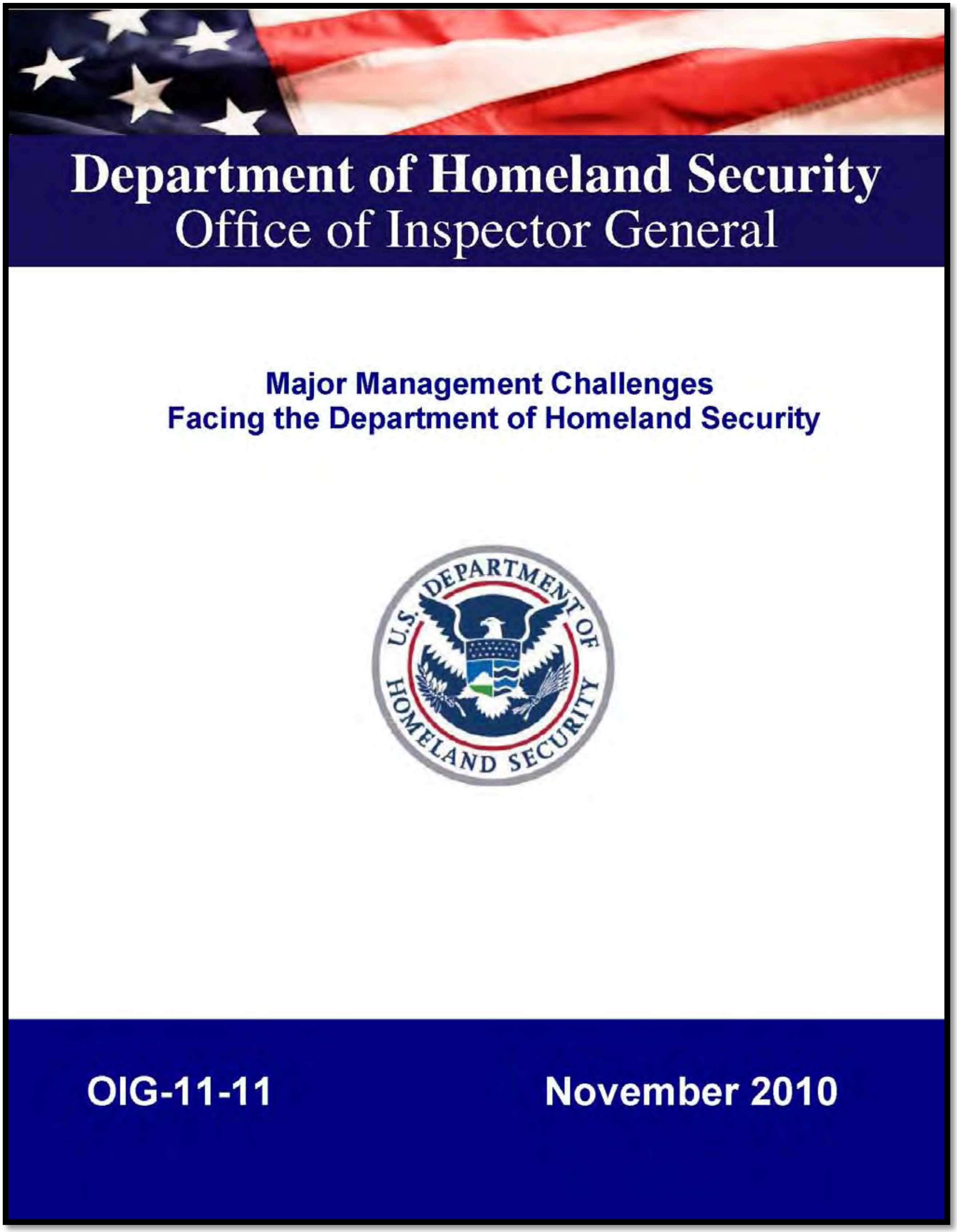
FROM: Richard L. Skinner
Inspector General

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

Attached for your information is our annual report, *Major Management Challenges Facing the Department of Homeland Security*, for inclusion in the Department of Homeland Security 2010 *Annual Financial Report*

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

Attachment

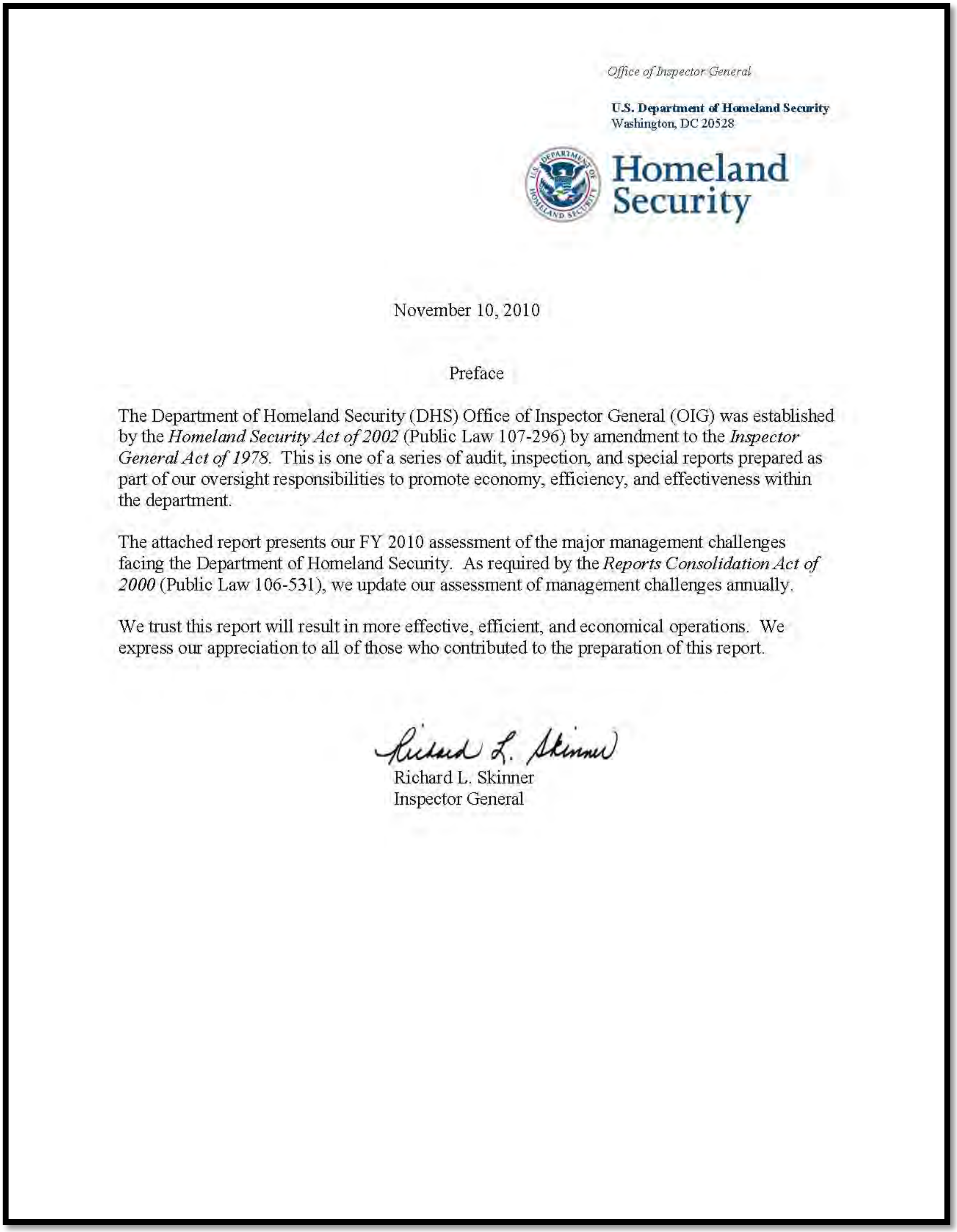


Department of Homeland Security
Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

OIG-11-11

November 2010



Office of Inspector General

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

Homeland
Security

November 10, 2010

Preface

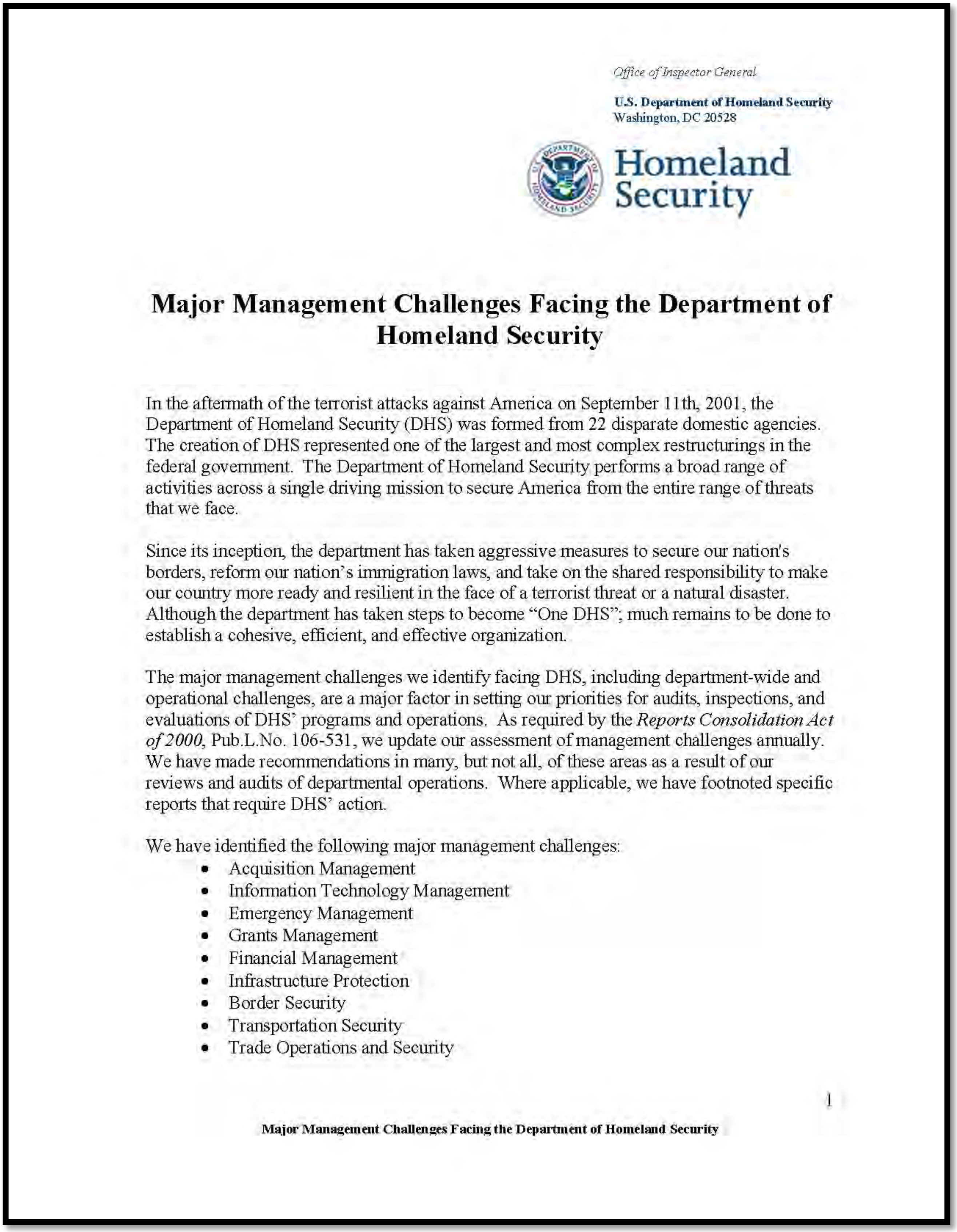
The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight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

The attached report presents our FY 2010 assessment of the major management challenges facing the Department of Homeland Security. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually.

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

Richard L. Skinner

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

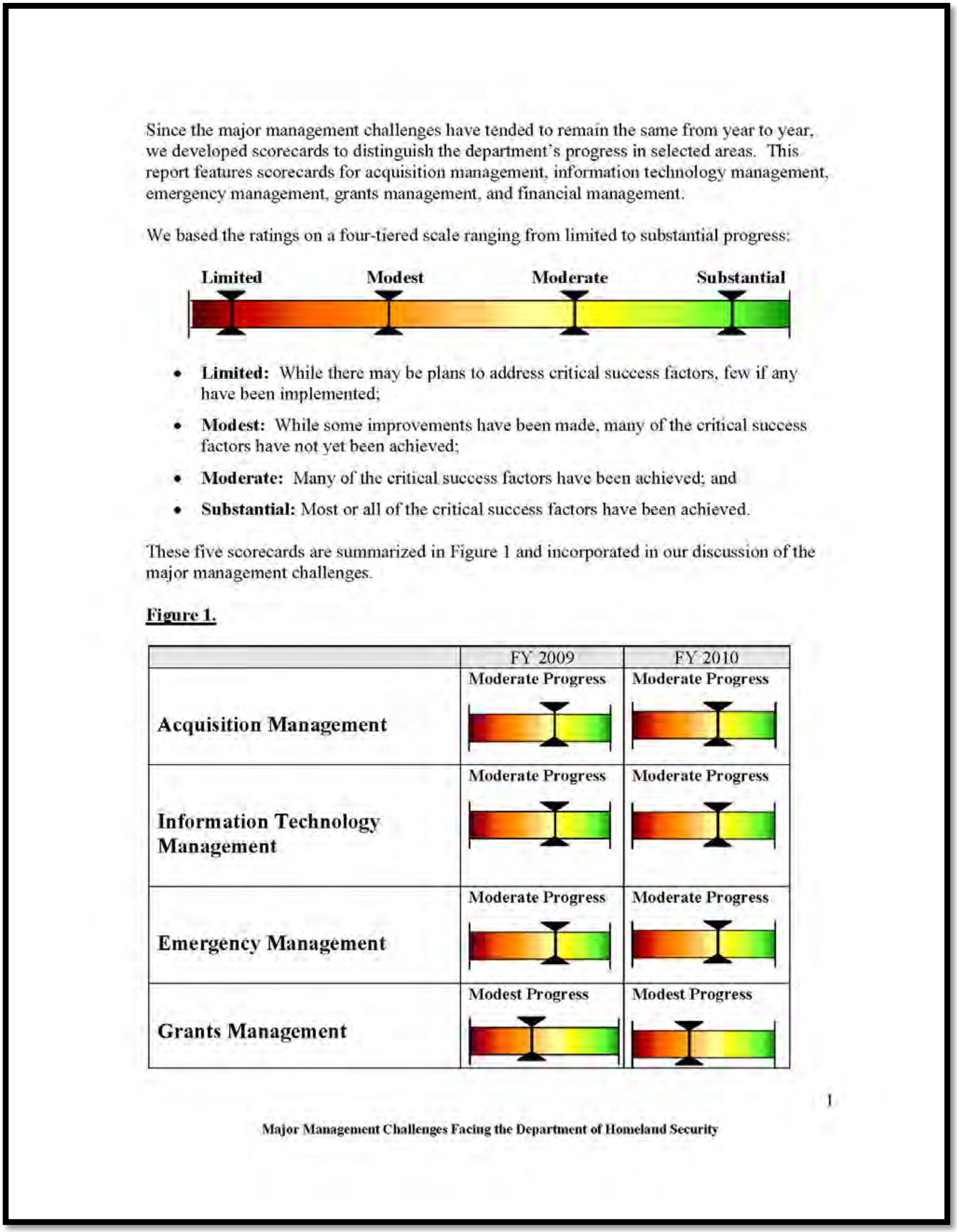
In the aftermath of the terrorist attacks against America on September 11th, 2001, the Department of Homeland Security (DHS) was formed from 22 disparate domestic agencies. The creation of DHS represented one of the largest and most complex restructurings in the federal government. The Department of Homeland Security performs a broad range of activities across a single driving mission to secure America from the entire range of threats that we face.

Since its inception, the department has taken aggressive measures to secure our nation's borders, reform our nation's immigration laws, and take on the shared responsibility to make our country more ready and resilient in the face of a terrorist threat or a natural disaster. Although the department has taken steps to become "One DHS"; much remains to be done to establish a cohesive, efficient, and effective organization.

The major management challenges we identify facing DHS, including department-wide and operational challenges, are a major factor in setting our priorities for audits, inspections, and evaluations of DHS' programs and operations. As required by the *Reports Consolidation Act of 2000*, Pub.L.No. 106-531, we update our assessment of management challenges annually. We have made recommendations in many, but not all, of these areas as a result of our reviews and audits of departmental operations. Where applicable, we have footnoted specific reports that require DHS' action.

We have identified the following major management challenges:

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



Since the major management challenges have tended to remain the same from year to year, we developed scorecards to distinguish the department's progress in selected areas. This report features scorecards for acquisition management, information technology management, emergency management, grants management, and financial management.

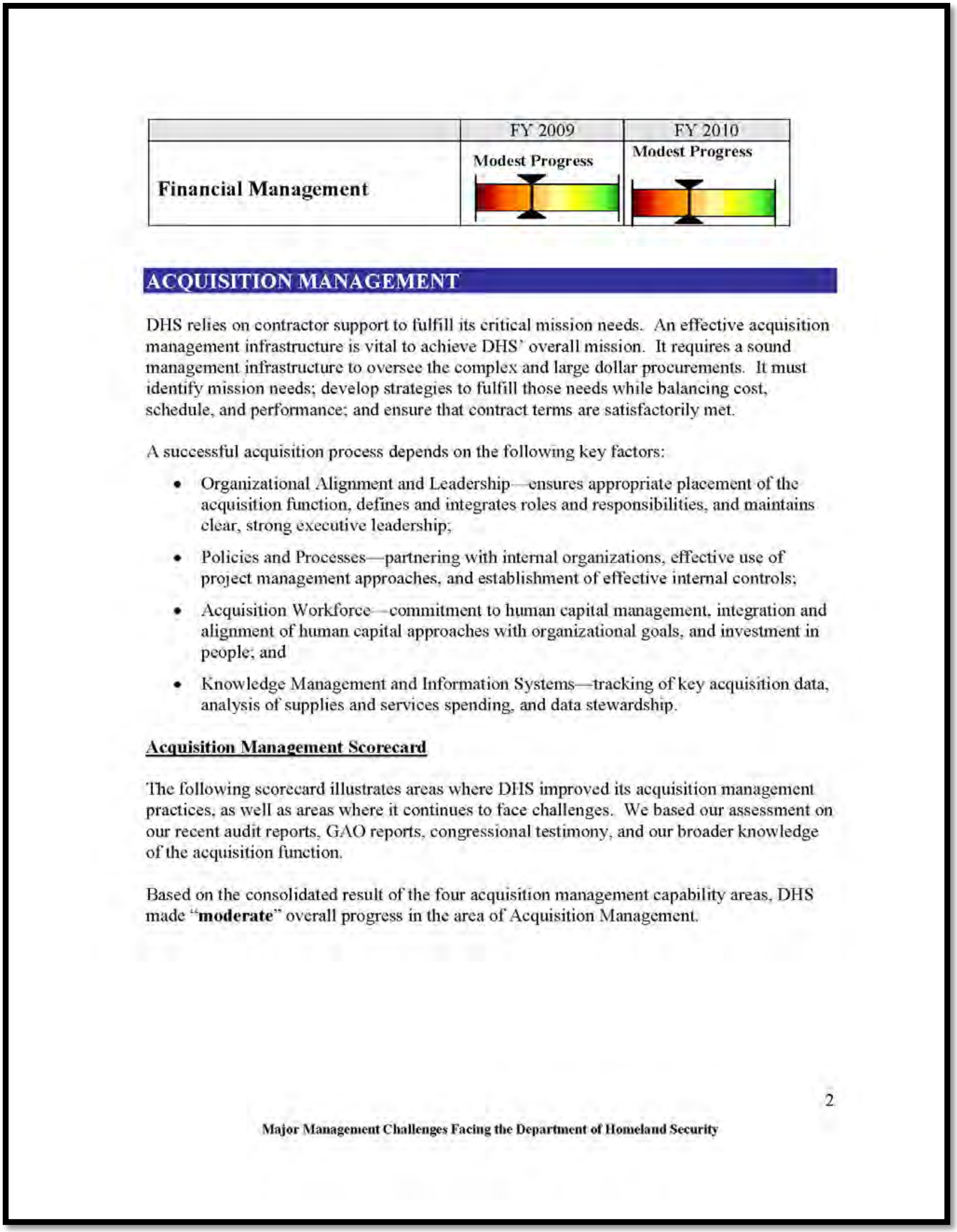
We based the ratings on a four-tiered scale ranging from limited to substantial progress:

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

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

Figure 1.

	FY 2009	FY 2010
Acquisition Management	Moderate Progress	Moderate Progress
Information Technology Management	Moderate Progress	Moderate Progress
Emergency Management	Moderate Progress	Moderate Progress
Grants Management	Modest Progress	Modest Progress



	FY 2009	FY 2010
Financial Management	**Modest Progress**	**Modest Progress**

ACQUISITION MANAGEMENT

DHS relies on contractor support to fulfill its critical mission needs. An effective acquisition management infrastructure is vital to achieve DHS' overall mission. It requires a sound management infrastructure to oversee the complex and large dollar procurements. It must identify mission needs; develop strategies to fulfill those needs while balancing cost, schedule, and performance; and ensure that contract terms are satisfactorily met.

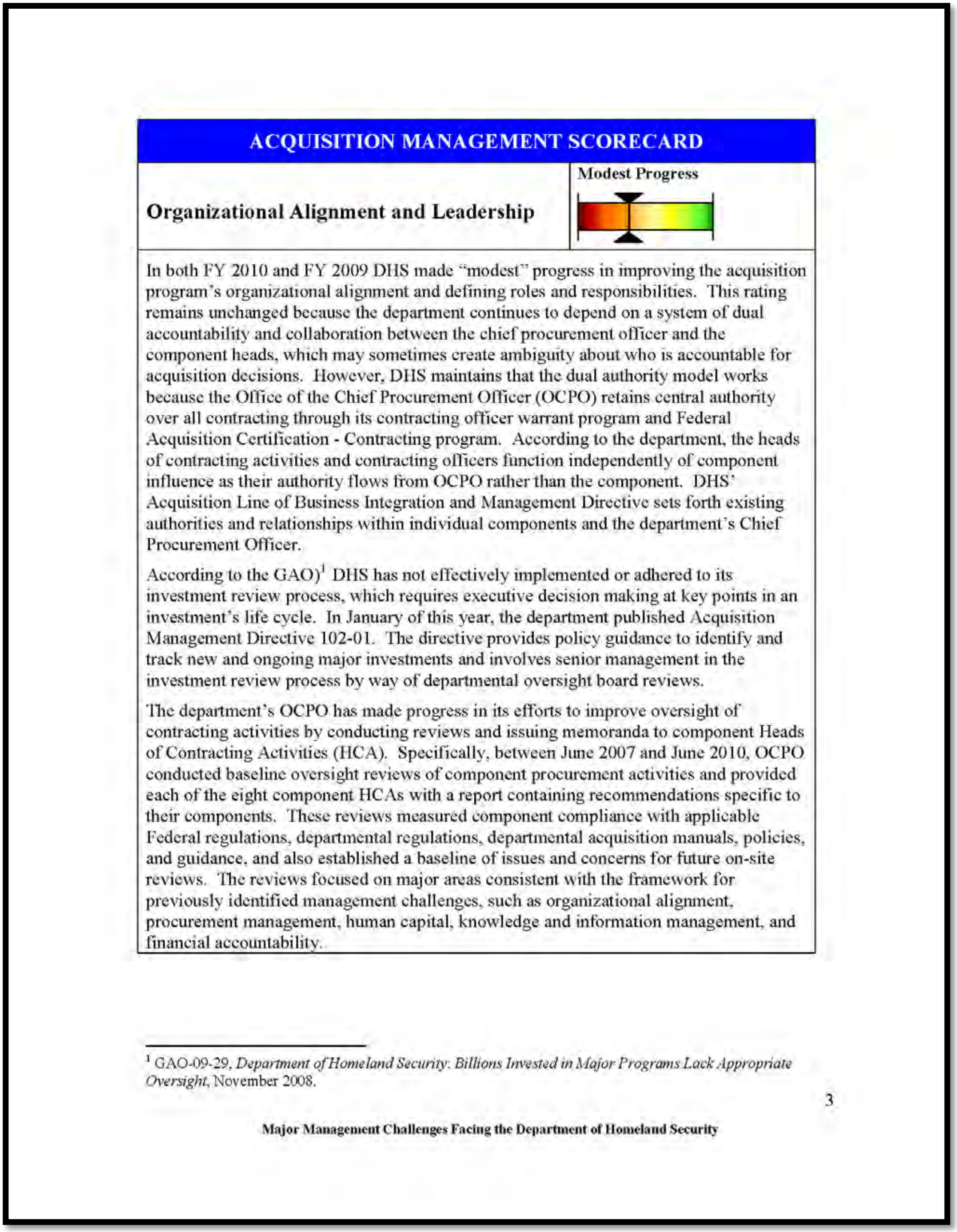
A successful acquisition process depends on the following key factors:

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

Acquisition Management Scorecard

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

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



ACQUISITION MANAGEMENT SCORECARD

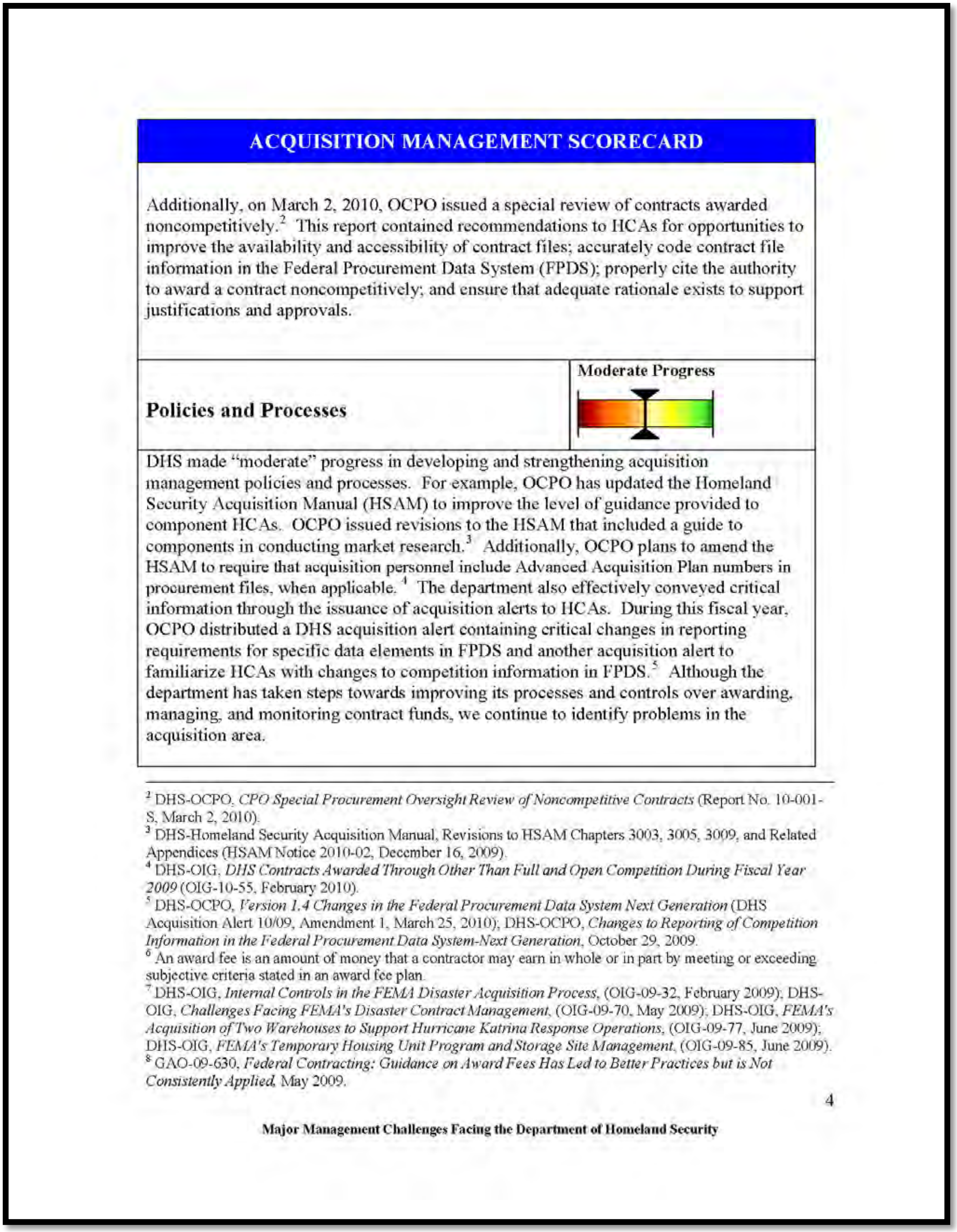
Organizational Alignment and Leadership	**Modest Progress**

In both FY 2010 and FY 2009 DHS made "modest" progress in improving the acquisition program's organizational alignment and defining roles and responsibilities. This rating remains unchanged because the department continues to depend on a system of dual accountability and collaboration between the chief procurement officer and the component heads, which may sometimes create ambiguity about who is accountable for acquisition decisions. However, DHS maintains that the dual authority model works because the Office of the Chief Procurement Officer (OCPO) retains central authority over all contracting through its contracting officer warrant program and Federal Acquisition Certification - Contracting program. According to the department, the heads of contracting activities and contracting officers function independently of component influence as their authority flows from OCPO rather than the component. DHS' Acquisition Line of Business Integration and Management Directive sets forth existing authorities and relationships within individual components and the department's Chief Procurement Officer.

According to the GAO)[1] DHS has not effectively implemented or adhered to its investment review process, which requires executive decision making at key points in an investment's life cycle. In January of this year, the department published Acquisition Management Directive 102-01. The directive provides policy guidance to identify and track new and ongoing major investments and involves senior management in the investment review process by way of departmental oversight board reviews.

The department's OCPO has made progress in its efforts to improve oversight of contracting activities by conducting reviews and issuing memoranda to component Heads of Contracting Activities (HCA). Specifically, between June 2007 and June 2010, OCPO conducted baseline oversight reviews of component procurement activities and provided each of the eight component HCAs with a report containing recommendations specific to their components. These reviews measured component compliance with applicable Federal regulations, departmental regulations, departmental acquisition manuals, policies, and guidance, and also established a baseline of issues and concerns for future on-site reviews. The reviews focused on major areas consistent with the framework for previously identified management challenges, such as organizational alignment, procurement management, human capital, knowledge and information management, and financial accountability.

[1] GAO-09-29, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, November 2008.



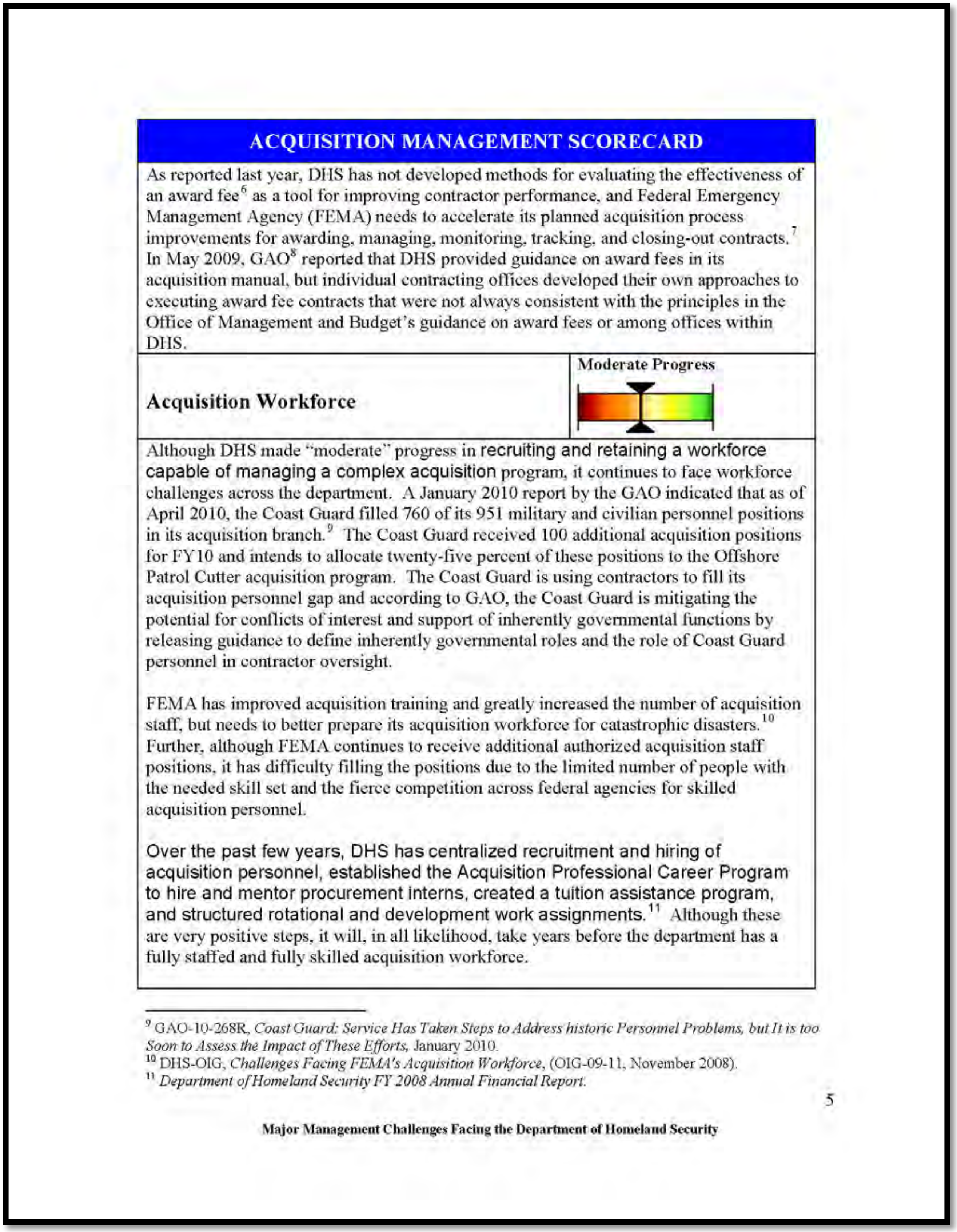
ACQUISITION MANAGEMENT SCORECARD

Additionally, on March 2, 2010, OCPO issued a special review of contracts awarded noncompetitively.[2] This report contained recommendations to HCAs for opportunities to improve the availability and accessibility of contract files; accurately code contract file information in the Federal Procurement Data System (FPDS); properly cite the authority to award a contract noncompetitively; and ensure that adequate rationale exists to support justifications and approvals.

Policies and Processes	**Moderate Progress**

DHS made "moderate" progress in developing and strengthening acquisition management policies and processes. For example, OCPO has updated the Homeland Security Acquisition Manual (HSAM) to improve the level of guidance provided to component HCAs. OCPO issued revisions to the HSAM that included a guide to components in conducting market research.[3] Additionally, OCPO plans to amend the HSAM to require that acquisition personnel include Advanced Acquisition Plan numbers in procurement files, when applicable. [4] The department also effectively conveyed critical information through the issuance of acquisition alerts to HCAs. During this fiscal year, OCPO distributed a DHS acquisition alert containing critical changes in reporting requirements for specific data elements in FPDS and another acquisition alert to familiarize HCAs with changes to competition information in FPDS.[5] Although the department has taken steps towards improving its processes and controls over awarding, managing, and monitoring contract funds, we continue to identify problems in the acquisition area.

[2] DHS-OCPO, *CPO Special Procurement Oversight Review of Noncompetitive Contracts* (Report No. 10-001-S, March 2, 2010).
[3] DHS-Homeland Security Acquisition Manual, Revisions to HSAM Chapters 3003, 3005, 3009, and Related Appendices (HSAM Notice 2010-02, December 16, 2009).
[4] DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition During Fiscal Year 2009* (OIG-10-55, February 2010).
[5] DHS-OCPO, *Version 1.4 Changes in the Federal Procurement Data System Next Generation* (DHS Acquisition Alert 10/09, Amendment 1, March 25, 2010); DHS-OCPO, *Changes to Reporting of Competition Information in the Federal Procurement Data System-Next Generation*, October 29, 2009.
[6] An award fee is an amount of money that a contractor may earn in whole or in part by meeting or exceeding subjective criteria stated in an award fee plan.
[7] DHS-OIG, *Internal Controls in the FEMA Disaster Acquisition Process*, (OIG-09-32, February 2009); DHS-OIG, *Challenges Facing FEMA's Disaster Contract Management*, (OIG-09-70, May 2009); DHS-OIG, *FEMA's Acquisition of Two Warehouses to Support Hurricane Katrina Response Operations*, (OIG-09-77, June 2009); DHS-OIG, *FEMA's Temporary Housing Unit Program and Storage Site Management*, (OIG-09-85, June 2009).
[8] GAO-09-630, *Federal Contracting: Guidance on Award Fees Has Led to Better Practices but is Not Consistently Applied*, May 2009.



ACQUISITION MANAGEMENT SCORECARD

As reported last year, DHS has not developed methods for evaluating the effectiveness of an award fee[6] as a tool for improving contractor performance, and Federal Emergency Management Agency (FEMA) needs to accelerate its planned acquisition process improvements for awarding, managing, monitoring, tracking, and closing-out contracts.[7] In May 2009, GAO[8] reported that DHS provided guidance on award fees in its acquisition manual, but individual contracting offices developed their own approaches to executing award fee contracts that were not always consistent with the principles in the Office of Management and Budget's guidance on award fees or among offices within DHS.

Acquisition Workforce

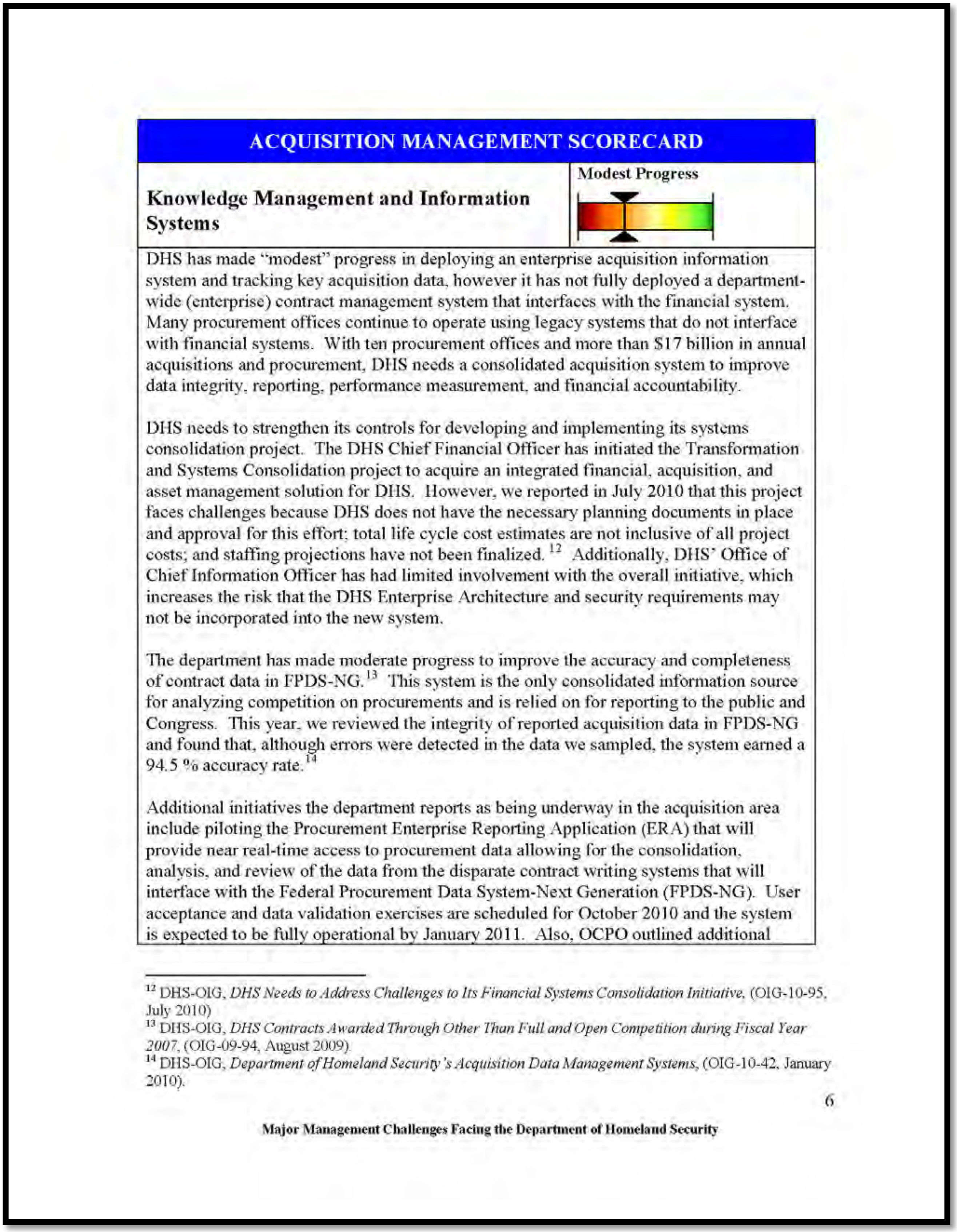
Moderate Progress

Although DHS made "moderate" progress in recruiting and retaining a workforce capable of managing a complex acquisition program, it continues to face workforce challenges across the department. A January 2010 report by the GAO indicated that as of April 2010, the Coast Guard filled 760 of its 951 military and civilian personnel positions in its acquisition branch.[9] The Coast Guard received 100 additional acquisition positions for FY10 and intends to allocate twenty-five percent of these positions to the Offshore Patrol Cutter acquisition program. The Coast Guard is using contractors to fill its acquisition personnel gap and according to GAO, the Coast Guard is mitigating the potential for conflicts of interest and support of inherently governmental functions by releasing guidance to define inherently governmental roles and the role of Coast Guard personnel in contractor oversight.

FEMA has improved acquisition training and greatly increased the number of acquisition staff, but needs to better prepare its acquisition workforce for catastrophic disasters.[10] Further, although FEMA continues to receive additional authorized acquisition staff positions, it has difficulty filling the positions due to the limited number of people with the needed skill set and the fierce competition across federal agencies for skilled acquisition personnel.

Over the past few years, DHS has centralized recruitment and hiring of acquisition personnel, established the Acquisition Professional Career Program to hire and mentor procurement interns, created a tuition assistance program, and structured rotational and development work assignments.[11] Although these are very positive steps, it will, in all likelihood, take years before the department has a fully staffed and fully skilled acquisition workforce.

[9] GAO-10-268R, *Coast Guard: Service Has Taken Steps to Address historic Personnel Problems, but It is too Soon to Assess the Impact of These Efforts*, January 2010.
[10] DHS-OIG, *Challenges Facing FEMA's Acquisition Workforce*, (OIG-09-11, November 2008).
[11] *Department of Homeland Security FY 2008 Annual Financial Report.*



ACQUISITION MANAGEMENT SCORECARD

Knowledge Management and Information Systems

Modest Progress

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

DHS needs to strengthen its controls for developing and implementing its systems consolidation project. The DHS Chief Financial Officer has initiated the Transformation and Systems Consolidation project to acquire an integrated financial, acquisition, and asset management solution for DHS. However, we reported in July 2010 that this project faces challenges because DHS does not have the necessary planning documents in place and approval for this effort; total life cycle cost estimates are not inclusive of all project costs; and staffing projections have not been finalized. [12] Additionally, DHS' Office of Chief Information Officer has had limited involvement with the overall initiative, which increases the risk that the DHS Enterprise Architecture and security requirements may not be incorporated into the new system.

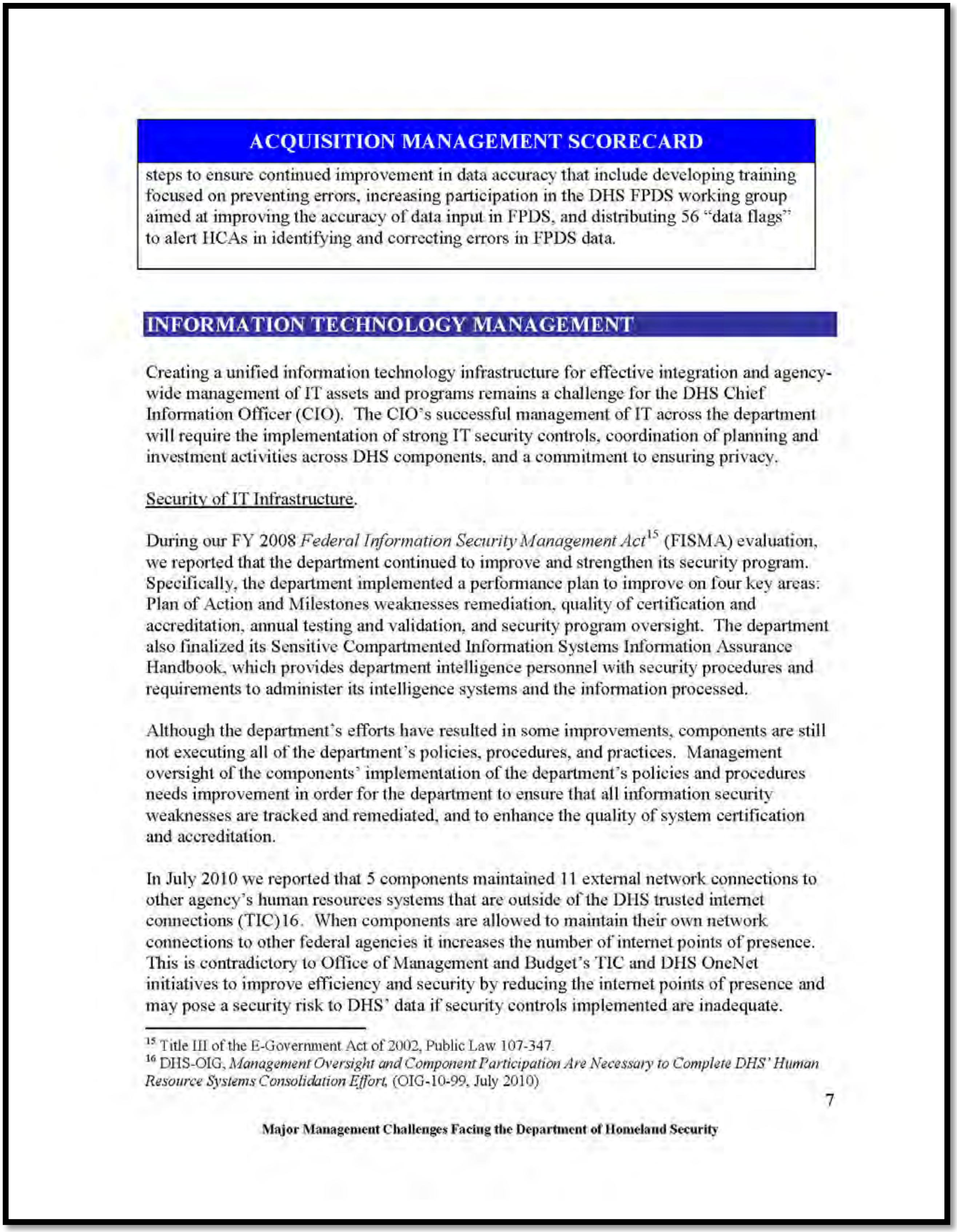
The department has made moderate progress to improve the accuracy and completeness of contract data in FPDS-NG.[13] This system is the only consolidated information source for analyzing competition on procurements and is relied on for reporting to the public and Congress. This year, we reviewed the integrity of reported acquisition data in FPDS-NG and found that, although errors were detected in the data we sampled, the system earned a 94.5 % accuracy rate.[14]

Additional initiatives the department reports as being underway in the acquisition area include piloting the Procurement Enterprise Reporting Application (ERA) that will provide near real-time access to procurement data allowing for the consolidation, analysis, and review of the data from the disparate contract writing systems that will interface with the Federal Procurement Data System-Next Generation (FPDS-NG). User acceptance and data validation exercises are scheduled for October 2010 and the system is expected to be fully operational by January 2011. Also, OCPO outlined additional

[12] DHS-OIG, *DHS Needs to Address Challenges to Its Financial Systems Consolidation Initiative*, (OIG-10-95, July 2010)

[13] DHS-OIG, *DHS Contracts Awarded Through Other Than Full and Open Competition during Fiscal Year 2007*, (OIG-09-94, August 2009)

[14] DHS-OIG, *Department of Homeland Security's Acquisition Data Management Systems*, (OIG-10-42, January 2010).



ACQUISITION MANAGEMENT SCORECARD

steps to ensure continued improvement in data accuracy that include developing training focused on preventing errors, increasing participation in the DHS FPDS working group aimed at improving the accuracy of data input in FPDS, and distributing 56 "data flags" to alert HCAs in identifying and correcting errors in FPDS data.

INFORMATION TECHNOLOGY MANAGEMENT

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

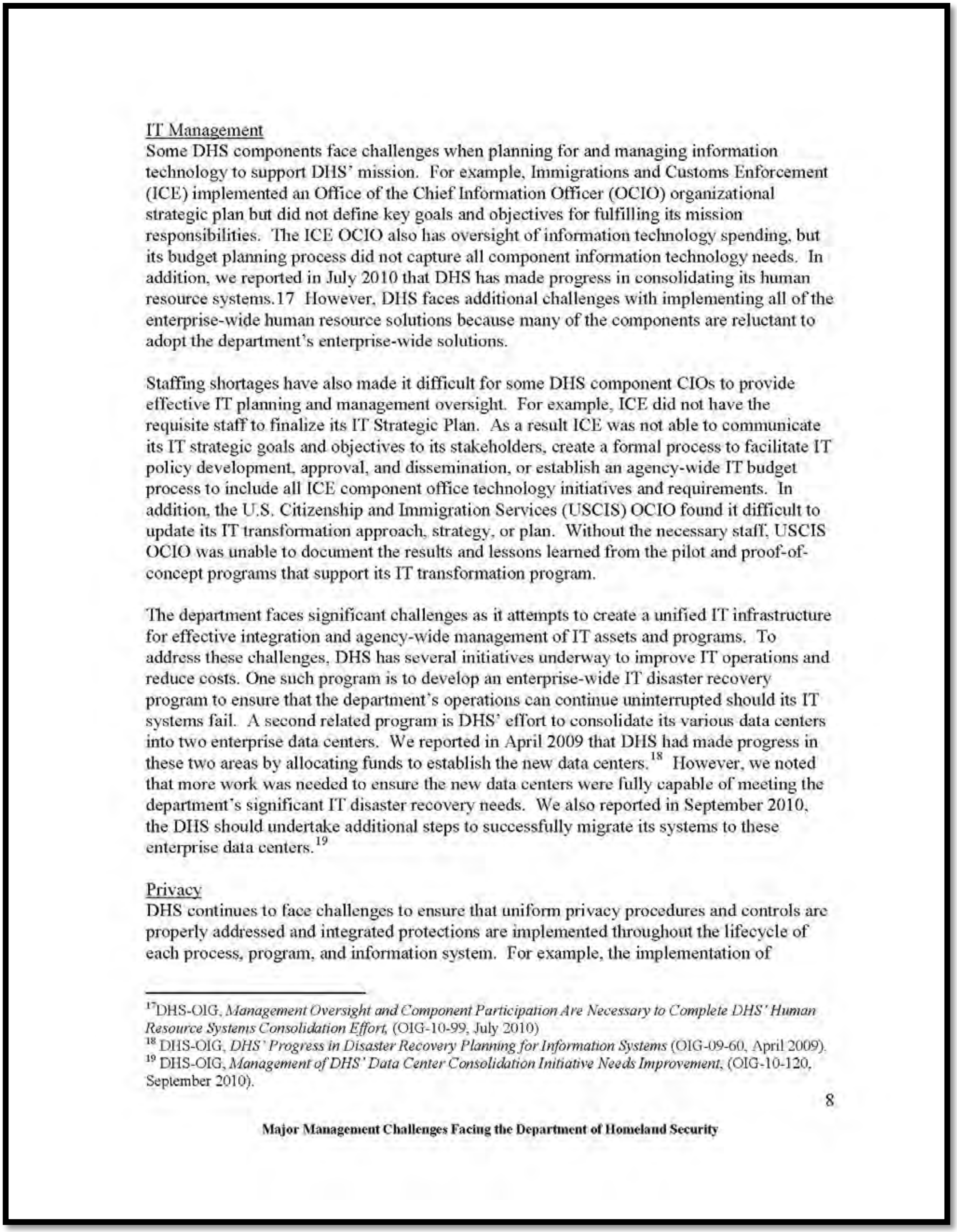
Security of IT Infrastructure.

During our FY 2008 *Federal Information Security Management Act*[15] (FISMA) evaluation, we reported that the department continued to improve and strengthen its security program. Specifically, the department implemented a performance plan to improve on four key areas: Plan of Action and Milestones weaknesses remediation, quality of certification and accreditation, annual testing and validation, and security program oversight. The department also finalized its Sensitive Compartmented Information Systems Information Assurance Handbook, which provides department intelligence personnel with security procedures and requirements to administer its intelligence systems and the information processed.

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

In July 2010 we reported that 5 components maintained 11 external network connections to other agency's human resources systems that are outside of the DHS trusted internet connections (TIC)16. When components are allowed to maintain their own network connections to other federal agencies it increases the number of internet points of presence. This is contradictory to Office of Management and Budget's TIC and DHS OneNet initiatives to improve efficiency and security by reducing the internet points of presence and may pose a security risk to DHS' data if security controls implemented are inadequate.

[15] Title III of the E-Government Act of 2002, Public Law 107-347.
[16] DHS-OIG, *Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort,* (OIG-10-99, July 2010)



IT Management

Some DHS components face challenges when planning for and managing information technology to support DHS' mission. For example, Immigrations and Customs Enforcement (ICE) implemented an Office of the Chief Information Officer (OCIO) organizational strategic plan but did not define key goals and objectives for fulfilling its mission responsibilities. The ICE OCIO also has oversight of information technology spending, but its budget planning process did not capture all component information technology needs. In addition, we reported in July 2010 that DHS has made progress in consolidating its human resource systems.17 However, DHS faces additional challenges with implementing all of the enterprise-wide human resource solutions because many of the components are reluctant to adopt the department's enterprise-wide solutions.

Staffing shortages have also made it difficult for some DHS component CIOs to provide effective IT planning and management oversight. For example, ICE did not have the requisite staff to finalize its IT Strategic Plan. As a result ICE was not able to communicate its IT strategic goals and objectives to its stakeholders, create a formal process to facilitate IT policy development, approval, and dissemination, or establish an agency-wide IT budget process to include all ICE component office technology initiatives and requirements. In addition, the U.S. Citizenship and Immigration Services (USCIS) OCIO found it difficult to update its IT transformation approach, strategy, or plan. Without the necessary staff, USCIS OCIO was unable to document the results and lessons learned from the pilot and proof-of-concept programs that support its IT transformation program.

The department faces significant challenges as it attempts to create a unified IT infrastructure for effective integration and agency-wide management of IT assets and programs. To address these challenges, DHS has several initiatives underway to improve IT operations and reduce costs. One such program is to develop an enterprise-wide IT disaster recovery program to ensure that the department's operations can continue uninterrupted should its IT systems fail. A second related program is DHS' effort to consolidate its various data centers into two enterprise data centers. We reported in April 2009 that DHS had made progress in these two areas by allocating funds to establish the new data centers.[18] However, we noted that more work was needed to ensure the new data centers were fully capable of meeting the department's significant IT disaster recovery needs. We also reported in September 2010, the DHS should undertake additional steps to successfully migrate its systems to these enterprise data centers.[19]

Privacy

DHS continues to face challenges to ensure that uniform privacy procedures and controls are properly addressed and integrated protections are implemented throughout the lifecycle of each process, program, and information system. For example, the implementation of

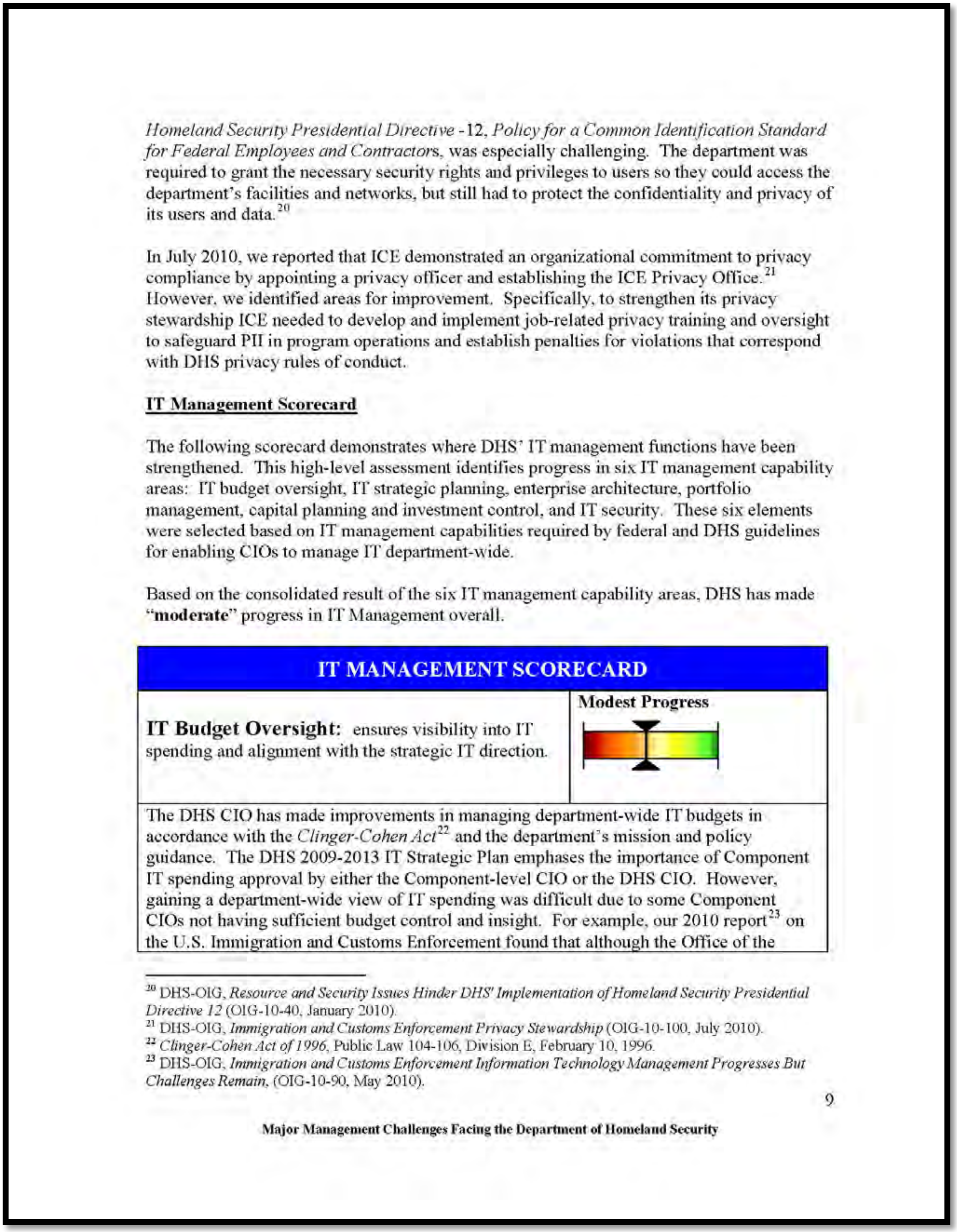
[17]DHS-OIG, *Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort*, (OIG-10-99, July 2010)

[18] DHS-OIG, *DHS' Progress in Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

[19] DHS-OIG, *Management of DHS' Data Center Consolidation Initiative Needs Improvement*, (OIG-10-120, September 2010).

8

Major Management Challenges Facing the Department of Homeland Security



Homeland Security Presidential Directive -12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was especially challenging. The department was required to grant the necessary security rights and privileges to users so they could access the department's facilities and networks, but still had to protect the confidentiality and privacy of its users and data.[20]

In July 2010, we reported that ICE demonstrated an organizational commitment to privacy compliance by appointing a privacy officer and establishing the ICE Privacy Office.[21] However, we identified areas for improvement. Specifically, to strengthen its privacy stewardship ICE needed to develop and implement job-related privacy training and oversight to safeguard PII in program operations and establish penalties for violations that correspond with DHS privacy rules of conduct.

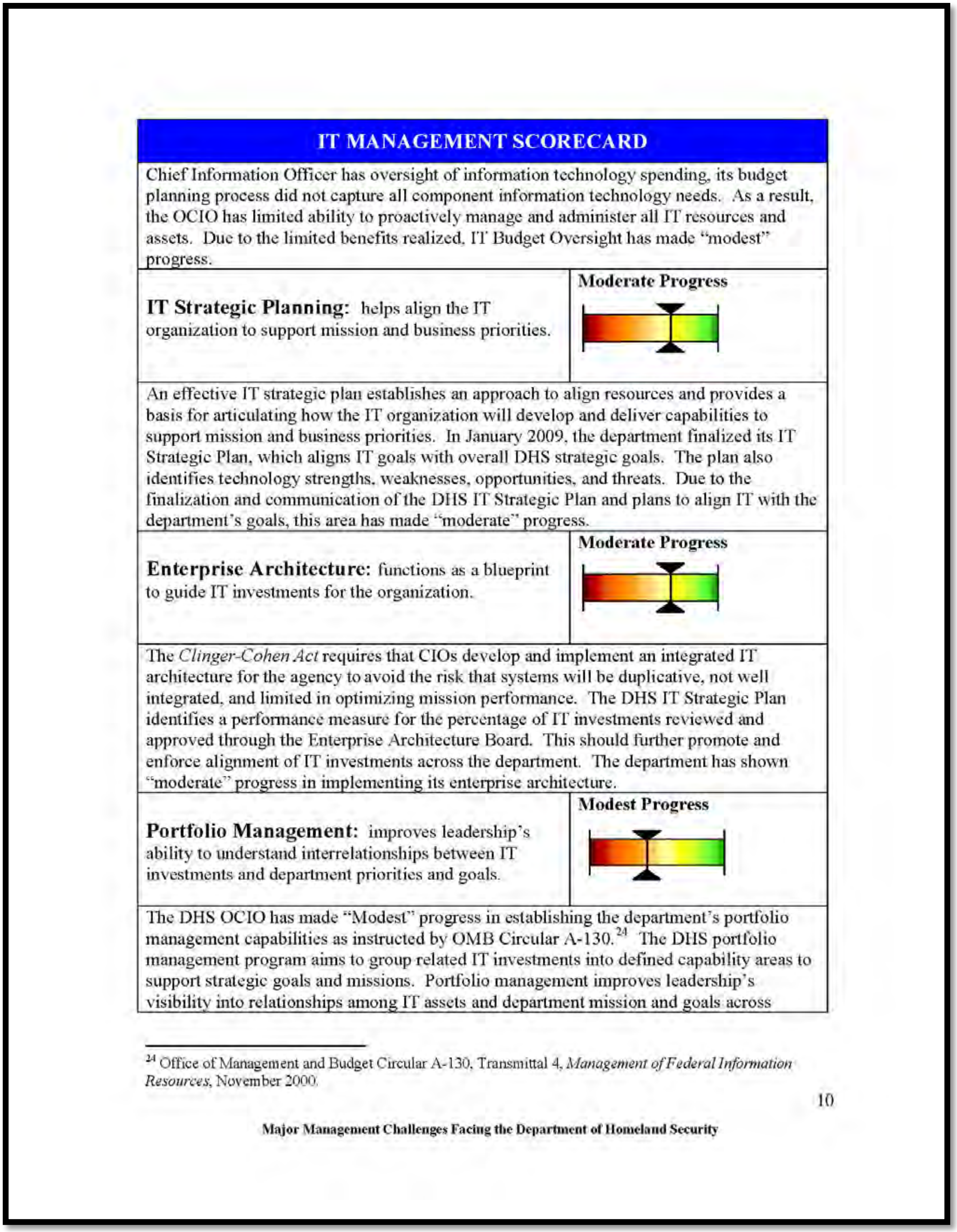
IT Management Scorecard

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

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

IT MANAGEMENT SCORECARD	
IT Budget Oversight: ensures visibility into IT spending and alignment with the strategic IT direction.	**Modest Progress**
The DHS CIO has made improvements in managing department-wide IT budgets in accordance with the *Clinger-Cohen Act*[22] and the department's mission and policy guidance. The DHS 2009-2013 IT Strategic Plan emphases the importance of Component IT spending approval by either the Component-level CIO or the DHS CIO. However, gaining a department-wide view of IT spending was difficult due to some Component CIOs not having sufficient budget control and insight. For example, our 2010 report[23] on the U.S. Immigration and Customs Enforcement found that although the Office of the	

[20] DHS-OIG, *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12* (OIG-10-40, January 2010).
[21] DHS-OIG, *Immigration and Customs Enforcement Privacy Stewardship* (OIG-10-100, July 2010).
[22] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, February 10, 1996.
[23] DHS-OIG, *Immigration and Customs Enforcement Information Technology Management Progresses But Challenges Remain*, (OIG-10-90, May 2010).



IT MANAGEMENT SCORECARD

Chief Information Officer has oversight of information technology spending, its budget planning process did not capture all component information technology needs. As a result, the OCIO has limited ability to proactively manage and administer all IT resources and assets. Due to the limited benefits realized, IT Budget Oversight has made "modest" progress.

IT Strategic Planning: helps align the IT organization to support mission and business priorities.	**Moderate Progress**

An effective IT strategic plan establishes an approach to align resources and provides a basis for articulating how the IT organization will develop and deliver capabilities to support mission and business priorities. In January 2009, the department finalized its IT Strategic Plan, which aligns IT goals with overall DHS strategic goals. The plan also identifies technology strengths, weaknesses, opportunities, and threats. Due to the finalization and communication of the DHS IT Strategic Plan and plans to align IT with the department's goals, this area has made "moderate" progress.

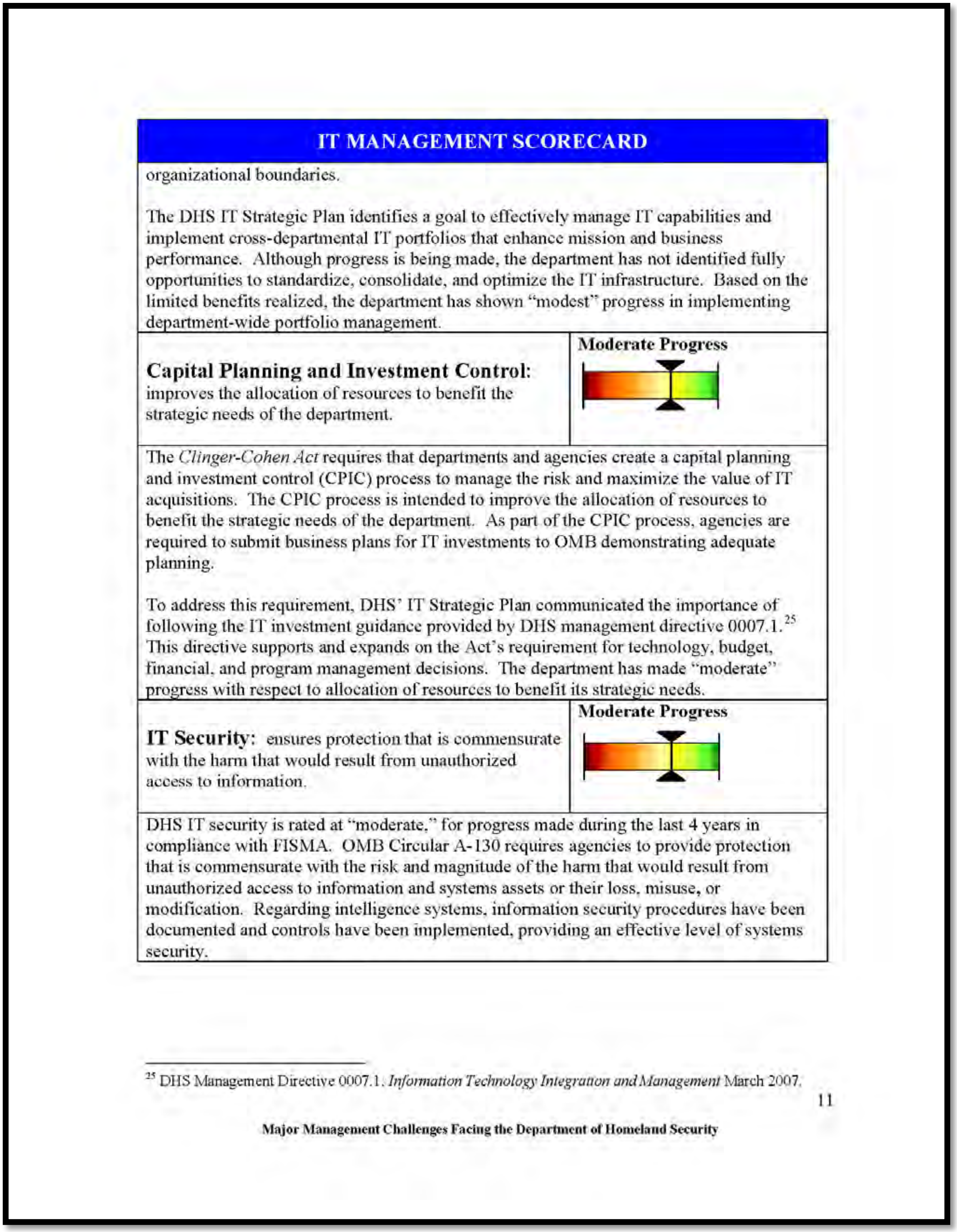
Enterprise Architecture: functions as a blueprint to guide IT investments for the organization.	**Moderate Progress**

The *Clinger-Cohen Act* requires that CIOs develop and implement an integrated IT architecture for the agency to avoid the risk that systems will be duplicative, not well integrated, and limited in optimizing mission performance. The DHS IT Strategic Plan identifies a performance measure for the percentage of IT investments reviewed and approved through the Enterprise Architecture Board. This should further promote and enforce alignment of IT investments across the department. The department has shown "moderate" progress in implementing its enterprise architecture.

Portfolio Management: improves leadership's ability to understand interrelationships between IT investments and department priorities and goals.	**Modest Progress**

The DHS OCIO has made "Modest" progress in establishing the department's portfolio management capabilities as instructed by OMB Circular A-130.[24] The DHS portfolio management program aims to group related IT investments into defined capability areas to support strategic goals and missions. Portfolio management improves leadership's visibility into relationships among IT assets and department mission and goals across

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



IT MANAGEMENT SCORECARD

organizational boundaries.

The DHS IT Strategic Plan identifies a goal to effectively manage IT capabilities and implement cross-departmental IT portfolios that enhance mission and business performance. Although progress is being made, the department has not identified fully opportunities to standardize, consolidate, and optimize the IT infrastructure. Based on the limited benefits realized, the department has shown "modest" progress in implementing department-wide portfolio management.

Capital Planning and Investment Control: improves the allocation of resources to benefit the strategic needs of the department.	**Moderate Progress**

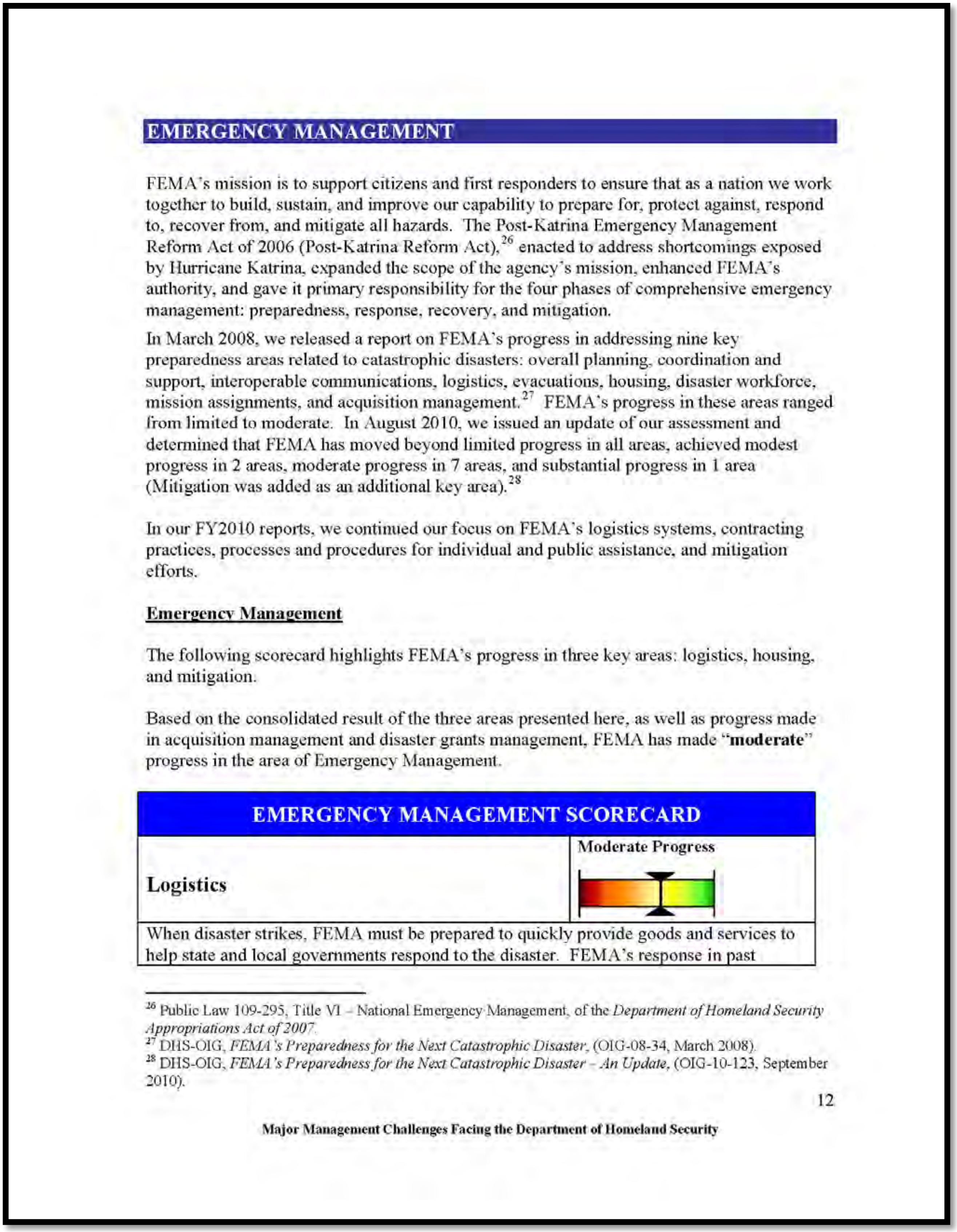
The *Clinger-Cohen Act* requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning.

To address this requirement, DHS' IT Strategic Plan communicated the importance of following the IT investment guidance provided by DHS management directive 0007.1.[25] This directive supports and expands on the Act's requirement for technology, budget, financial, and program management decisions. The department has made "moderate" progress with respect to allocation of resources to benefit its strategic needs.

IT Security: ensures protection that is commensurate with the harm that would result from unauthorized access to information.	**Moderate Progress**

DHS IT security is rated at "moderate," for progress made during the last 4 years in compliance with FISMA. OMB Circular A-130 requires agencies to provide protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to information and systems assets or their loss, misuse, or modification. Regarding intelligence systems, information security procedures have been documented and controls have been implemented, providing an effective level of systems security.

[25] DHS Management Directive 0007.1, *Information Technology Integration and Management* March 2007.



EMERGENCY MANAGEMENT

FEMA's mission is to support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. The Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Reform Act),[26] enacted to address shortcomings exposed by Hurricane Katrina, expanded the scope of the agency's mission, enhanced FEMA's authority, and gave it primary responsibility for the four phases of comprehensive emergency management: preparedness, response, recovery, and mitigation.

In March 2008, we released a report on FEMA's progress in addressing nine key preparedness areas related to catastrophic disasters: overall planning, coordination and support, interoperable communications, logistics, evacuations, housing, disaster workforce, mission assignments, and acquisition management.[27] FEMA's progress in these areas ranged from limited to moderate. In August 2010, we issued an update of our assessment and determined that FEMA has moved beyond limited progress in all areas, achieved modest progress in 2 areas, moderate progress in 7 areas, and substantial progress in 1 area (Mitigation was added as an additional key area).[28]

In our FY2010 reports, we continued our focus on FEMA's logistics systems, contracting practices, processes and procedures for individual and public assistance, and mitigation efforts.

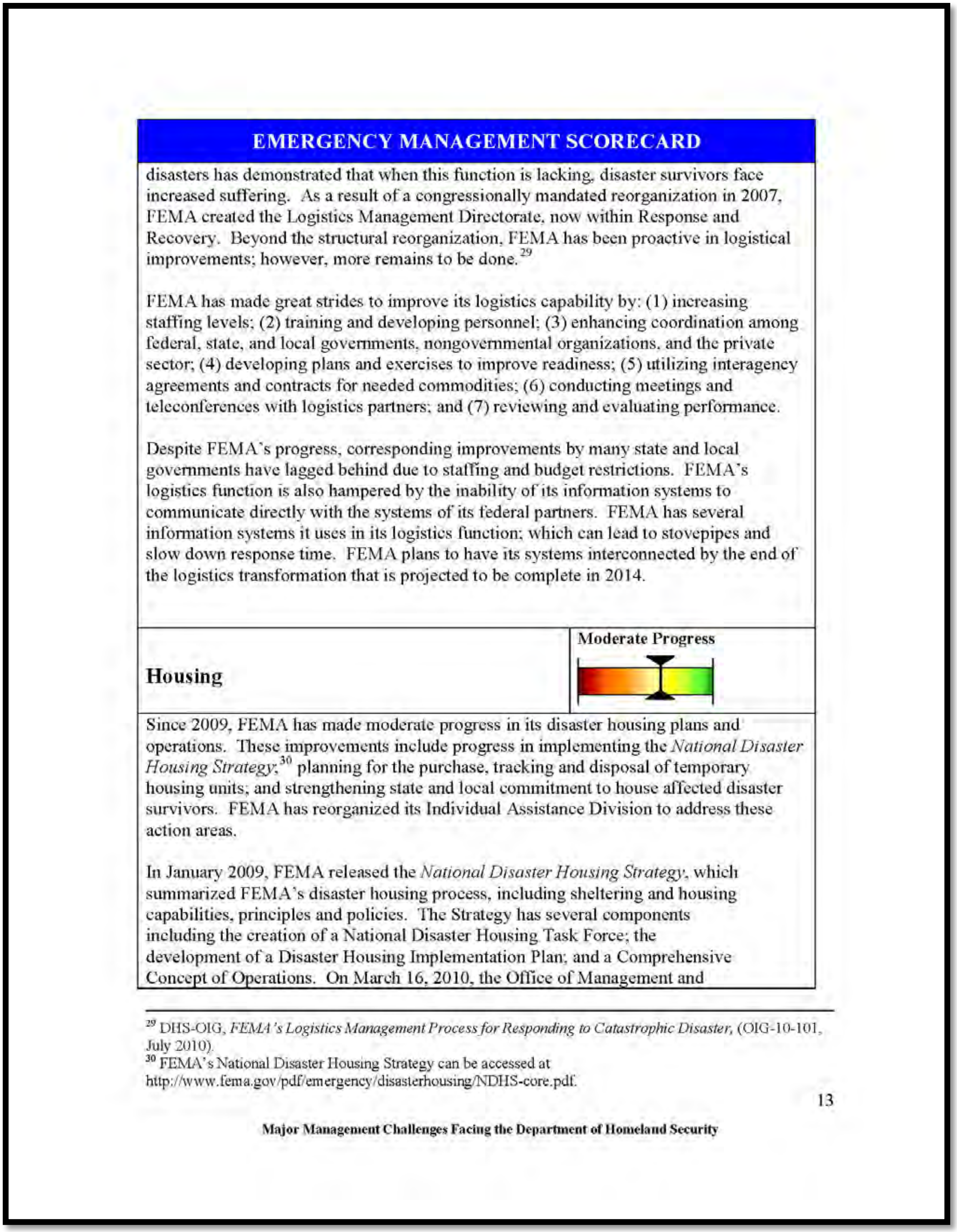
Emergency Management

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

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

EMERGENCY MANAGEMENT SCORECARD	
Logistics	**Moderate Progress**
When disaster strikes, FEMA must be prepared to quickly provide goods and services to help state and local governments respond to the disaster. FEMA's response in past	

[26] Public Law 109-295, Title VI – National Emergency Management, of the *Department of Homeland Security Appropriations Act of 2007*.
[27] DHS-OIG, *FEMA's Preparedness for the Next Catastrophic Disaster*, (OIG-08-34, March 2008).
[28] DHS-OIG, *FEMA's Preparedness for the Next Catastrophic Disaster – An Update*, (OIG-10-123, September 2010).



EMERGENCY MANAGEMENT SCORECARD

disasters has demonstrated that when this function is lacking, disaster survivors face increased suffering. As a result of a congressionally mandated reorganization in 2007, FEMA created the Logistics Management Directorate, now within Response and Recovery. Beyond the structural reorganization, FEMA has been proactive in logistical improvements; however, more remains to be done.[29]

FEMA has made great strides to improve its logistics capability by: (1) increasing staffing levels; (2) training and developing personnel; (3) enhancing coordination among federal, state, and local governments, nongovernmental organizations, and the private sector; (4) developing plans and exercises to improve readiness; (5) utilizing interagency agreements and contracts for needed commodities; (6) conducting meetings and teleconferences with logistics partners; and (7) reviewing and evaluating performance.

Despite FEMA's progress, corresponding improvements by many state and local governments have lagged behind due to staffing and budget restrictions. FEMA's logistics function is also hampered by the inability of its information systems to communicate directly with the systems of its federal partners. FEMA has several information systems it uses in its logistics function; which can lead to stovepipes and slow down response time. FEMA plans to have its systems interconnected by the end of the logistics transformation that is projected to be complete in 2014.

Housing

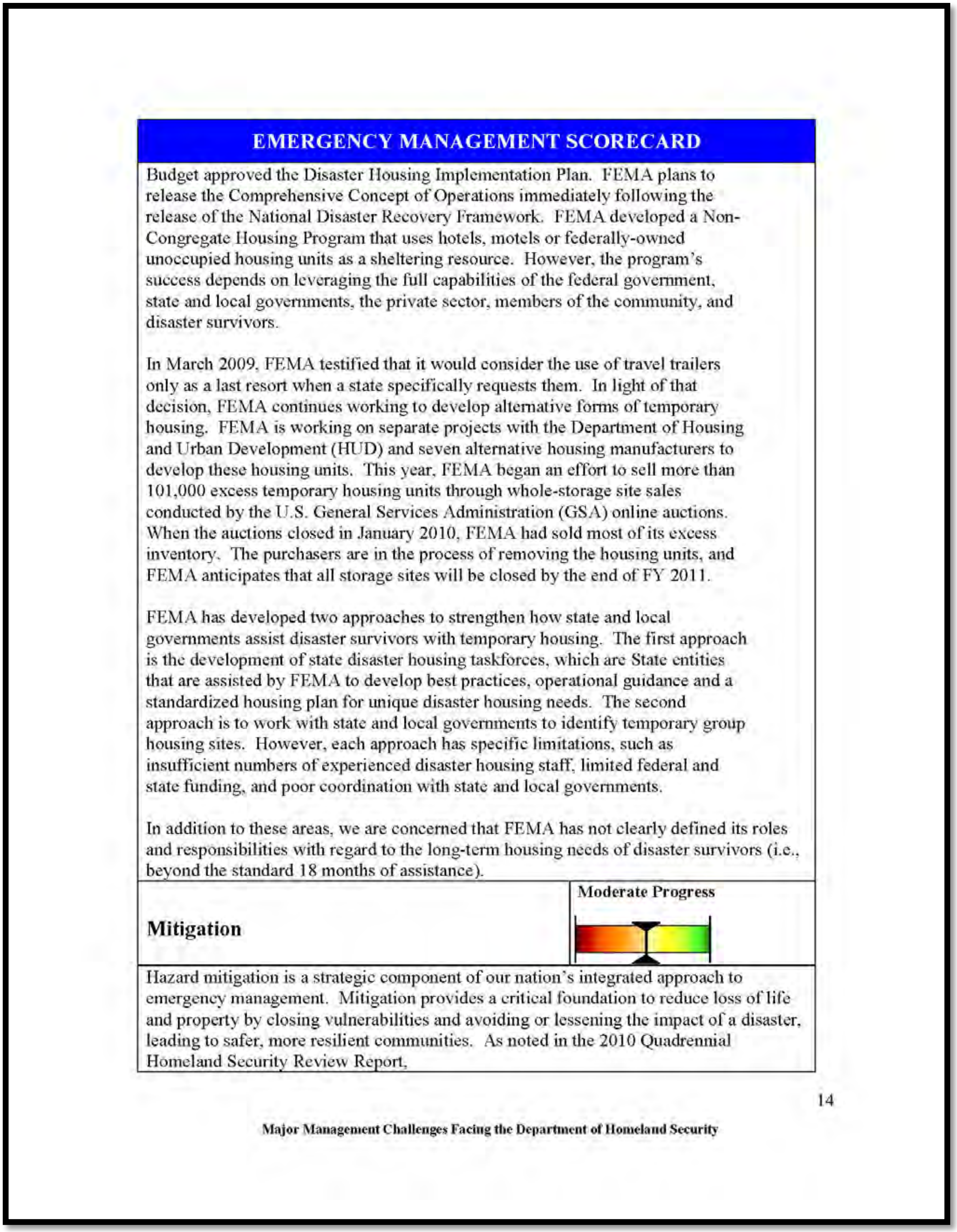
Moderate Progress

Since 2009, FEMA has made moderate progress in its disaster housing plans and operations. These improvements include progress in implementing the *National Disaster Housing Strategy*,[30] planning for the purchase, tracking and disposal of temporary housing units; and strengthening state and local commitment to house affected disaster survivors. FEMA has reorganized its Individual Assistance Division to address these action areas.

In January 2009, FEMA released the *National Disaster Housing Strategy*, which summarized FEMA's disaster housing process, including sheltering and housing capabilities, principles and policies. The Strategy has several components including the creation of a National Disaster Housing Task Force; the development of a Disaster Housing Implementation Plan; and a Comprehensive Concept of Operations. On March 16, 2010, the Office of Management and

[29] DHS-OIG, *FEMA's Logistics Management Process for Responding to Catastrophic Disaster*, (OIG-10-101, July 2010).

[30] FEMA's National Disaster Housing Strategy can be accessed at http://www.fema.gov/pdf/emergency/disasterhousing/NDHS-core.pdf.



EMERGENCY MANAGEMENT SCORECARD

Budget approved the Disaster Housing Implementation Plan. FEMA plans to release the Comprehensive Concept of Operations immediately following the release of the National Disaster Recovery Framework. FEMA developed a Non-Congregate Housing Program that uses hotels, motels or federally-owned unoccupied housing units as a sheltering resource. However, the program's success depends on leveraging the full capabilities of the federal government, state and local governments, the private sector, members of the community, and disaster survivors.

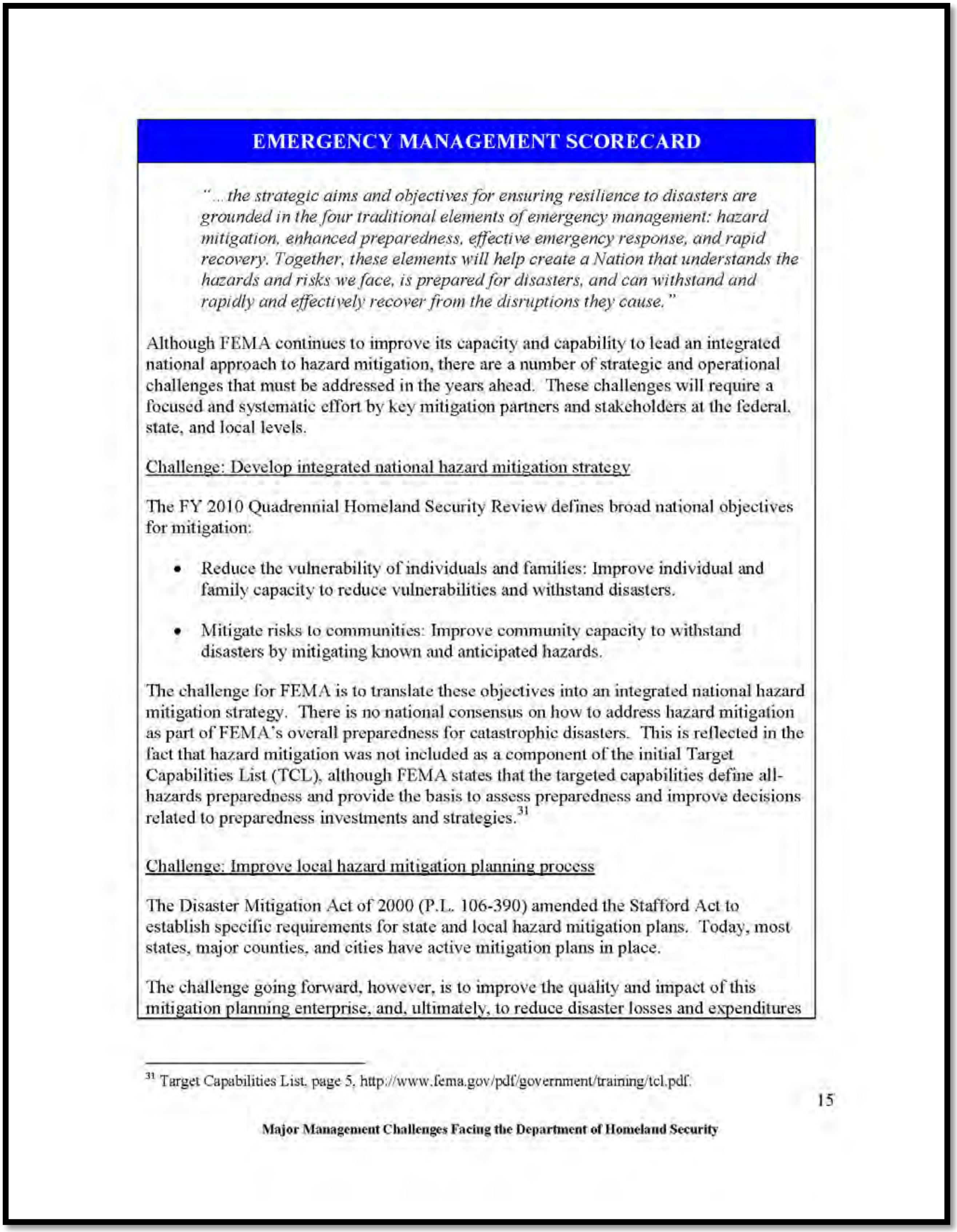
In March 2009, FEMA testified that it would consider the use of travel trailers only as a last resort when a state specifically requests them. In light of that decision, FEMA continues working to develop alternative forms of temporary housing. FEMA is working on separate projects with the Department of Housing and Urban Development (HUD) and seven alternative housing manufacturers to develop these housing units. This year, FEMA began an effort to sell more than 101,000 excess temporary housing units through whole-storage site sales conducted by the U.S. General Services Administration (GSA) online auctions. When the auctions closed in January 2010, FEMA had sold most of its excess inventory. The purchasers are in the process of removing the housing units, and FEMA anticipates that all storage sites will be closed by the end of FY 2011.

FEMA has developed two approaches to strengthen how state and local governments assist disaster survivors with temporary housing. The first approach is the development of state disaster housing taskforces, which are State entities that are assisted by FEMA to develop best practices, operational guidance and a standardized housing plan for unique disaster housing needs. The second approach is to work with state and local governments to identify temporary group housing sites. However, each approach has specific limitations, such as insufficient numbers of experienced disaster housing staff, limited federal and state funding, and poor coordination with state and local governments.

In addition to these areas, we are concerned that FEMA has not clearly defined its roles and responsibilities with regard to the long-term housing needs of disaster survivors (i.e., beyond the standard 18 months of assistance).

Mitigation	**Moderate Progress**

Hazard mitigation is a strategic component of our nation's integrated approach to emergency management. Mitigation provides a critical foundation to reduce loss of life and property by closing vulnerabilities and avoiding or lessening the impact of a disaster, leading to safer, more resilient communities. As noted in the 2010 Quadrennial Homeland Security Review Report,



EMERGENCY MANAGEMENT SCORECARD

> *"... the strategic aims and objectives for ensuring resilience to disasters are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements will help create a Nation that understands the hazards and risks we face, is prepared for disasters, and can withstand and rapidly and effectively recover from the disruptions they cause."*

Although FEMA continues to improve its capacity and capability to lead an integrated national approach to hazard mitigation, there are a number of strategic and operational challenges that must be addressed in the years ahead. These challenges will require a focused and systematic effort by key mitigation partners and stakeholders at the federal, state, and local levels.

Challenge: Develop integrated national hazard mitigation strategy

The FY 2010 Quadrennial Homeland Security Review defines broad national objectives for mitigation:

- Reduce the vulnerability of individuals and families: Improve individual and family capacity to reduce vulnerabilities and withstand disasters.
- Mitigate risks to communities: Improve community capacity to withstand disasters by mitigating known and anticipated hazards.

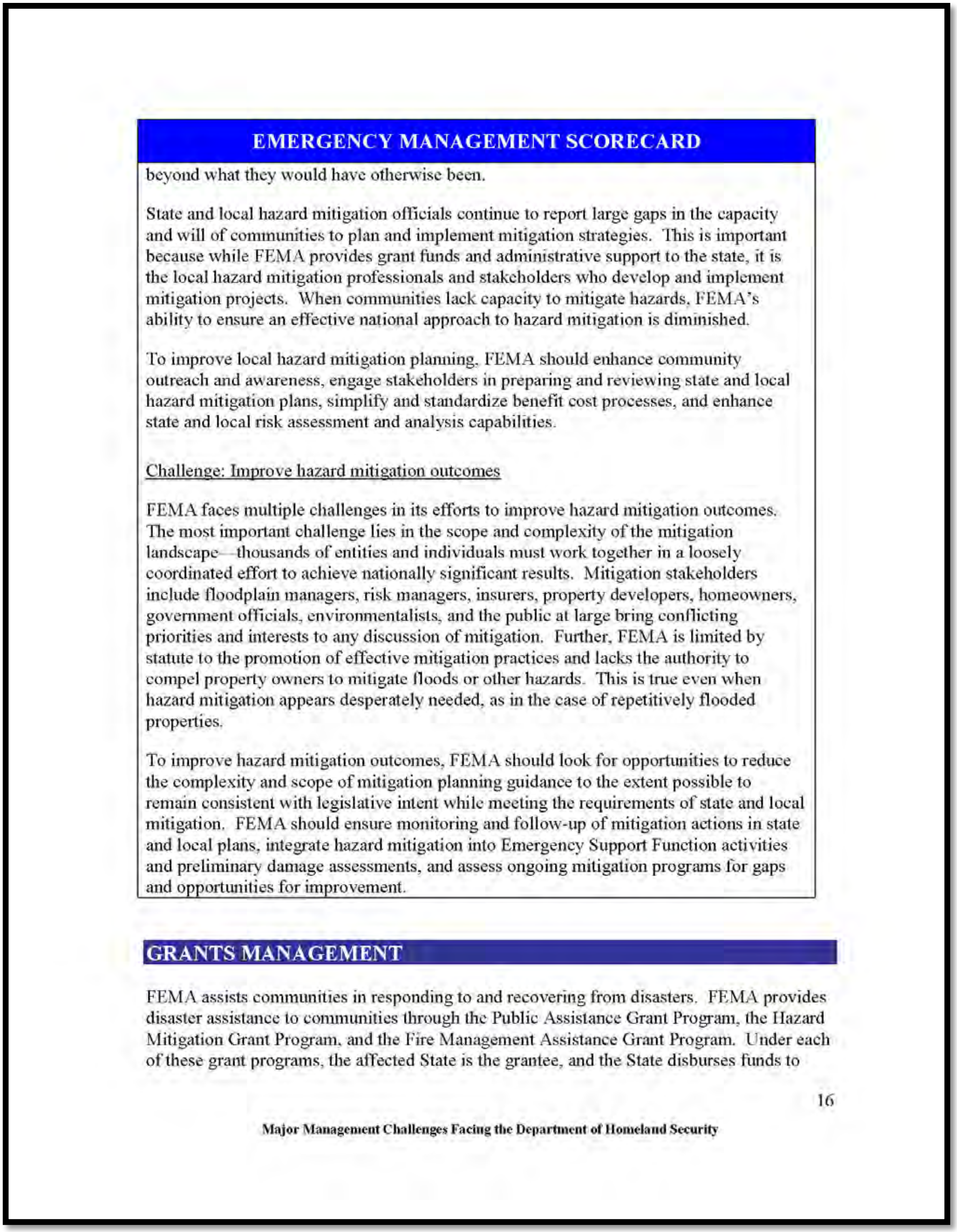
The challenge for FEMA is to translate these objectives into an integrated national hazard mitigation strategy. There is no national consensus on how to address hazard mitigation as part of FEMA's overall preparedness for catastrophic disasters. This is reflected in the fact that hazard mitigation was not included as a component of the initial Target Capabilities List (TCL), although FEMA states that the targeted capabilities define all-hazards preparedness and provide the basis to assess preparedness and improve decisions related to preparedness investments and strategies.[31]

Challenge: Improve local hazard mitigation planning process

The Disaster Mitigation Act of 2000 (P.L. 106-390) amended the Stafford Act to establish specific requirements for state and local hazard mitigation plans. Today, most states, major counties, and cities have active mitigation plans in place.

The challenge going forward, however, is to improve the quality and impact of this mitigation planning enterprise, and, ultimately, to reduce disaster losses and expenditures

[31] Target Capabilities List, page 5, http://www.fema.gov/pdf/government/training/tcl.pdf.



EMERGENCY MANAGEMENT SCORECARD

beyond what they would have otherwise been.

State and local hazard mitigation officials continue to report large gaps in the capacity and will of communities to plan and implement mitigation strategies. This is important because while FEMA provides grant funds and administrative support to the state, it is the local hazard mitigation professionals and stakeholders who develop and implement mitigation projects. When communities lack capacity to mitigate hazards, FEMA's ability to ensure an effective national approach to hazard mitigation is diminished.

To improve local hazard mitigation planning, FEMA should enhance community outreach and awareness, engage stakeholders in preparing and reviewing state and local hazard mitigation plans, simplify and standardize benefit cost processes, and enhance state and local risk assessment and analysis capabilities.

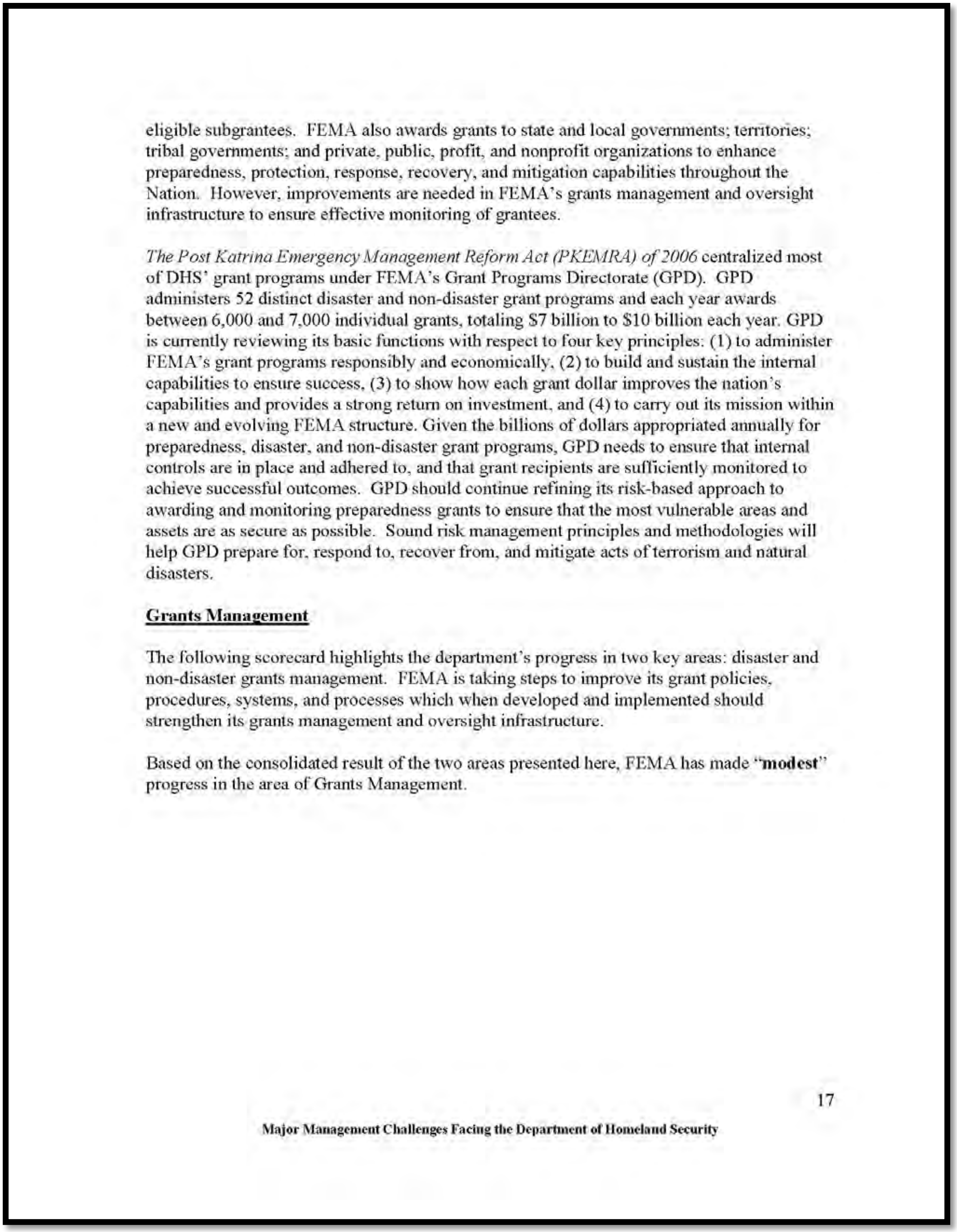
Challenge: Improve hazard mitigation outcomes

FEMA faces multiple challenges in its efforts to improve hazard mitigation outcomes. The most important challenge lies in the scope and complexity of the mitigation landscape—thousands of entities and individuals must work together in a loosely coordinated effort to achieve nationally significant results. Mitigation stakeholders include floodplain managers, risk managers, insurers, property developers, homeowners, government officials, environmentalists, and the public at large bring conflicting priorities and interests to any discussion of mitigation. Further, FEMA is limited by statute to the promotion of effective mitigation practices and lacks the authority to compel property owners to mitigate floods or other hazards. This is true even when hazard mitigation appears desperately needed, as in the case of repetitively flooded properties.

To improve hazard mitigation outcomes, FEMA should look for opportunities to reduce the complexity and scope of mitigation planning guidance to the extent possible to remain consistent with legislative intent while meeting the requirements of state and local mitigation. FEMA should ensure monitoring and follow-up of mitigation actions in state and local plans, integrate hazard mitigation into Emergency Support Function activities and preliminary damage assessments, and assess ongoing mitigation programs for gaps and opportunities for improvement.

GRANTS MANAGEMENT

FEMA assists communities in responding to and recovering from disasters. FEMA provides disaster assistance to communities through the Public Assistance Grant Program, the Hazard Mitigation Grant Program, and the Fire Management Assistance Grant Program. Under each of these grant programs, the affected State is the grantee, and the State disburses funds to



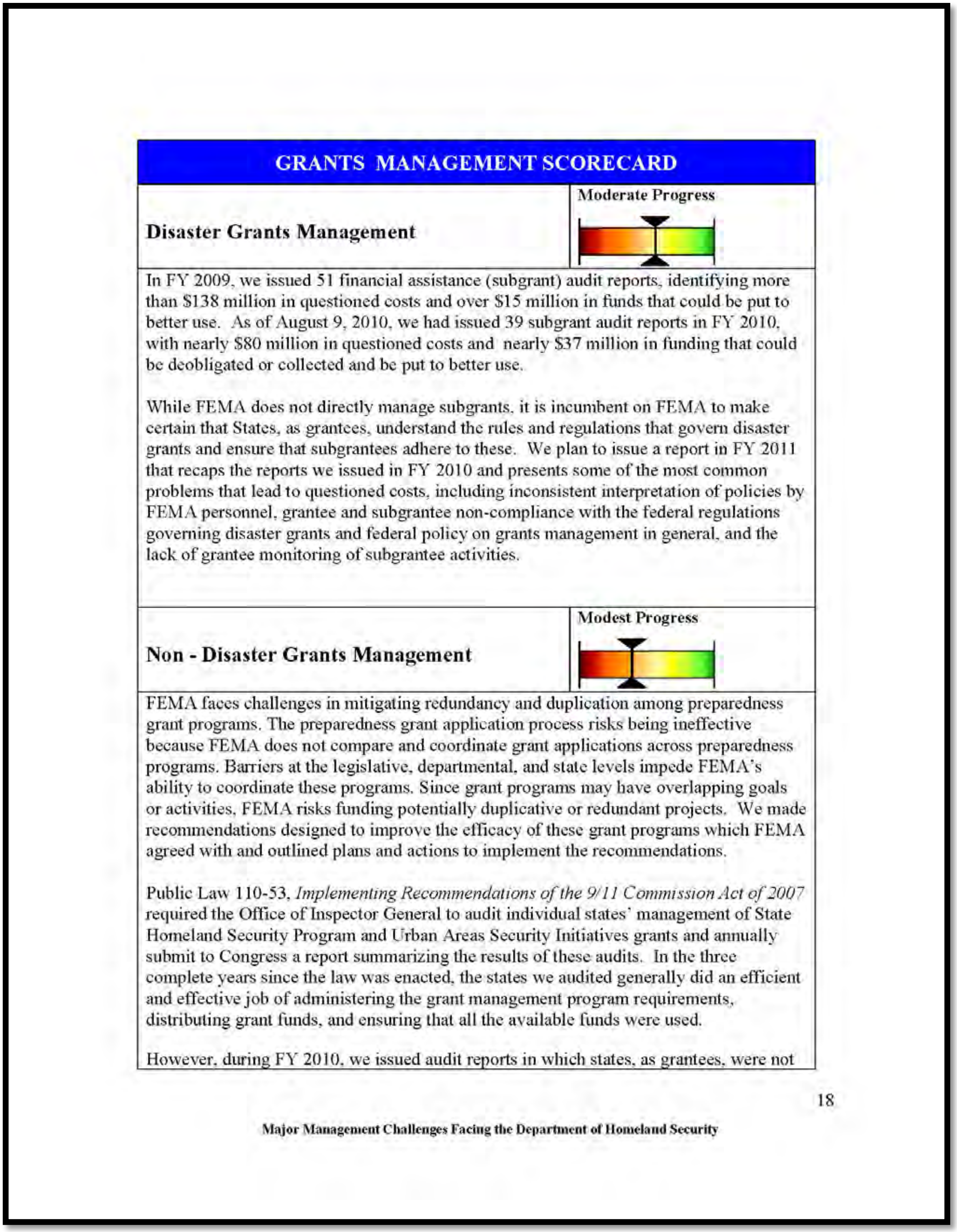
eligible subgrantees. FEMA also awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. However, improvements are needed in FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees.

The Post Katrina Emergency Management Reform Act (PKEMRA) of 2006 centralized most of DHS' grant programs under FEMA's Grant Programs Directorate (GPD). GPD administers 52 distinct disaster and non-disaster grant programs and each year awards between 6,000 and 7,000 individual grants, totaling $7 billion to $10 billion each year. GPD is currently reviewing its basic functions with respect to four key principles: (1) to administer FEMA's grant programs responsibly and economically, (2) to build and sustain the internal capabilities to ensure success, (3) to show how each grant dollar improves the nation's capabilities and provides a strong return on investment, and (4) to carry out its mission within a new and evolving FEMA structure. Given the billions of dollars appropriated annually for preparedness, disaster, and non-disaster grant programs, GPD needs to ensure that internal controls are in place and adhered to, and that grant recipients are sufficiently monitored to achieve successful outcomes. GPD should continue refining its risk-based approach to awarding and monitoring preparedness grants to ensure that the most vulnerable areas and assets are as secure as possible. Sound risk management principles and methodologies will help GPD prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.

Grants Management

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

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



GRANTS MANAGEMENT SCORECARD

Disaster Grants Management

Moderate Progress

In FY 2009, we issued 51 financial assistance (subgrant) audit reports, identifying more than $138 million in questioned costs and over $15 million in funds that could be put to better use. As of August 9, 2010, we had issued 39 subgrant audit reports in FY 2010, with nearly $80 million in questioned costs and nearly $37 million in funding that could be deobligated or collected and be put to better use.

While FEMA does not directly manage subgrants, it is incumbent on FEMA to make certain that States, as grantees, understand the rules and regulations that govern disaster grants and ensure that subgrantees adhere to these. We plan to issue a report in FY 2011 that recaps the reports we issued in FY 2010 and presents some of the most common problems that lead to questioned costs, including inconsistent interpretation of policies by FEMA personnel, grantee and subgrantee non-compliance with the federal regulations governing disaster grants and federal policy on grants management in general, and the lack of grantee monitoring of subgrantee activities.

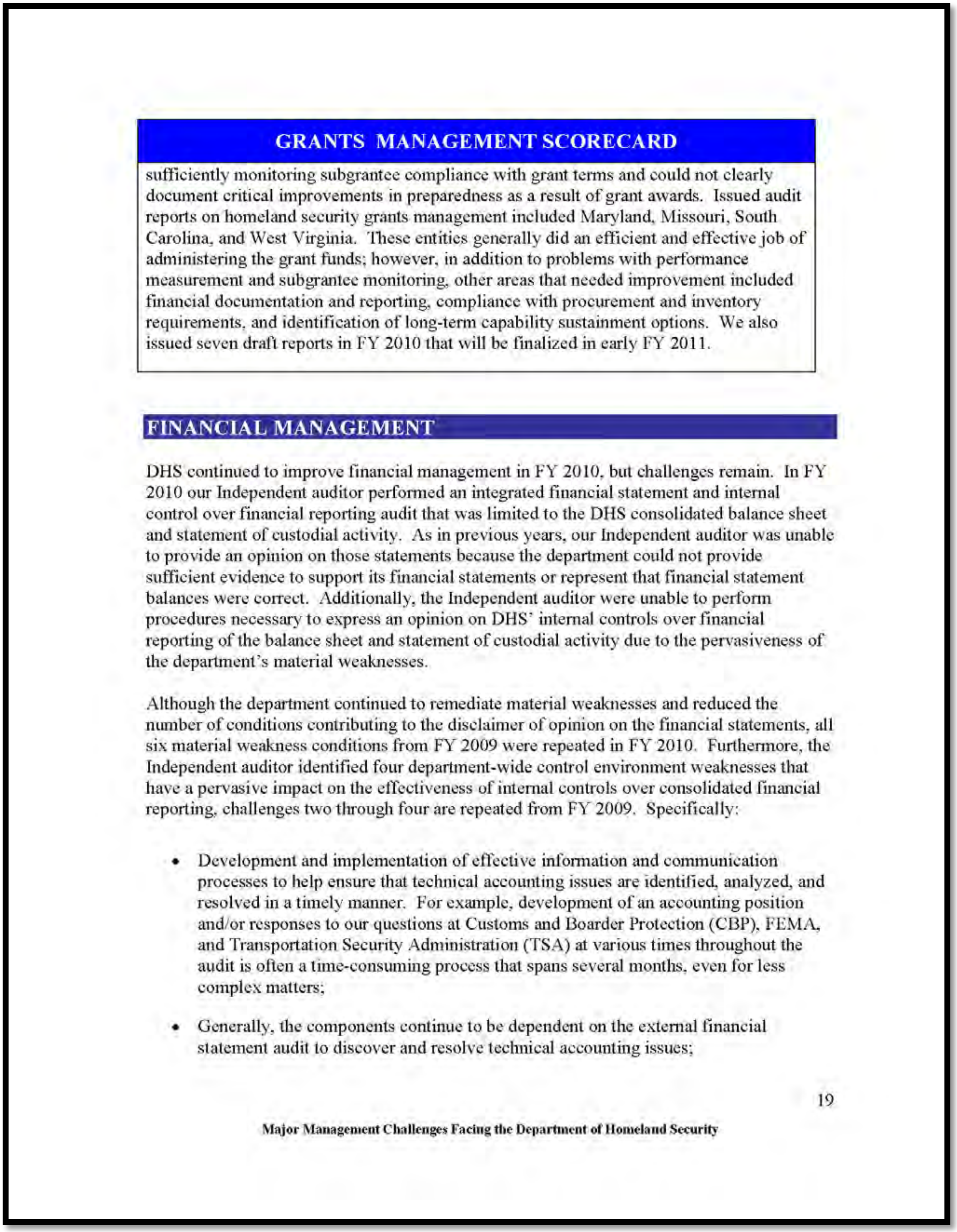
Non - Disaster Grants Management

Modest Progress

FEMA faces challenges in mitigating redundancy and duplication among preparedness grant programs. The preparedness grant application process risks being ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Barriers at the legislative, departmental, and state levels impede FEMA's ability to coordinate these programs. Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects. We made recommendations designed to improve the efficacy of these grant programs which FEMA agreed with and outlined plans and actions to implement the recommendations.

Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007* required the Office of Inspector General to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the three complete years since the law was enacted, the states we audited generally did an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used.

However, during FY 2010, we issued audit reports in which states, as grantees, were not



GRANTS MANAGEMENT SCORECARD

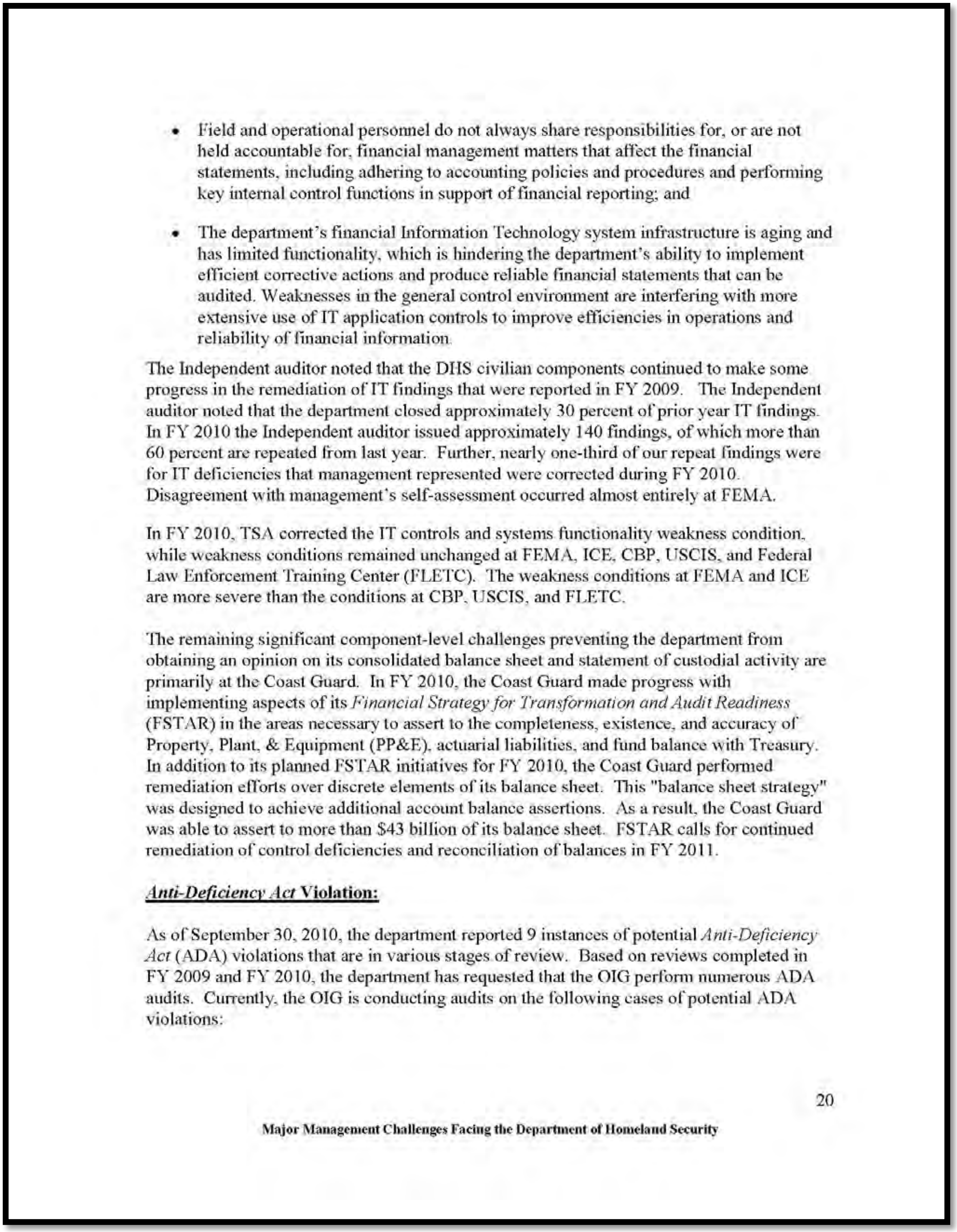
sufficiently monitoring subgrantee compliance with grant terms and could not clearly document critical improvements in preparedness as a result of grant awards. Issued audit reports on homeland security grants management included Maryland, Missouri, South Carolina, and West Virginia. These entities generally did an efficient and effective job of administering the grant funds; however, in addition to problems with performance measurement and subgrantee monitoring, other areas that needed improvement included financial documentation and reporting, compliance with procurement and inventory requirements, and identification of long-term capability sustainment options. We also issued seven draft reports in FY 2010 that will be finalized in early FY 2011.

FINANCIAL MANAGEMENT

DHS continued to improve financial management in FY 2010, but challenges remain. In FY 2010 our Independent auditor performed an integrated financial statement and internal control over financial reporting audit that was limited to the DHS consolidated balance sheet and statement of custodial activity. As in previous years, our Independent auditor was unable to provide an opinion on those statements because the department could not provide sufficient evidence to support its financial statements or represent that financial statement balances were correct. Additionally, the Independent auditor were unable to perform procedures necessary to express an opinion on DHS' internal controls over financial reporting of the balance sheet and statement of custodial activity due to the pervasiveness of the department's material weaknesses.

Although the department continued to remediate material weaknesses and reduced the number of conditions contributing to the disclaimer of opinion on the financial statements, all six material weakness conditions from FY 2009 were repeated in FY 2010. Furthermore, the Independent auditor identified four department-wide control environment weaknesses that have a pervasive impact on the effectiveness of internal controls over consolidated financial reporting, challenges two through four are repeated from FY 2009. Specifically:

- Development and implementation of effective information and communication processes to help ensure that technical accounting issues are identified, analyzed, and resolved in a timely manner. For example, development of an accounting position and/or responses to our questions at Customs and Boarder Protection (CBP), FEMA, and Transportation Security Administration (TSA) at various times throughout the audit is often a time-consuming process that spans several months, even for less complex matters;
- Generally, the components continue to be dependent on the external financial statement audit to discover and resolve technical accounting issues;



- Field and operational personnel do not always share responsibilities for, or are not held accountable for, financial management matters that affect the financial statements, including adhering to accounting policies and procedures and performing key internal control functions in support of financial reporting; and

- The department's financial Information Technology system infrastructure is aging and has limited functionality, which is hindering the department's ability to implement efficient corrective actions and produce reliable financial statements that can be audited. Weaknesses in the general control environment are interfering with more extensive use of IT application controls to improve efficiencies in operations and reliability of financial information.

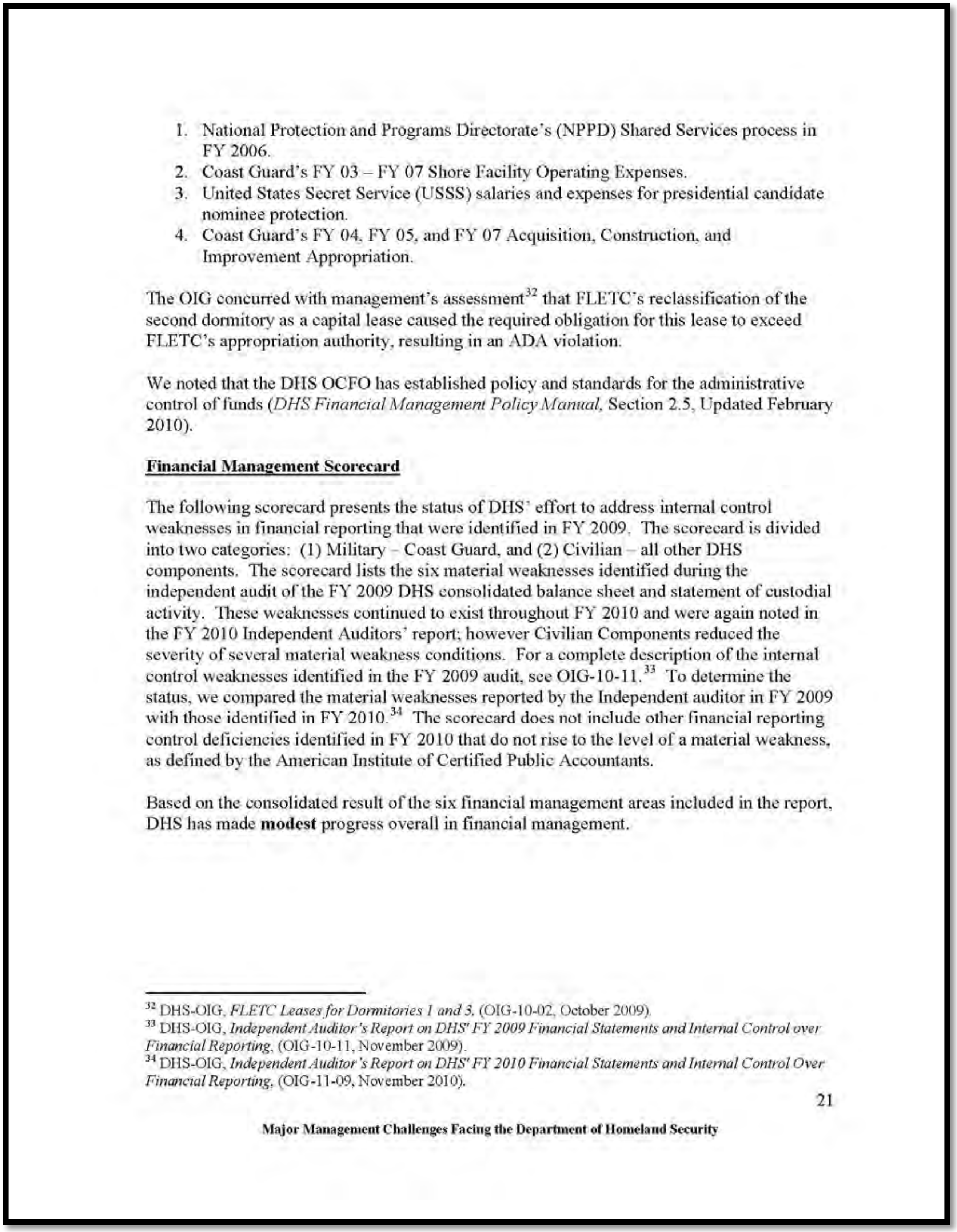
The Independent auditor noted that the DHS civilian components continued to make some progress in the remediation of IT findings that were reported in FY 2009. The Independent auditor noted that the department closed approximately 30 percent of prior year IT findings. In FY 2010 the Independent auditor issued approximately 140 findings, of which more than 60 percent are repeated from last year. Further, nearly one-third of our repeat findings were for IT deficiencies that management represented were corrected during FY 2010. Disagreement with management's self-assessment occurred almost entirely at FEMA.

In FY 2010, TSA corrected the IT controls and systems functionality weakness condition, while weakness conditions remained unchanged at FEMA, ICE, CBP, USCIS, and Federal Law Enforcement Training Center (FLETC). The weakness conditions at FEMA and ICE are more severe than the conditions at CBP, USCIS, and FLETC.

The remaining significant component-level challenges preventing the department from obtaining an opinion on its consolidated balance sheet and statement of custodial activity are primarily at the Coast Guard. In FY 2010, the Coast Guard made progress with implementing aspects of its *Financial Strategy for Transformation and Audit Readiness* (FSTAR) in the areas necessary to assert to the completeness, existence, and accuracy of Property, Plant, & Equipment (PP&E), actuarial liabilities, and fund balance with Treasury. In addition to its planned FSTAR initiatives for FY 2010, the Coast Guard performed remediation efforts over discrete elements of its balance sheet. This "balance sheet strategy" was designed to achieve additional account balance assertions. As a result, the Coast Guard was able to assert to more than $43 billion of its balance sheet. FSTAR calls for continued remediation of control deficiencies and reconciliation of balances in FY 2011.

<u>*Anti-Deficiency Act* Violation:</u>

As of September 30, 2010, the department reported 9 instances of potential *Anti-Deficiency Act* (ADA) violations that are in various stages of review. Based on reviews completed in FY 2009 and FY 2010, the department has requested that the OIG perform numerous ADA audits. Currently, the OIG is conducting audits on the following cases of potential ADA violations:



1. National Protection and Programs Directorate's (NPPD) Shared Services process in FY 2006.
2. Coast Guard's FY 03 – FY 07 Shore Facility Operating Expenses.
3. United States Secret Service (USSS) salaries and expenses for presidential candidate nominee protection.
4. Coast Guard's FY 04, FY 05, and FY 07 Acquisition, Construction, and Improvement Appropriation.

The OIG concurred with management's assessment[32] that FLETC's reclassification of the second dormitory as a capital lease caused the required obligation for this lease to exceed FLETC's appropriation authority, resulting in an ADA violation.

We noted that the DHS OCFO has established policy and standards for the administrative control of funds (*DHS Financial Management Policy Manual,* Section 2.5, Updated February 2010).

Financial Management Scorecard

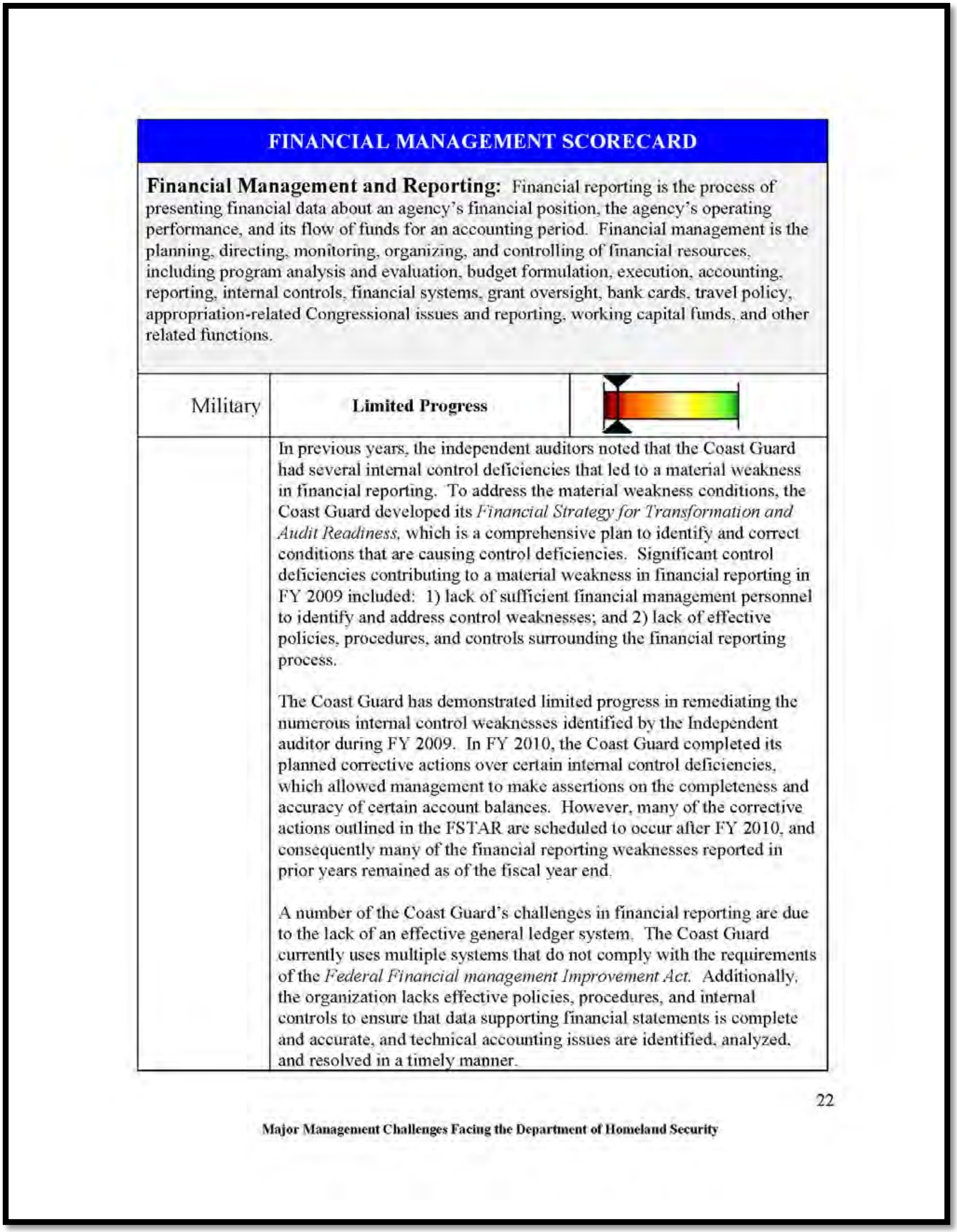
The following scorecard presents the status of DHS' effort to address internal control weaknesses in financial reporting that were identified in FY 2009. The scorecard is divided into two categories: (1) Military – Coast Guard, and (2) Civilian – all other DHS components. The scorecard lists the six material weaknesses identified during the independent audit of the FY 2009 DHS consolidated balance sheet and statement of custodial activity. These weaknesses continued to exist throughout FY 2010 and were again noted in the FY 2010 Independent Auditors' report; however Civilian Components reduced the severity of several material weakness conditions. For a complete description of the internal control weaknesses identified in the FY 2009 audit, see OIG-10-11.[33] To determine the status, we compared the material weaknesses reported by the Independent auditor in FY 2009 with those identified in FY 2010.[34] The scorecard does not include other financial reporting control deficiencies identified in FY 2010 that do not rise to the level of a material weakness, as defined by the American Institute of Certified Public Accountants.

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

[32] DHS-OIG, *FLETC Leases for Dormitories 1 and 3,* (OIG-10-02, October 2009).

[33] DHS-OIG, *Independent Auditor's Report on DHS' FY 2009 Financial Statements and Internal Control over Financial Reporting,* (OIG-10-11, November 2009).

[34] DHS-OIG, *Independent Auditor's Report on DHS' FY 2010 Financial Statements and Internal Control Over Financial Reporting,* (OIG-11-09, November 2010).



FINANCIAL MANAGEMENT SCORECARD

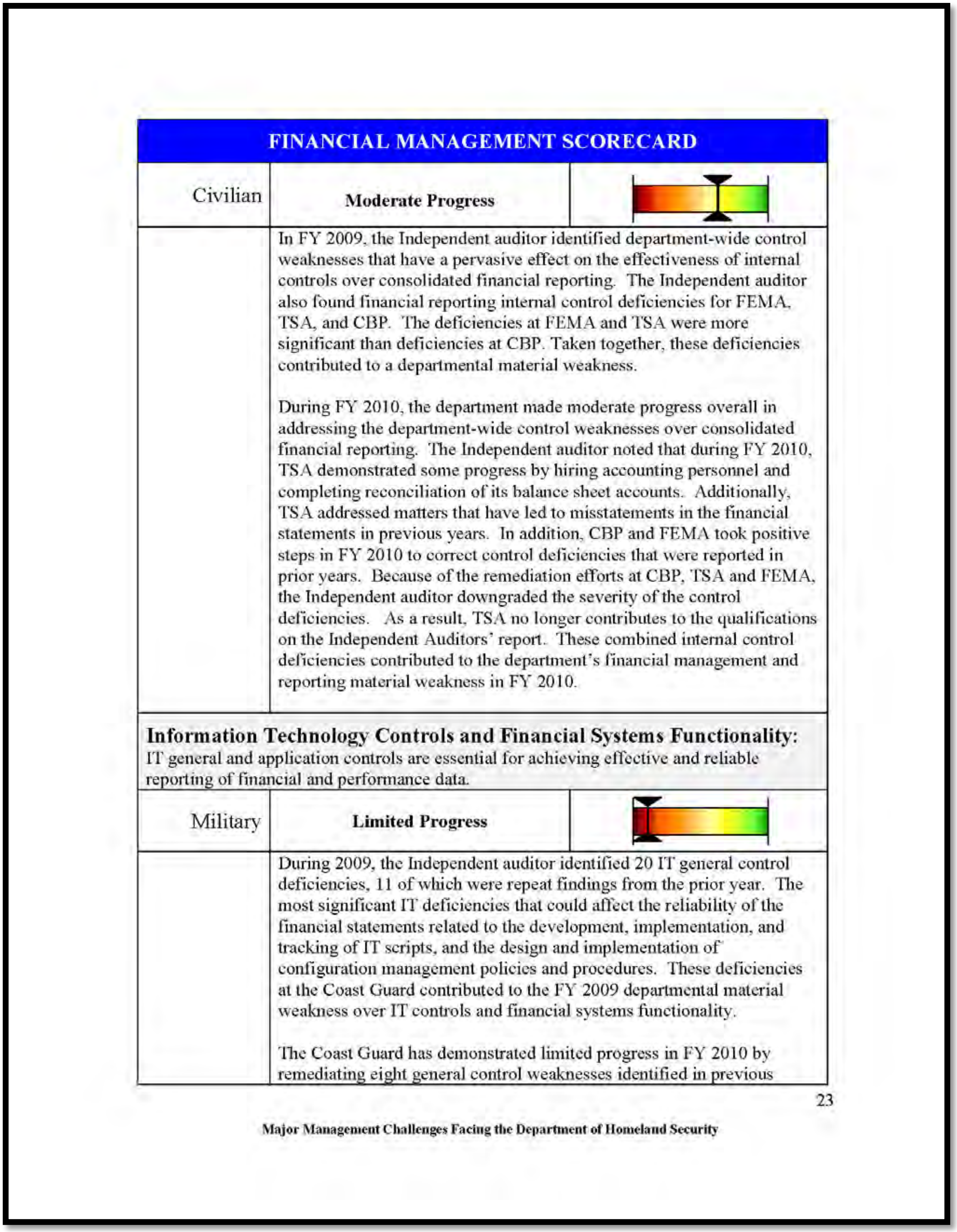
Financial Management and Reporting: Financial reporting is the process of presenting financial data about an agency's financial position, the agency's operating performance, and its flow of funds for an accounting period. Financial management is the planning, directing, monitoring, organizing, and controlling of financial resources, including program analysis and evaluation, budget formulation, execution, accounting, reporting, internal controls, financial systems, grant oversight, bank cards, travel policy, appropriation-related Congressional issues and reporting, working capital funds, and other related functions.

Military	**Limited Progress**	

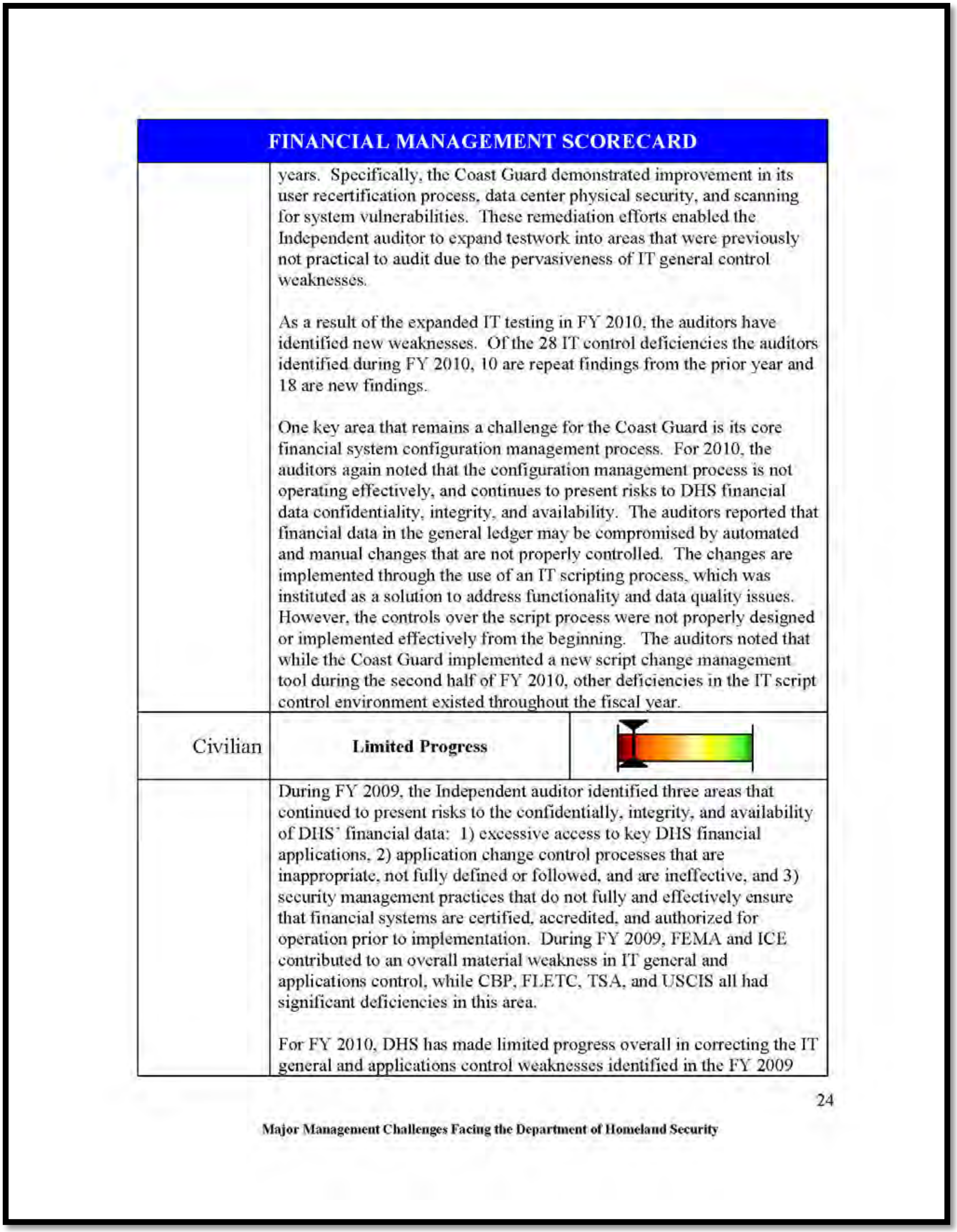
In previous years, the independent auditors noted that the Coast Guard had several internal control deficiencies that led to a material weakness in financial reporting. To address the material weakness conditions, the Coast Guard developed its *Financial Strategy for Transformation and Audit Readiness*, which is a comprehensive plan to identify and correct conditions that are causing control deficiencies. Significant control deficiencies contributing to a material weakness in financial reporting in FY 2009 included: 1) lack of sufficient financial management personnel to identify and address control weaknesses; and 2) lack of effective policies, procedures, and controls surrounding the financial reporting process.

The Coast Guard has demonstrated limited progress in remediating the numerous internal control weaknesses identified by the Independent auditor during FY 2009. In FY 2010, the Coast Guard completed its planned corrective actions over certain internal control deficiencies, which allowed management to make assertions on the completeness and accuracy of certain account balances. However, many of the corrective actions outlined in the FSTAR are scheduled to occur after FY 2010, and consequently many of the financial reporting weaknesses reported in prior years remained as of the fiscal year end.

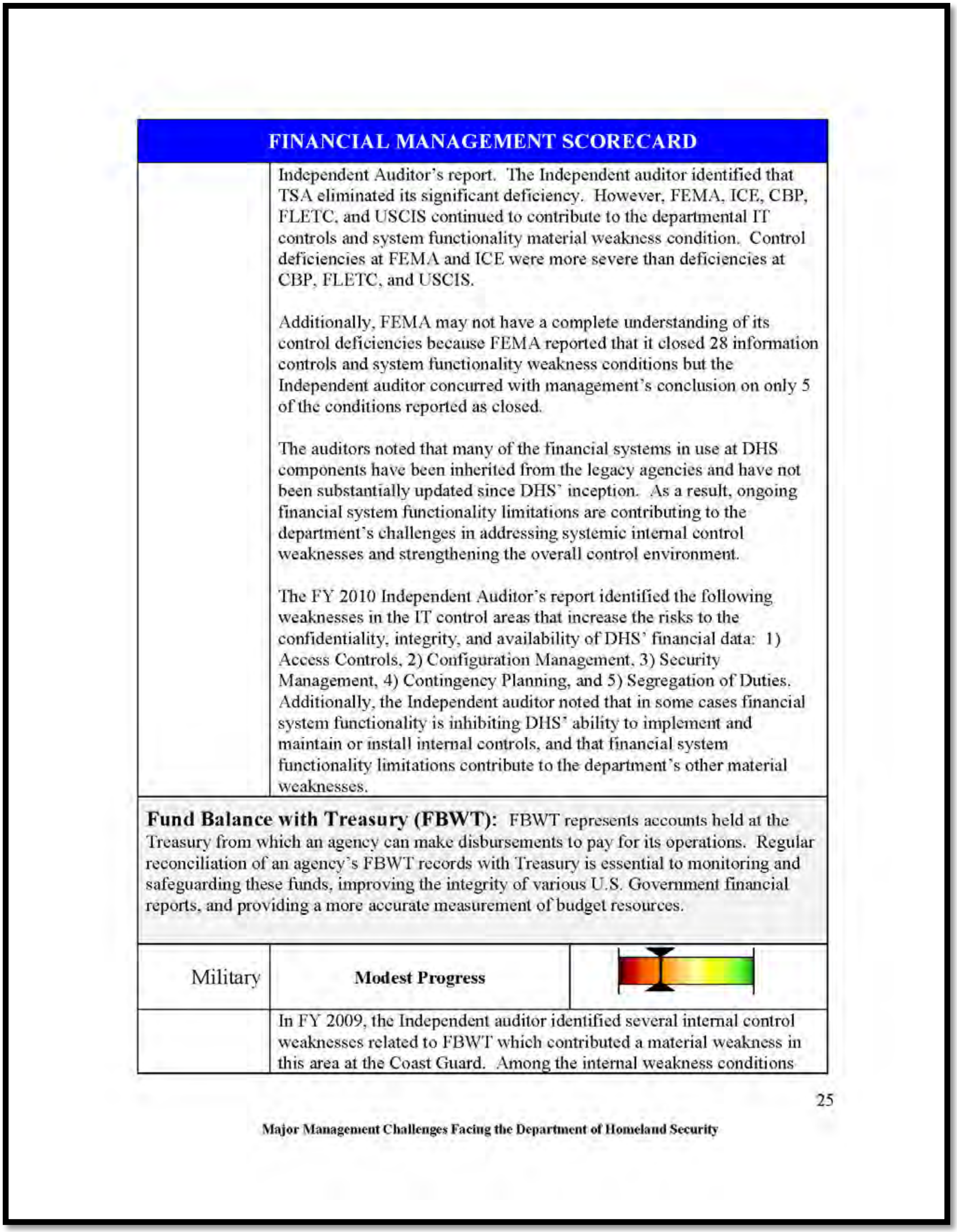
A number of the Coast Guard's challenges in financial reporting are due to the lack of an effective general ledger system. The Coast Guard currently uses multiple systems that do not comply with the requirements of the *Federal Financial management Improvement Act*. Additionally, the organization lacks effective policies, procedures, and internal controls to ensure that data supporting financial statements is complete and accurate, and technical accounting issues are identified, analyzed, and resolved in a timely manner.



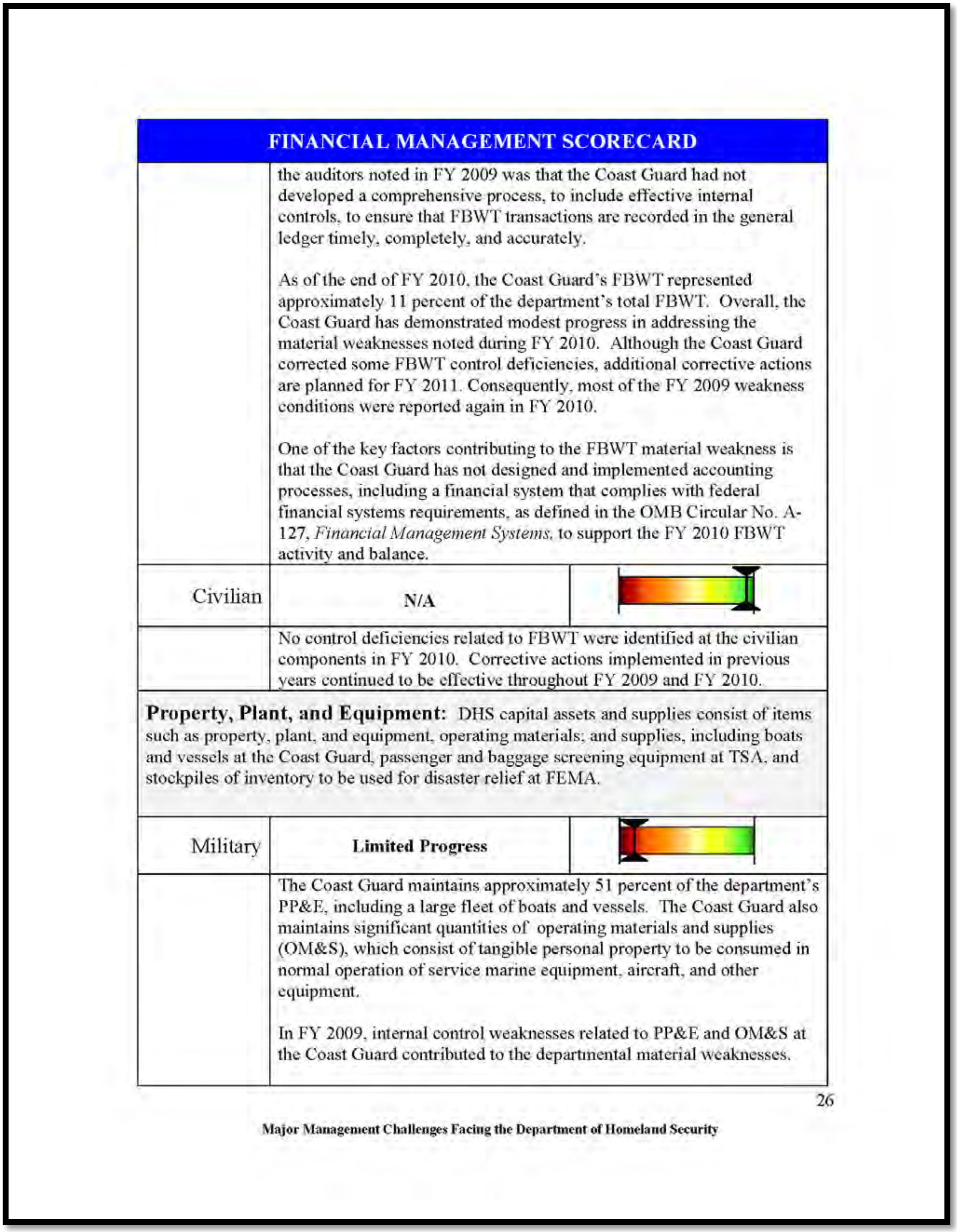
FINANCIAL MANAGEMENT SCORECARD		
Civilian	**Moderate Progress**	
	In FY 2009, the Independent auditor identified department-wide control weaknesses that have a pervasive effect on the effectiveness of internal controls over consolidated financial reporting. The Independent auditor also found financial reporting internal control deficiencies for FEMA, TSA, and CBP. The deficiencies at FEMA and TSA were more significant than deficiencies at CBP. Taken together, these deficiencies contributed to a departmental material weakness. During FY 2010, the department made moderate progress overall in addressing the department-wide control weaknesses over consolidated financial reporting. The Independent auditor noted that during FY 2010, TSA demonstrated some progress by hiring accounting personnel and completing reconciliation of its balance sheet accounts. Additionally, TSA addressed matters that have led to misstatements in the financial statements in previous years. In addition, CBP and FEMA took positive steps in FY 2010 to correct control deficiencies that were reported in prior years. Because of the remediation efforts at CBP, TSA and FEMA, the Independent auditor downgraded the severity of the control deficiencies. As a result, TSA no longer contributes to the qualifications on the Independent Auditors' report. These combined internal control deficiencies contributed to the department's financial management and reporting material weakness in FY 2010.	
Information Technology Controls and Financial Systems Functionality: IT general and application controls are essential for achieving effective and reliable reporting of financial and performance data.		
Military	**Limited Progress**	
	During 2009, the Independent auditor identified 20 IT general control deficiencies, 11 of which were repeat findings from the prior year. The most significant IT deficiencies that could affect the reliability of the financial statements related to the development, implementation, and tracking of IT scripts, and the design and implementation of configuration management policies and procedures. These deficiencies at the Coast Guard contributed to the FY 2009 departmental material weakness over IT controls and financial systems functionality. The Coast Guard has demonstrated limited progress in FY 2010 by remediating eight general control weaknesses identified in previous	



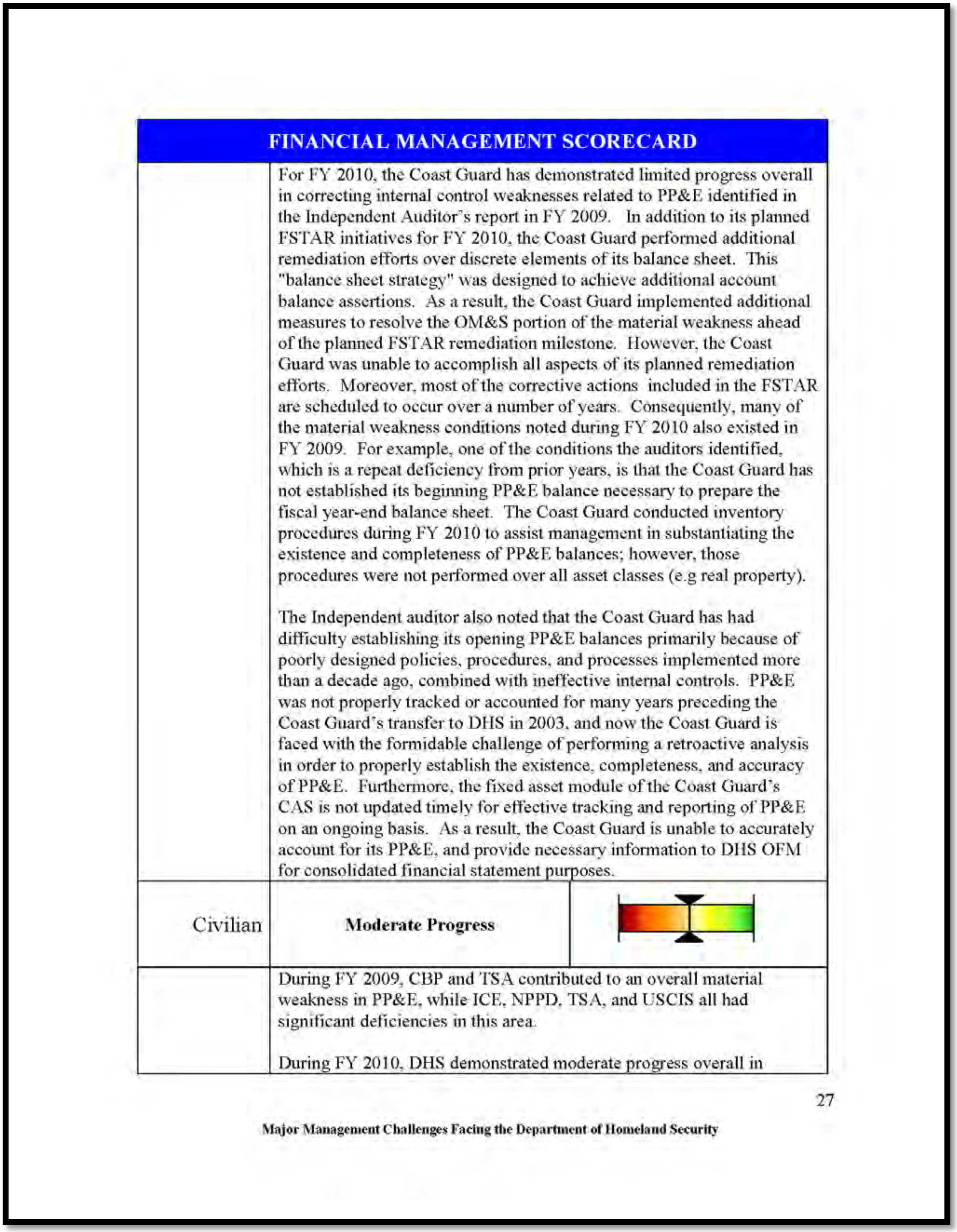
FINANCIAL MANAGEMENT SCORECARD		
	years. Specifically, the Coast Guard demonstrated improvement in its user recertification process, data center physical security, and scanning for system vulnerabilities. These remediation efforts enabled the Independent auditor to expand testwork into areas that were previously not practical to audit due to the pervasiveness of IT general control weaknesses. As a result of the expanded IT testing in FY 2010, the auditors have identified new weaknesses. Of the 28 IT control deficiencies the auditors identified during FY 2010, 10 are repeat findings from the prior year and 18 are new findings. One key area that remains a challenge for the Coast Guard is its core financial system configuration management process. For 2010, the auditors again noted that the configuration management process is not operating effectively, and continues to present risks to DHS financial data confidentiality, integrity, and availability. The auditors reported that financial data in the general ledger may be compromised by automated and manual changes that are not properly controlled. The changes are implemented through the use of an IT scripting process, which was instituted as a solution to address functionality and data quality issues. However, the controls over the script process were not properly designed or implemented effectively from the beginning. The auditors noted that while the Coast Guard implemented a new script change management tool during the second half of FY 2010, other deficiencies in the IT script control environment existed throughout the fiscal year.	
Civilian	**Limited Progress**	
	During FY 2009, the Independent auditor identified three areas that continued to present risks to the confidentially, integrity, and availability of DHS' financial data: 1) excessive access to key DHS financial applications, 2) application change control processes that are inappropriate, not fully defined or followed, and are ineffective, and 3) security management practices that do not fully and effectively ensure that financial systems are certified, accredited, and authorized for operation prior to implementation. During FY 2009, FEMA and ICE contributed to an overall material weakness in IT general and applications control, while CBP, FLETC, TSA, and USCIS all had significant deficiencies in this area. For FY 2010, DHS has made limited progress overall in correcting the IT general and applications control weaknesses identified in the FY 2009	



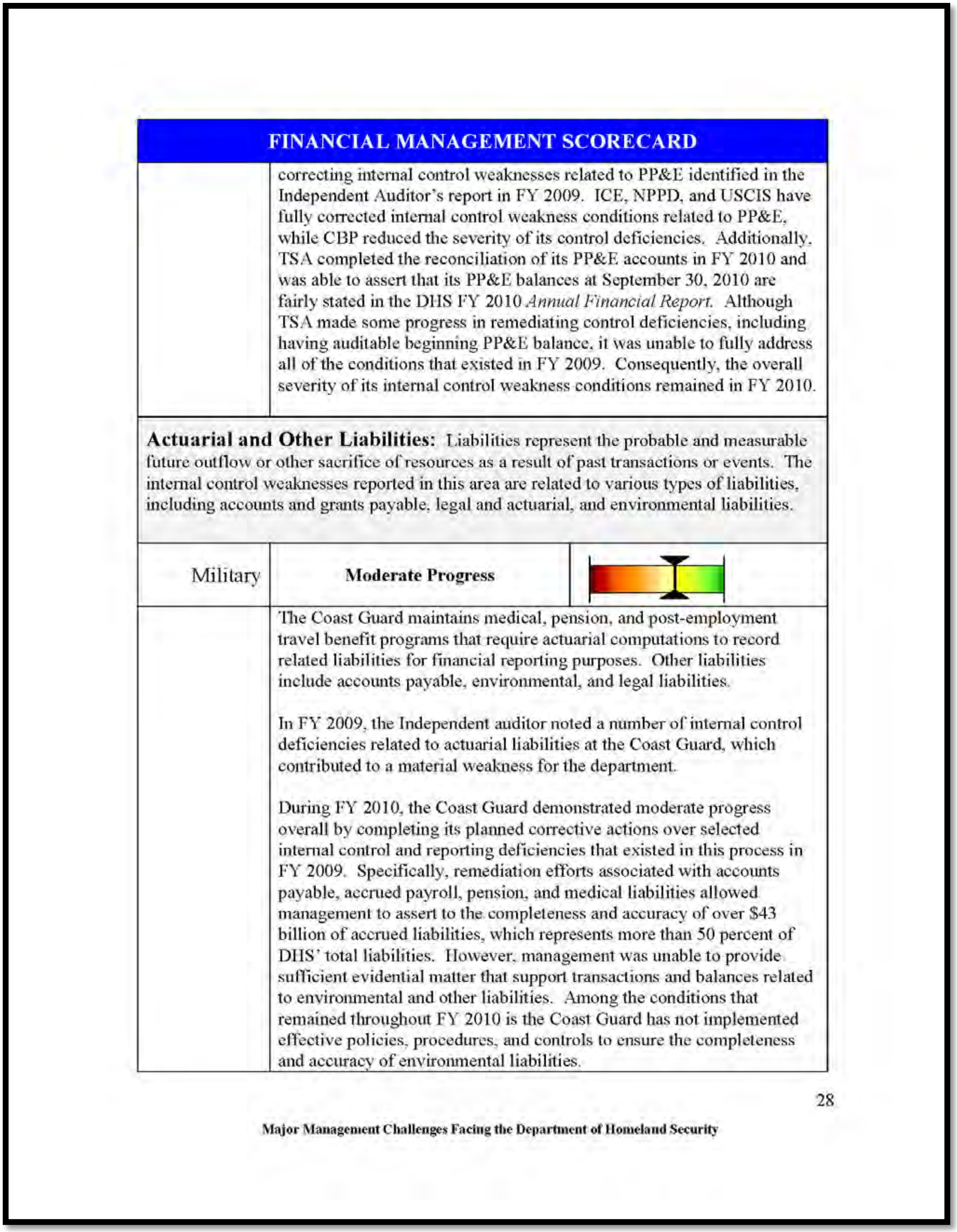
<table>
<tr><th colspan="3">FINANCIAL MANAGEMENT SCORECARD</th></tr>
<tr><td></td><td colspan="2">Independent Auditor's report. The Independent auditor identified that TSA eliminated its significant deficiency. However, FEMA, ICE, CBP, FLETC, and USCIS continued to contribute to the departmental IT controls and system functionality material weakness condition. Control deficiencies at FEMA and ICE were more severe than deficiencies at CBP, FLETC, and USCIS.
Additionally, FEMA may not have a complete understanding of its control deficiencies because FEMA reported that it closed 28 information controls and system functionality weakness conditions but the Independent auditor concurred with management's conclusion on only 5 of the conditions reported as closed.
The auditors noted that many of the financial systems in use at DHS components have been inherited from the legacy agencies and have not been substantially updated since DHS' inception. As a result, ongoing financial system functionality limitations are contributing to the department's challenges in addressing systemic internal control weaknesses and strengthening the overall control environment.
The FY 2010 Independent Auditor's report identified the following weaknesses in the IT control areas that increase the risks to the confidentiality, integrity, and availability of DHS' financial data: 1) Access Controls, 2) Configuration Management, 3) Security Management, 4) Contingency Planning, and 5) Segregation of Duties. Additionally, the Independent auditor noted that in some cases financial system functionality is inhibiting DHS' ability to implement and maintain or install internal controls, and that financial system functionality limitations contribute to the department's other material weaknesses.</td></tr>
<tr><td colspan="3"><b>Fund Balance with Treasury (FBWT):</b> FBWT represents accounts held at the Treasury from which an agency can make disbursements to pay for its operations. Regular reconciliation of an agency's FBWT records with Treasury is essential to monitoring and safeguarding these funds, improving the integrity of various U.S. Government financial reports, and providing a more accurate measurement of budget resources.</td></tr>
<tr><td>Military</td><td><b>Modest Progress</b></td><td></td></tr>
<tr><td></td><td colspan="2">In FY 2009, the Independent auditor identified several internal control weaknesses related to FBWT which contributed a material weakness in this area at the Coast Guard. Among the internal weakness conditions</td></tr>
</table>



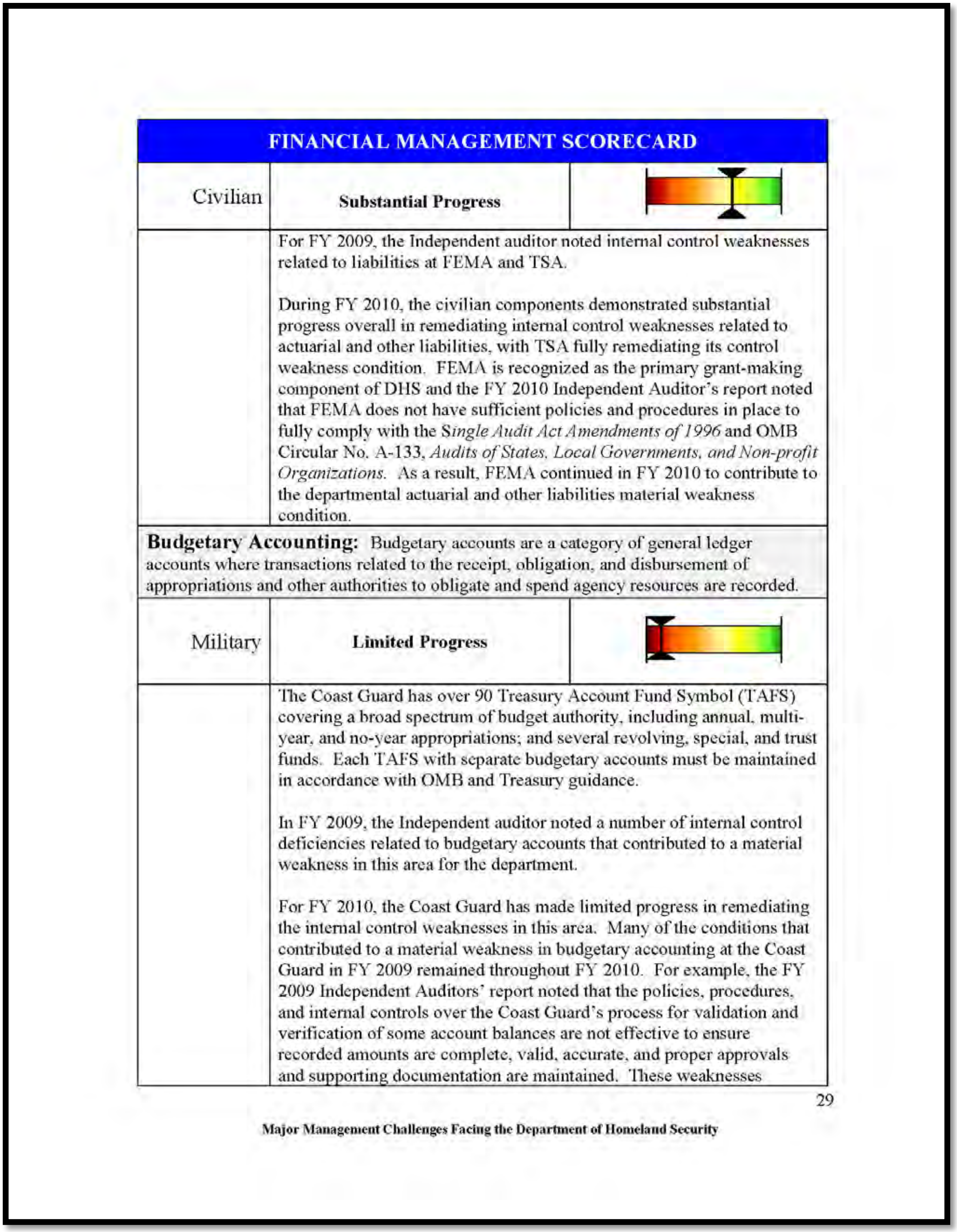
FINANCIAL MANAGEMENT SCORECARD		
	the auditors noted in FY 2009 was that the Coast Guard had not developed a comprehensive process, to include effective internal controls, to ensure that FBWT transactions are recorded in the general ledger timely, completely, and accurately. As of the end of FY 2010, the Coast Guard's FBWT represented approximately 11 percent of the department's total FBWT. Overall, the Coast Guard has demonstrated modest progress in addressing the material weaknesses noted during FY 2010. Although the Coast Guard corrected some FBWT control deficiencies, additional corrective actions are planned for FY 2011. Consequently, most of the FY 2009 weakness conditions were reported again in FY 2010. One of the key factors contributing to the FBWT material weakness is that the Coast Guard has not designed and implemented accounting processes, including a financial system that complies with federal financial systems requirements, as defined in the OMB Circular No. A-127, *Financial Management Systems*, to support the FY 2010 FBWT activity and balance.	
Civilian	**N/A**	
	No control deficiencies related to FBWT were identified at the civilian components in FY 2010. Corrective actions implemented in previous years continued to be effective throughout FY 2009 and FY 2010.	
Property, Plant, and Equipment: DHS capital assets and supplies consist of items such as property, plant, and equipment, operating materials; and supplies, including boats and vessels at the Coast Guard, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA.		
Military	**Limited Progress**	
	The Coast Guard maintains approximately 51 percent of the department's PP&E, including a large fleet of boats and vessels. The Coast Guard also maintains significant quantities of operating materials and supplies (OM&S), which consist of tangible personal property to be consumed in normal operation of service marine equipment, aircraft, and other equipment. In FY 2009, internal control weaknesses related to PP&E and OM&S at the Coast Guard contributed to the departmental material weaknesses.	



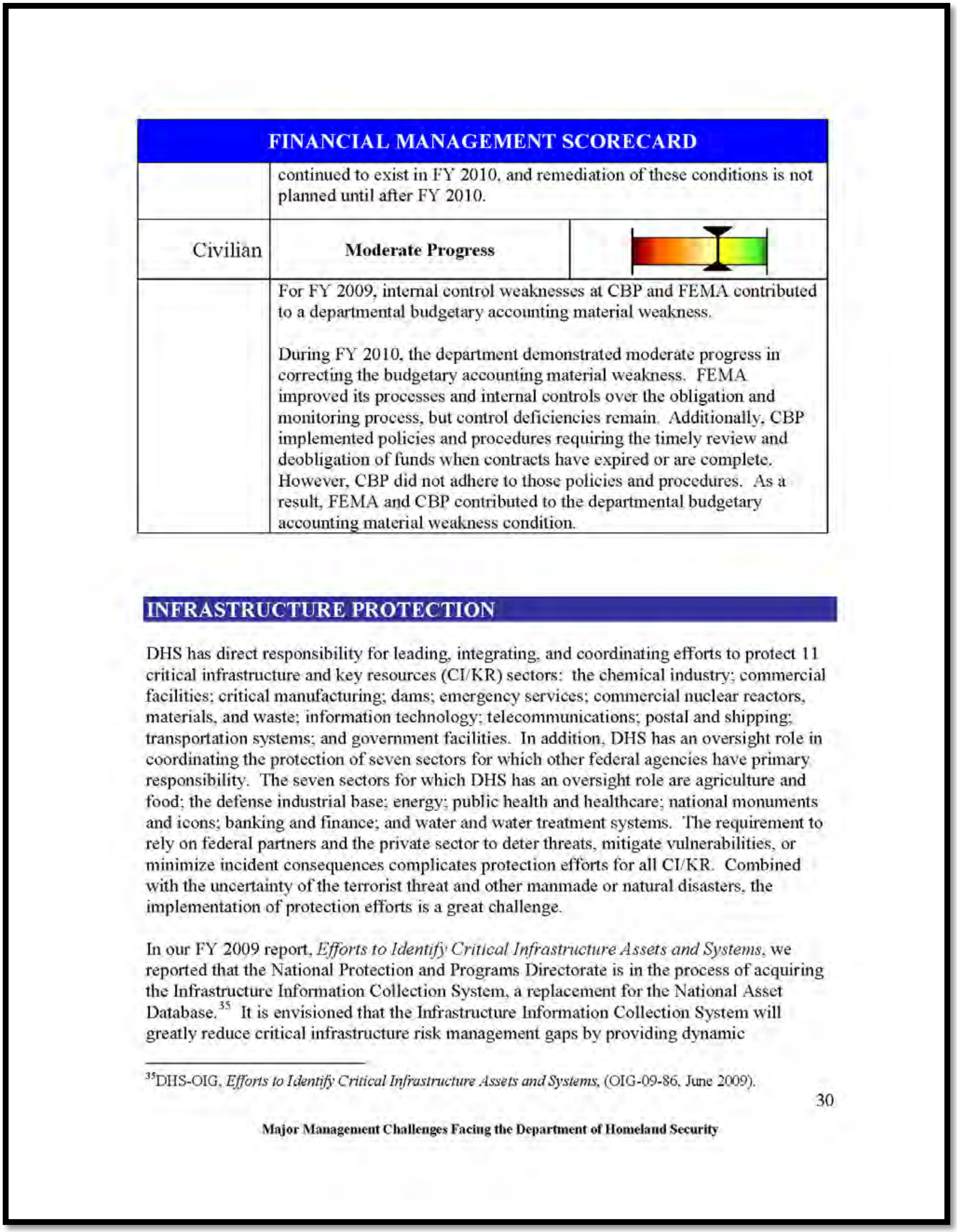
FINANCIAL MANAGEMENT SCORECARD		
	For FY 2010, the Coast Guard has demonstrated limited progress overall in correcting internal control weaknesses related to PP&E identified in the Independent Auditor's report in FY 2009. In addition to its planned FSTAR initiatives for FY 2010, the Coast Guard performed additional remediation efforts over discrete elements of its balance sheet. This "balance sheet strategy" was designed to achieve additional account balance assertions. As a result, the Coast Guard implemented additional measures to resolve the OM&S portion of the material weakness ahead of the planned FSTAR remediation milestone. However, the Coast Guard was unable to accomplish all aspects of its planned remediation efforts. Moreover, most of the corrective actions included in the FSTAR are scheduled to occur over a number of years. Consequently, many of the material weakness conditions noted during FY 2010 also existed in FY 2009. For example, one of the conditions the auditors identified, which is a repeat deficiency from prior years, is that the Coast Guard has not established its beginning PP&E balance necessary to prepare the fiscal year-end balance sheet. The Coast Guard conducted inventory procedures during FY 2010 to assist management in substantiating the existence and completeness of PP&E balances; however, those procedures were not performed over all asset classes (e.g real property). The Independent auditor also noted that the Coast Guard has had difficulty establishing its opening PP&E balances primarily because of poorly designed policies, procedures, and processes implemented more than a decade ago, combined with ineffective internal controls. PP&E was not properly tracked or accounted for many years preceding the Coast Guard's transfer to DHS in 2003, and now the Coast Guard is faced with the formidable challenge of performing a retroactive analysis in order to properly establish the existence, completeness, and accuracy of PP&E. Furthermore, the fixed asset module of the Coast Guard's CAS is not updated timely for effective tracking and reporting of PP&E on an ongoing basis. As a result, the Coast Guard is unable to accurately account for its PP&E, and provide necessary information to DHS OFM for consolidated financial statement purposes.	
Civilian	**Moderate Progress**	
	During FY 2009, CBP and TSA contributed to an overall material weakness in PP&E, while ICE, NPPD, TSA, and USCIS all had significant deficiencies in this area. During FY 2010, DHS demonstrated moderate progress overall in	



<table>
<tr><th colspan="3">FINANCIAL MANAGEMENT SCORECARD</th></tr>
<tr><td></td><td colspan="2">correcting internal control weaknesses related to PP&E identified in the Independent Auditor's report in FY 2009. ICE, NPPD, and USCIS have fully corrected internal control weakness conditions related to PP&E, while CBP reduced the severity of its control deficiencies. Additionally, TSA completed the reconciliation of its PP&E accounts in FY 2010 and was able to assert that its PP&E balances at September 30, 2010 are fairly stated in the DHS FY 2010 <i>Annual Financial Report.</i> Although TSA made some progress in remediating control deficiencies, including having auditable beginning PP&E balance, it was unable to fully address all of the conditions that existed in FY 2009. Consequently, the overall severity of its internal control weakness conditions remained in FY 2010.</td></tr>
<tr><td colspan="3"><b>Actuarial and Other Liabilities:</b> Liabilities represent the probable and measurable future outflow or other sacrifice of resources as a result of past transactions or events. The internal control weaknesses reported in this area are related to various types of liabilities, including accounts and grants payable, legal and actuarial, and environmental liabilities.</td></tr>
<tr><td>Military</td><td><b>Moderate Progress</b></td><td></td></tr>
<tr><td></td><td colspan="2">The Coast Guard maintains medical, pension, and post-employment travel benefit programs that require actuarial computations to record related liabilities for financial reporting purposes. Other liabilities include accounts payable, environmental, and legal liabilities.
In FY 2009, the Independent auditor noted a number of internal control deficiencies related to actuarial liabilities at the Coast Guard, which contributed to a material weakness for the department.
During FY 2010, the Coast Guard demonstrated moderate progress overall by completing its planned corrective actions over selected internal control and reporting deficiencies that existed in this process in FY 2009. Specifically, remediation efforts associated with accounts payable, accrued payroll, pension, and medical liabilities allowed management to assert to the completeness and accuracy of over $43 billion of accrued liabilities, which represents more than 50 percent of DHS' total liabilities. However, management was unable to provide sufficient evidential matter that support transactions and balances related to environmental and other liabilities. Among the conditions that remained throughout FY 2010 is the Coast Guard has not implemented effective policies, procedures, and controls to ensure the completeness and accuracy of environmental liabilities.</td></tr>
</table>



FINANCIAL MANAGEMENT SCORECARD		
Civilian	**Substantial Progress**	
	For FY 2009, the Independent auditor noted internal control weaknesses related to liabilities at FEMA and TSA. During FY 2010, the civilian components demonstrated substantial progress overall in remediating internal control weaknesses related to actuarial and other liabilities, with TSA fully remediating its control weakness condition. FEMA is recognized as the primary grant-making component of DHS and the FY 2010 Independent Auditor's report noted that FEMA does not have sufficient policies and procedures in place to fully comply with the *Single Audit Act Amendments of 1996* and OMB Circular No. A-133, *Audits of States, Local Governments, and Non-profit Organizations*. As a result, FEMA continued in FY 2010 to contribute to the departmental actuarial and other liabilities material weakness condition.	
Budgetary Accounting: Budgetary accounts are a category of general ledger accounts where transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources are recorded.		
Military	**Limited Progress**	
	The Coast Guard has over 90 Treasury Account Fund Symbol (TAFS) covering a broad spectrum of budget authority, including annual, multi-year, and no-year appropriations; and several revolving, special, and trust funds. Each TAFS with separate budgetary accounts must be maintained in accordance with OMB and Treasury guidance. In FY 2009, the Independent auditor noted a number of internal control deficiencies related to budgetary accounts that contributed to a material weakness in this area for the department. For FY 2010, the Coast Guard has made limited progress in remediating the internal control weaknesses in this area. Many of the conditions that contributed to a material weakness in budgetary accounting at the Coast Guard in FY 2009 remained throughout FY 2010. For example, the FY 2009 Independent Auditors' report 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 recorded amounts are complete, valid, accurate, and proper approvals and supporting documentation are maintained. These weaknesses	



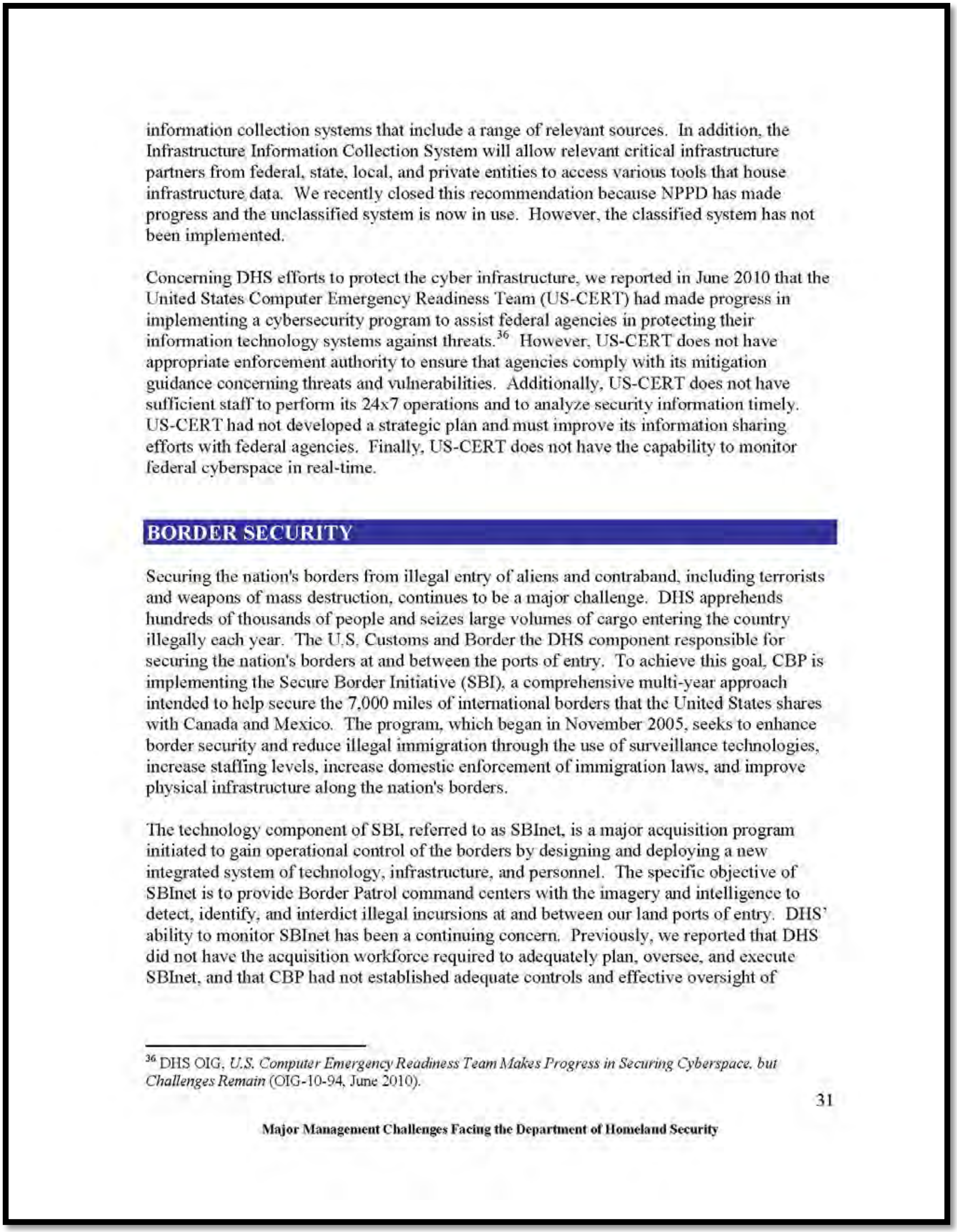
FINANCIAL MANAGEMENT SCORECARD		
	continued to exist in FY 2010, and remediation of these conditions is not planned until after FY 2010.	
Civilian	**Moderate Progress**	
	For FY 2009, internal control weaknesses at CBP and FEMA contributed to a departmental budgetary accounting material weakness. During FY 2010, the department demonstrated moderate progress in correcting the budgetary accounting material weakness. FEMA improved its processes and internal controls over the obligation and monitoring process, but control deficiencies remain. Additionally, CBP implemented policies and procedures requiring the timely review and deobligation of funds when contracts have expired or are complete. However, CBP did not adhere to those policies and procedures. As a result, FEMA and CBP contributed to the departmental budgetary accounting material weakness condition.	

INFRASTRUCTURE PROTECTION

DHS has direct responsibility for leading, integrating, and coordinating efforts to protect 11 critical infrastructure and key resources (CI/KR) sectors: the chemical industry; commercial facilities; critical manufacturing; dams; emergency services; commercial nuclear reactors, materials, and waste; information technology; telecommunications; postal and shipping; transportation systems; and government facilities. In addition, DHS has an oversight role in coordinating the protection of seven sectors for which other federal agencies have primary responsibility. The seven sectors for which DHS has an oversight role are agriculture and food; the defense industrial base; energy; public health and healthcare; national monuments and icons; banking and finance; and water and water treatment systems. The requirement to rely on federal partners and the private sector to deter threats, mitigate vulnerabilities, or minimize incident consequences complicates protection efforts for all CI/KR. Combined with the uncertainty of the terrorist threat and other manmade or natural disasters, the implementation of protection efforts is a great challenge.

In our FY 2009 report, *Efforts to Identify Critical Infrastructure Assets and Systems*, we reported that the National Protection and Programs Directorate is in the process of acquiring the Infrastructure Information Collection System, a replacement for the National Asset Database.[35] It is envisioned that the Infrastructure Information Collection System will greatly reduce critical infrastructure risk management gaps by providing dynamic

[35] DHS-OIG, *Efforts to Identify Critical Infrastructure Assets and Systems*, (OIG-09-86, June 2009).



information collection systems that include a range of relevant sources. In addition, the Infrastructure Information Collection System will allow relevant critical infrastructure partners from federal, state, local, and private entities to access various tools that house infrastructure data. We recently closed this recommendation because NPPD has made progress and the unclassified system is now in use. However, the classified system has not been implemented.

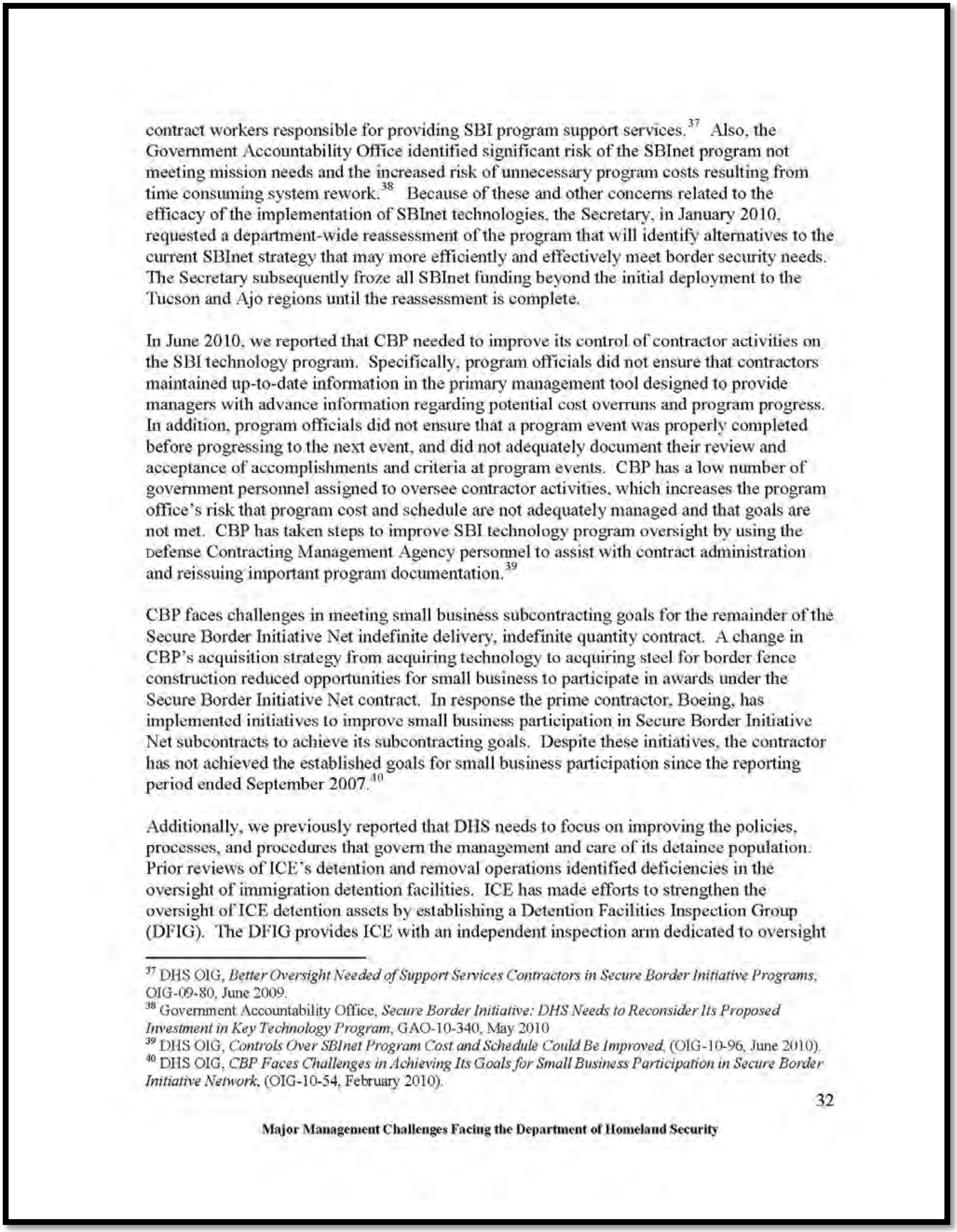
Concerning DHS efforts to protect the cyber infrastructure, we reported in June 2010 that the United States Computer Emergency Readiness Team (US-CERT) had made progress in implementing a cybersecurity program to assist federal agencies in protecting their information technology systems against threats.[36] However, US-CERT does not have appropriate enforcement authority to ensure that agencies comply with its mitigation guidance concerning threats and vulnerabilities. Additionally, US-CERT does not have sufficient staff to perform its 24x7 operations and to analyze security information timely. US-CERT had not developed a strategic plan and must improve its information sharing efforts with federal agencies. Finally, US-CERT does not have the capability to monitor federal cyberspace in real-time.

BORDER SECURITY

Securing the nation's borders from illegal entry of aliens and contraband, including terrorists and weapons of mass destruction, continues to be a major challenge. DHS apprehends hundreds of thousands of people and seizes large volumes of cargo entering the country illegally each year. The U.S. Customs and Border the DHS component responsible for securing the nation's borders at and between the ports of entry. To achieve this goal, CBP is implementing the Secure Border Initiative (SBI), a comprehensive multi-year approach intended to help secure the 7,000 miles of international borders that the United States shares with Canada and Mexico. The program, which began in November 2005, seeks to enhance border security and reduce illegal immigration through the use of surveillance technologies, increase staffing levels, increase domestic enforcement of immigration laws, and improve physical infrastructure along the nation's borders.

The technology component of SBI, referred to as SBInet, is a major acquisition program initiated to gain operational control of the borders by designing and deploying a new integrated system of technology, infrastructure, and personnel. The specific objective of SBInet is to provide Border Patrol command centers with the imagery and intelligence to detect, identify, and interdict illegal incursions at and between our land ports of entry. DHS' ability to monitor SBInet has been a continuing concern. Previously, we reported that DHS did not have the acquisition workforce required to adequately plan, oversee, and execute SBInet, and that CBP had not established adequate controls and effective oversight of

[36] DHS OIG, *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain* (OIG-10-94, June 2010).



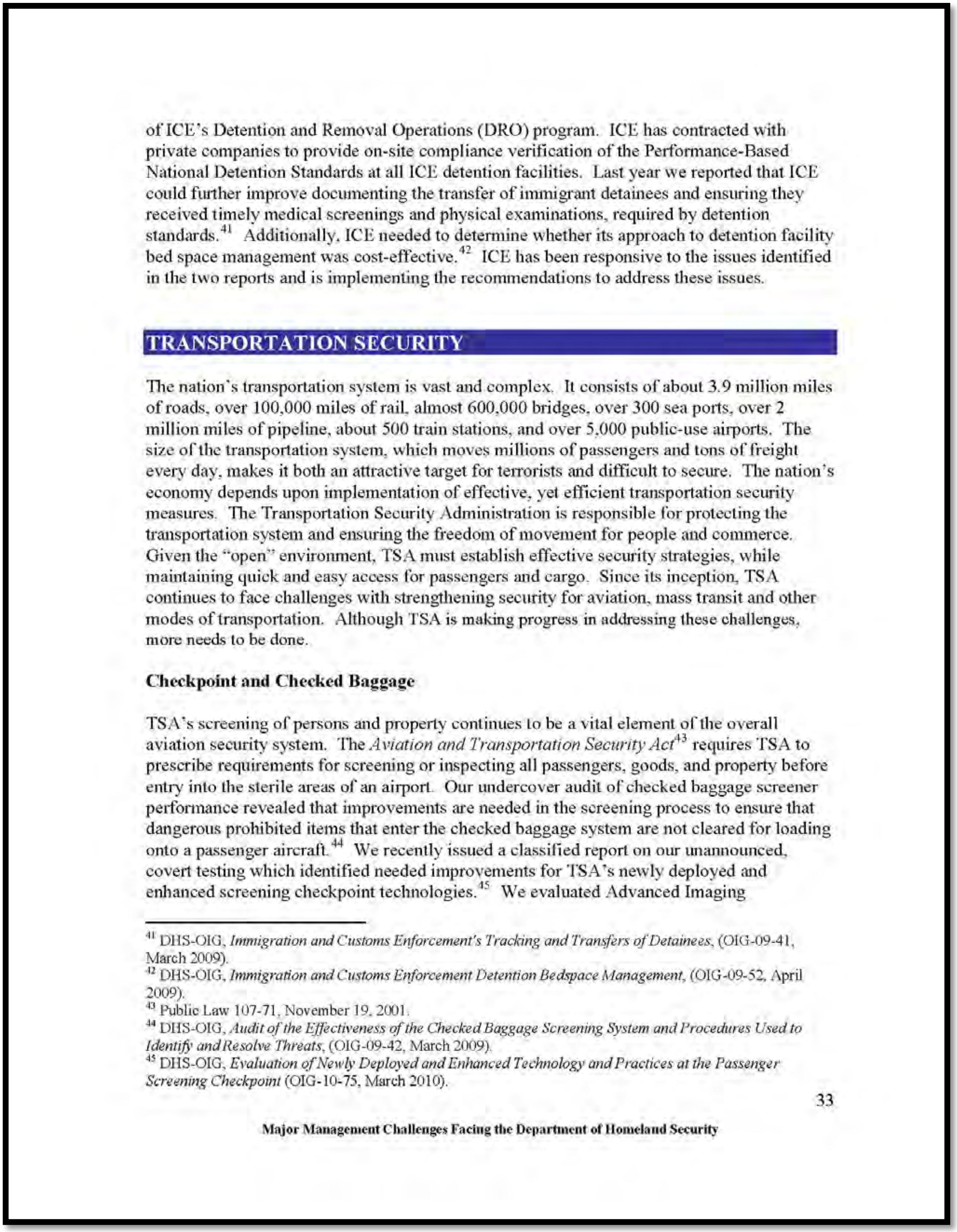
contract workers responsible for providing SBI program support services.[37] Also, the Government Accountability Office identified significant risk of the SBInet program not meeting mission needs and the increased risk of unnecessary program costs resulting from time consuming system rework.[38] Because of these and other concerns related to the efficacy of the implementation of SBInet technologies, the Secretary, in January 2010, requested a department-wide reassessment of the program that will identify alternatives to the current SBInet strategy that may more efficiently and effectively meet border security needs. The Secretary subsequently froze all SBInet funding beyond the initial deployment to the Tucson and Ajo regions until the reassessment is complete.

In June 2010, we reported that CBP needed to improve its control of contractor activities on the SBI technology program. Specifically, program officials did not ensure that contractors maintained up-to-date information in the primary management tool designed to provide managers with advance information regarding potential cost overruns and program progress. In addition, program officials did not ensure that a program event was properly completed before progressing to the next event, and did not adequately document their review and acceptance of accomplishments and criteria at program events. CBP has a low number of government personnel assigned to oversee contractor activities, which increases the program office's risk that program cost and schedule are not adequately managed and that goals are not met. CBP has taken steps to improve SBI technology program oversight by using the Defense Contracting Management Agency personnel to assist with contract administration and reissuing important program documentation.[39]

CBP faces challenges in meeting small business subcontracting goals for the remainder of the Secure Border Initiative Net indefinite delivery, indefinite quantity contract. A change in CBP's acquisition strategy from acquiring technology to acquiring steel for border fence construction reduced opportunities for small business to participate in awards under the Secure Border Initiative Net contract. In response the prime contractor, Boeing, has implemented initiatives to improve small business participation in Secure Border Initiative Net subcontracts to achieve its subcontracting goals. Despite these initiatives, the contractor has not achieved the established goals for small business participation since the reporting period ended September 2007.[40]

Additionally, we previously reported that DHS needs to focus on improving the policies, processes, and procedures that govern the management and care of its detainee population. Prior reviews of ICE's detention and removal operations identified deficiencies in the oversight of immigration detention facilities. ICE has made efforts to strengthen the oversight of ICE detention assets by establishing a Detention Facilities Inspection Group (DFIG). The DFIG provides ICE with an independent inspection arm dedicated to oversight

[37] DHS OIG, *Better Oversight Needed of Support Services Contractors in Secure Border Initiative Programs*, OIG-09-80, June 2009.
[38] Government Accountability Office, *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340, May 2010
[39] DHS OIG, *Controls Over SBInet Program Cost and Schedule Could Be Improved*, (OIG-10-96, June 2010).
[40] DHS OIG, *CBP Faces Challenges in Achieving Its Goals for Small Business Participation in Secure Border Initiative Network*, (OIG-10-54, February 2010).



of ICE's Detention and Removal Operations (DRO) program. ICE has contracted with private companies to provide on-site compliance verification of the Performance-Based National Detention Standards at all ICE detention facilities. Last year we reported that ICE could further improve documenting the transfer of immigrant detainees and ensuring they received timely medical screenings and physical examinations, required by detention standards.[41] Additionally, ICE needed to determine whether its approach to detention facility bed space management was cost-effective.[42] ICE has been responsive to the issues identified in the two reports and is implementing the recommendations to address these issues.

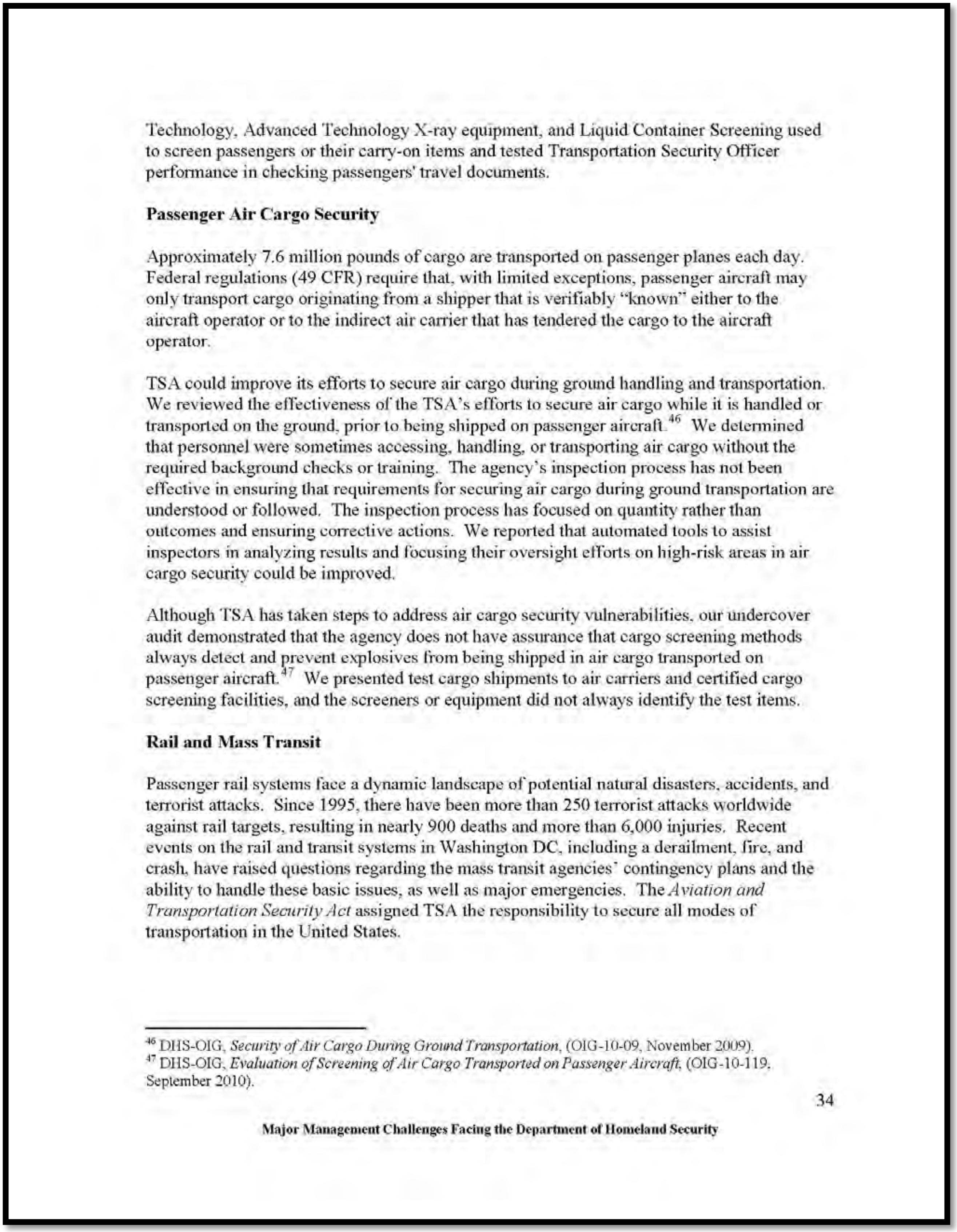
TRANSPORTATION SECURITY

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

Checkpoint and Checked Baggage

TSA's screening of persons and property continues to be a vital element of the overall aviation security system. The *Aviation and Transportation Security Act*[43] requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into the sterile areas of an airport. Our undercover audit of checked baggage screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items that enter the checked baggage system are not cleared for loading onto a passenger aircraft.[44] We recently issued a classified report on our unannounced, covert testing which identified needed improvements for TSA's newly deployed and enhanced screening checkpoint technologies.[45] We evaluated Advanced Imaging

[41] DHS-OIG, *Immigration and Customs Enforcement's Tracking and Transfers of Detainees*, (OIG-09-41, March 2009).
[42] DHS-OIG, *Immigration and Customs Enforcement Detention Bedspace Management*, (OIG-09-52, April 2009).
[43] Public Law 107-71, November 19, 2001.
[44] DHS-OIG, *Audit of the Effectiveness of the Checked Baggage Screening System and Procedures Used to Identify and Resolve Threats*, (OIG-09-42, March 2009).
[45] DHS-OIG, *Evaluation of Newly Deployed and Enhanced Technology and Practices at the Passenger Screening Checkpoint* (OIG-10-75, March 2010).



Technology, Advanced Technology X-ray equipment, and Liquid Container Screening used to screen passengers or their carry-on items and tested Transportation Security Officer performance in checking passengers' travel documents.

Passenger Air Cargo Security

Approximately 7.6 million pounds of cargo are transported on passenger planes each day. Federal regulations (49 CFR) require that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably "known" either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator.

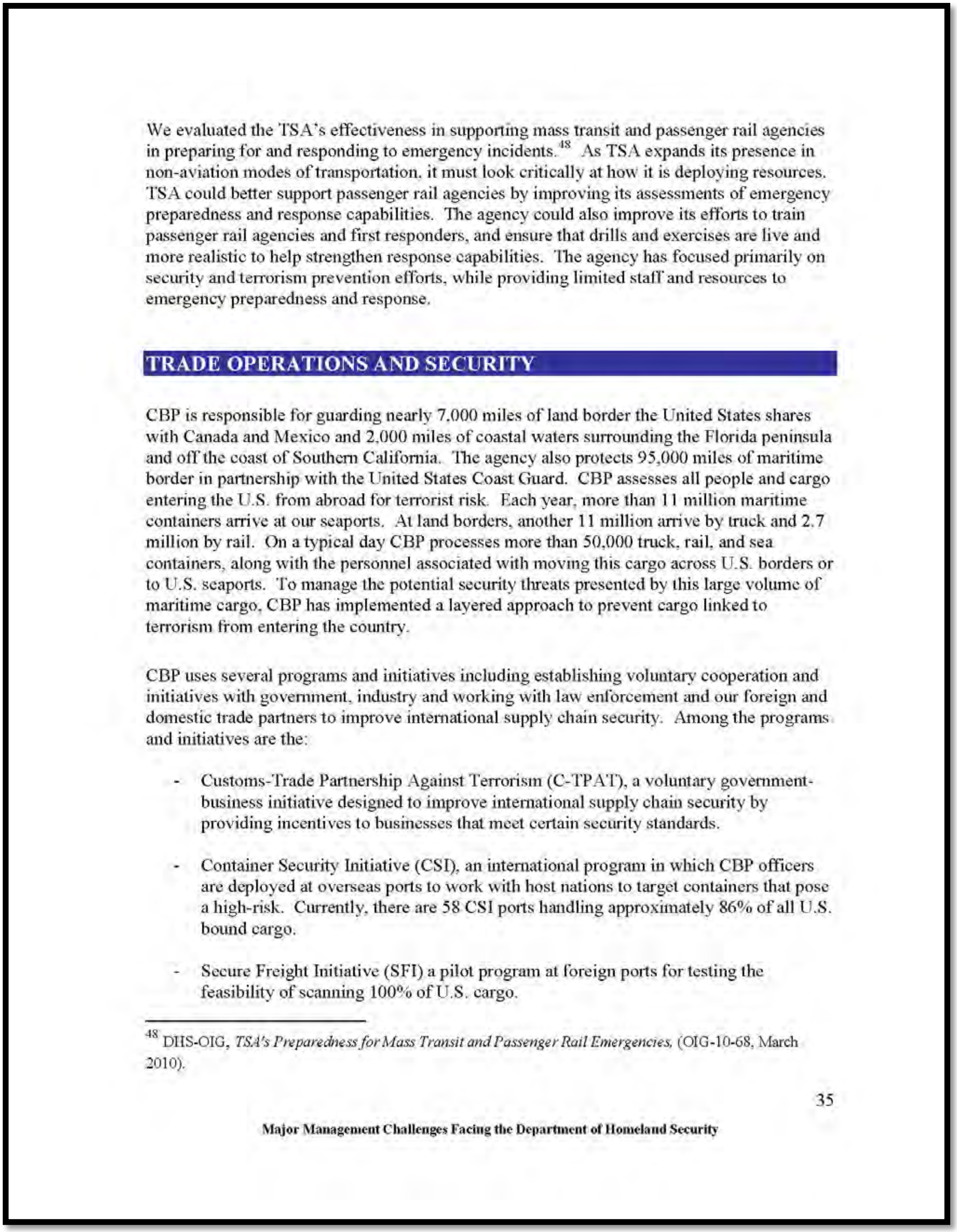
TSA could improve its efforts to secure air cargo during ground handling and transportation. We reviewed the effectiveness of the TSA's efforts to secure air cargo while it is handled or transported on the ground, prior to being shipped on passenger aircraft.[46] We determined that personnel were sometimes accessing, handling, or transporting air cargo without the required background checks or training. The agency's inspection process has not been effective in ensuring that requirements for securing air cargo during ground transportation are understood or followed. The inspection process has focused on quantity rather than outcomes and ensuring corrective actions. We reported that automated tools to assist inspectors in analyzing results and focusing their oversight efforts on high-risk areas in air cargo security could be improved.

Although TSA has taken steps to address air cargo security vulnerabilities, our undercover audit demonstrated that the agency does not have assurance that cargo screening methods always detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.[47] We presented test cargo shipments to air carriers and certified cargo screening facilities, and the screeners or equipment did not always identify the test items.

Rail and Mass Transit

Passenger rail systems face a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. Since 1995, there have been more than 250 terrorist attacks worldwide against rail targets, resulting in nearly 900 deaths and more than 6,000 injuries. Recent events on the rail and transit systems in Washington DC, including a derailment, fire, and crash, have raised questions regarding the mass transit agencies' contingency plans and the ability to handle these basic issues, as well as major emergencies. The *Aviation and Transportation Security Act* assigned TSA the responsibility to secure all modes of transportation in the United States.

[46] DHS-OIG, *Security of Air Cargo During Ground Transportation*, (OIG-10-09, November 2009).
[47] DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft*, (OIG-10-119, September 2010).



We evaluated the TSA's effectiveness in supporting mass transit and passenger rail agencies in preparing for and responding to emergency incidents.[48] As TSA expands its presence in non-aviation modes of transportation, it must look critically at how it is deploying resources. TSA could better support passenger rail agencies by improving its assessments of emergency preparedness and response capabilities. The agency could also improve its efforts to train passenger rail agencies and first responders, and ensure that drills and exercises are live and more realistic to help strengthen response capabilities. The agency has focused primarily on security and terrorism prevention efforts, while providing limited staff and resources to emergency preparedness and response.

TRADE OPERATIONS AND SECURITY

CBP is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard. CBP assesses all people and cargo entering the U.S. from abroad for terrorist risk. Each year, more than 11 million maritime containers arrive at our seaports. At land borders, another 11 million arrive by truck and 2.7 million by rail. On a typical day CBP processes more than 50,000 truck, rail, and sea containers, along with the personnel associated with moving this cargo across U.S. borders or to U.S. seaports. To manage the potential security threats presented by this large volume of maritime cargo, CBP has implemented a layered approach to prevent cargo linked to terrorism from entering the country.

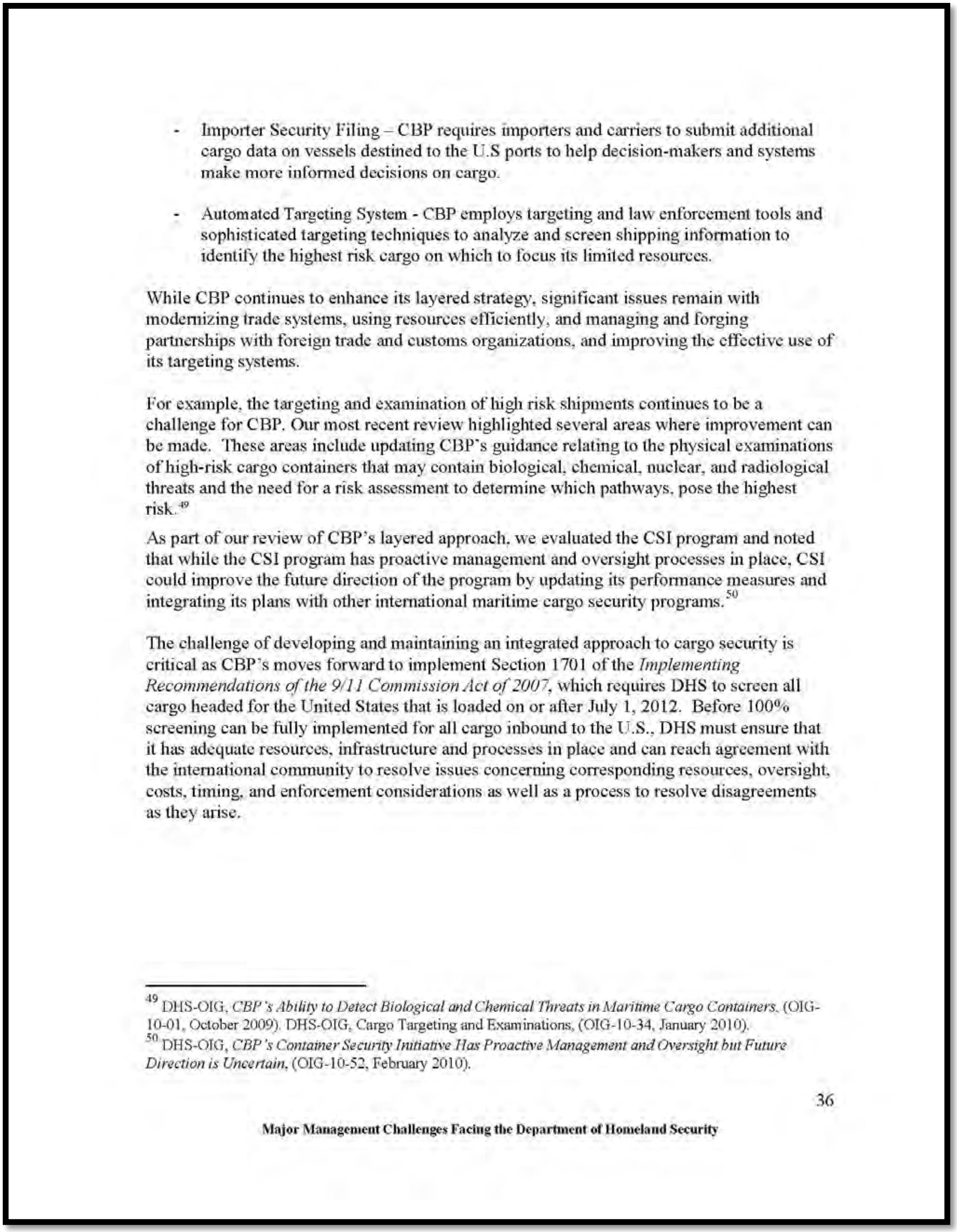
CBP uses several programs and initiatives including establishing voluntary cooperation and initiatives with government, industry and working with law enforcement and our foreign and domestic trade partners to improve international supply chain security. Among the programs and initiatives are the:

- Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary government-business initiative designed to improve international supply chain security by providing incentives to businesses that meet certain security standards.

- Container Security Initiative (CSI), an international program in which CBP officers are deployed at overseas ports to work with host nations to target containers that pose a high-risk. Currently, there are 58 CSI ports handling approximately 86% of all U.S. bound cargo.

- Secure Freight Initiative (SFI) a pilot program at foreign ports for testing the feasibility of scanning 100% of U.S. cargo.

[48] DHS-OIG, *TSA's Preparedness for Mass Transit and Passenger Rail Emergencies,* (OIG-10-68, March 2010).



- Importer Security Filing – CBP requires importers and carriers to submit additional cargo data on vessels destined to the U.S ports to help decision-makers and systems make more informed decisions on cargo.

- Automated Targeting System - CBP employs targeting and law enforcement tools and sophisticated targeting techniques to analyze and screen shipping information to identify the highest risk cargo on which to focus its limited resources.

While CBP continues to enhance its layered strategy, significant issues remain with modernizing trade systems, using resources efficiently, and managing and forging partnerships with foreign trade and customs organizations, and improving the effective use of its targeting systems.

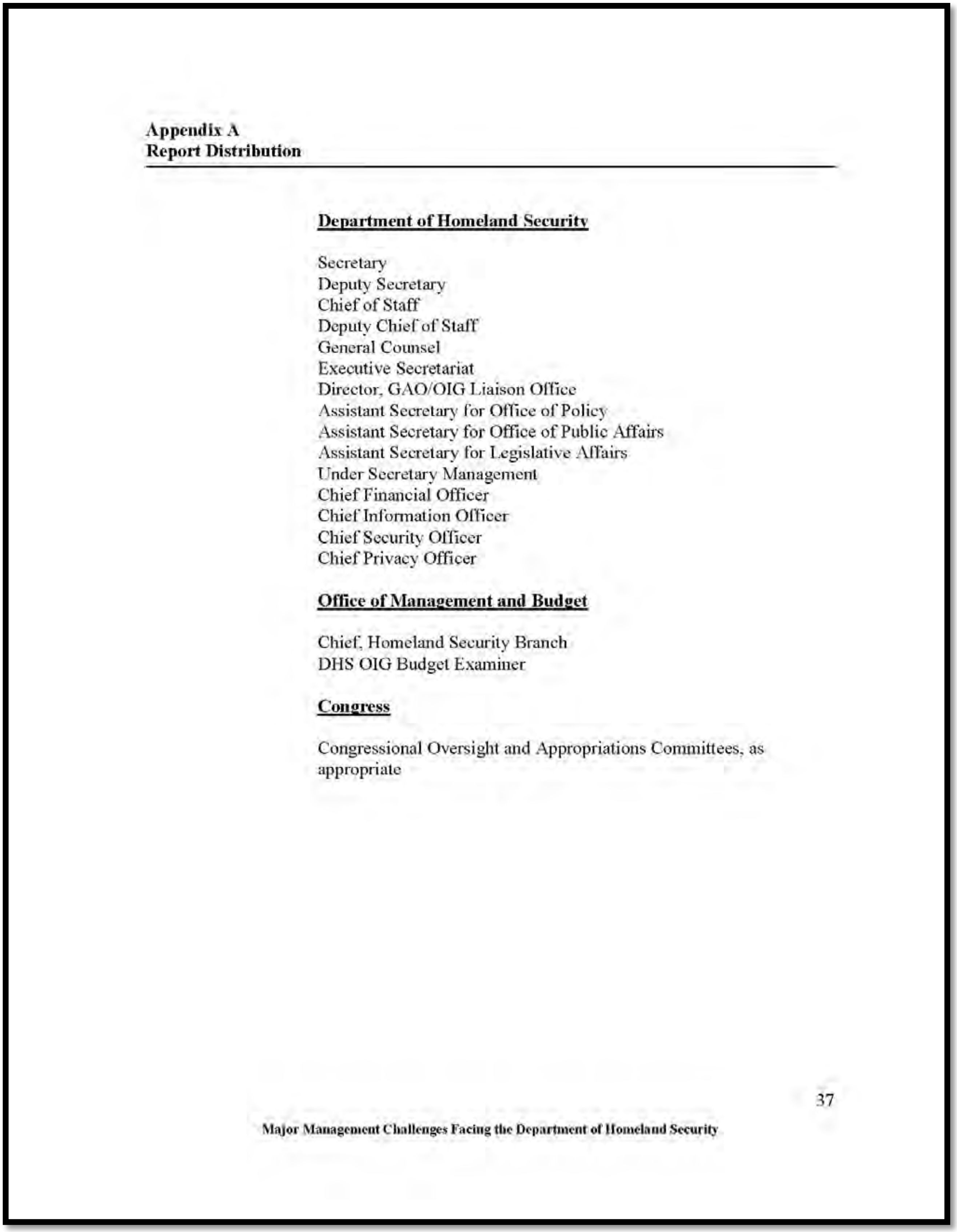
For example, the targeting and examination of high risk shipments continues to be a challenge for CBP. Our most recent review highlighted several areas where improvement can be made. These areas include updating CBP's guidance relating to the physical examinations of high-risk cargo containers that may contain biological, chemical, nuclear, and radiological threats and the need for a risk assessment to determine which pathways, pose the highest risk.[49]

As part of our review of CBP's layered approach, we evaluated the CSI program and noted that while the CSI program has proactive management and oversight processes in place, CSI could improve the future direction of the program by updating its performance measures and integrating its plans with other international maritime cargo security programs.[50]

The challenge of developing and maintaining an integrated approach to cargo security is critical as CBP's moves forward to implement Section 1701 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which requires DHS to screen all cargo headed for the United States that is loaded on or after July 1, 2012. Before 100% screening can be fully implemented for all cargo inbound to the U.S., DHS must ensure that it has adequate resources, infrastructure and processes in place and can reach agreement with the international community to resolve issues concerning corresponding resources, oversight, costs, timing, and enforcement considerations as well as a process to resolve disagreements as they arise.

[49] DHS-OIG, *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*, (OIG-10-01, October 2009). DHS-OIG, Cargo Targeting and Examinations, (OIG-10-34, January 2010).

[50] DHS-OIG, *CBP's Container Security Initiative Has Proactive Management and Oversight but Future Direction is Uncertain*, (OIG-10-52, February 2010).



Appendix A
Report Distribution

Department of Homeland Security

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

Office of Management and Budget

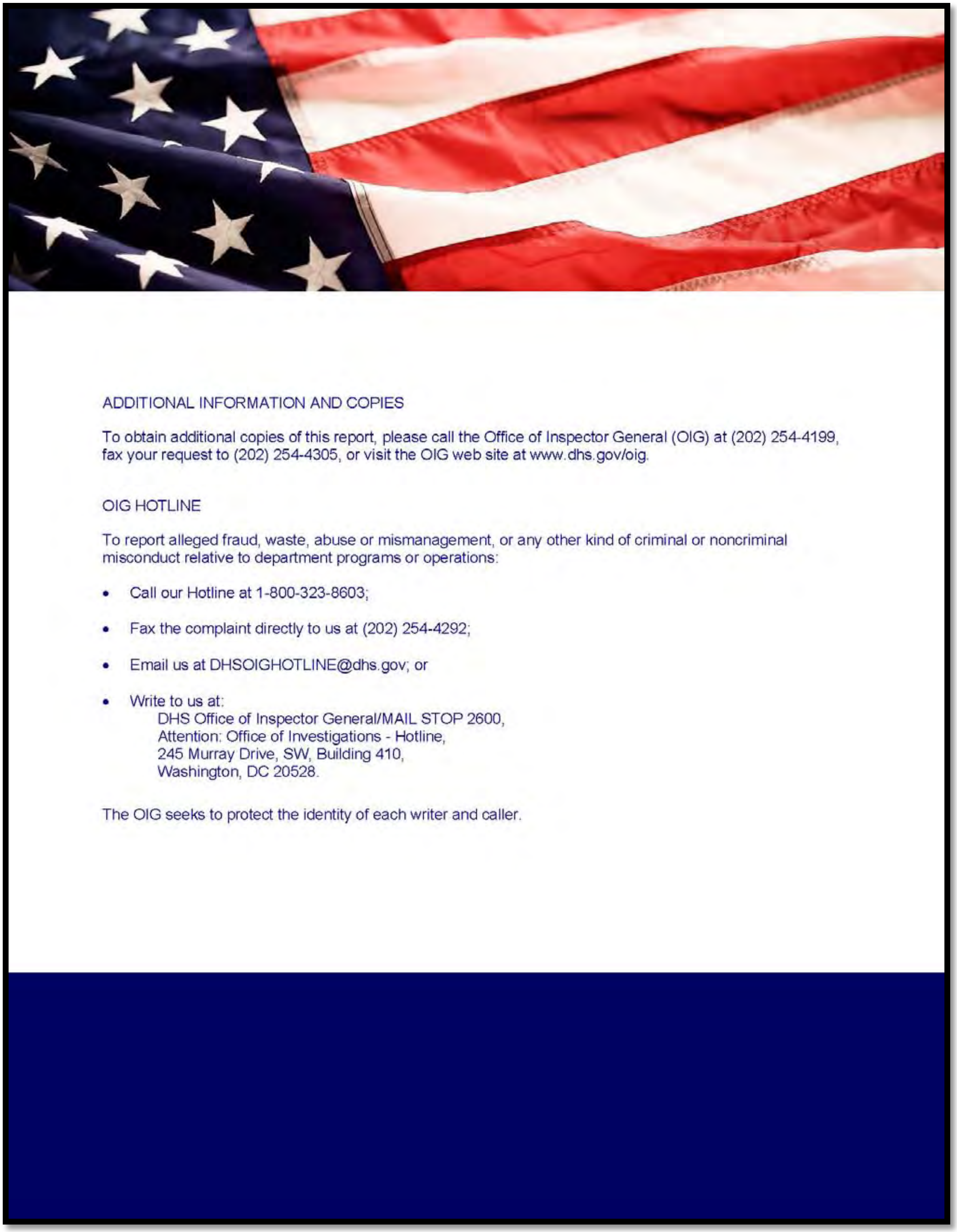
Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

37

Major Management Challenges Facing the Department of Homeland Security



ADDITIONAL INFORMATION AND COPIES

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

OIG HOTLINE

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

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

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

Management's Response

The Reports Consolidation Act of 2000 requires that, annually, the Office of Inspector General (OIG) prepare a statement summarizing the most serious management and performance challenges facing the Department and an assessment of the Department's progress in addressing those challenges. For FY 2010, the OIG considers the following to be the most serious challenges facing the Department:

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

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

The remainder of this section of the report details the Department's efforts in addressing each of the OIG challenges in FY 2010 and the plans it has in place to overcome the issues highlighted by the OIG.

Challenge #1: Acquisition Management

Acquisition Management

An effective acquisition management infrastructure is vital to achieving DHS's overall mission**.** It requires a sound management infrastructure to oversee the complex and large dollar procurements. A successful acquisition process depends on the following key factors: Organizational Alignment and Leadership; Policies and Processes; Acquisition Workforce; and Knowledge management and Information Systems.

Within the Office of the Chief Procurement Officer (OCPO), the acquisition workforce branch focuses on the numbers and skills of staff needed to carry out the functions of managing complex programs and effectively contracting for the products and services necessary to execute those programs and has been successful in building a responsive and skilled acquisition workforce.

Organizational Alignment and Leadership

According to the OIG, in both FY 2010 and FY 2009 DHS made "modest" progress in improving the acquisition program's organizational alignment and defining roles and responsibilities. This rating remains unchanged because the Department continues to depend on a system of dual accountability and collaboration between the Chief Procurement Officer and the Component heads, which may create ambiguity about who is accountable for acquisition decisions. However, DHS maintains that the dual authority model works because the OCPO retains central authority over all contracting through its contracting officer warrant program and Federal Acquisition Certification - Contracting program. According to the Department, the heads of contracting activities and contracting officers function independently of Component influence as their authority flows from OCPO rather than the Component. DHS's Acquisition Line of Business Integration and Management Directive sets forth existing authorities and relationships within individual Components and the Department's Chief Procurement Officer.

According to Government Accountability Office (GAO) report 09-29, DHS has not effectively implemented or adhered to its investment review process, which requires executive decision making at key points in an investment's life cycle. Findings in GAO-09-29 relate to a Management Directive (MD) that is no longer applicable. The report states "According to the Government Accountability Office (GAO), DHS has not effectively implemented or adhered to its investment review process, which requires executive decision making at key points in an investment's life cycle." This report was based on a GAO report completed in November 2008, which in turn was based on data from FY 2007. That report does not refer to the current guidance on acquisition management in MD 102.1; instead, addressed the MD 1400, which has been replaced by MD 102.1. The new, comprehensive Directive 102.1 was just implemented in draft form in November 2008 (FY 2009) and had not been reviewed in any fashion by the GAO in the report cited. Thus, use of that report to support the rating for 2010 is inappropriate and should be deleted from the draft report. DHS Acquisition Directive 102-01 was finalized and approved by the Undersecretary for Management on January 20, 2010.

FY 2010 Accomplishments

DHS OCPO drafted a Directive and Instruction which together are a complete revision of MD 0003, "Acquisition Line of Business Integration and Management." This establishes the accountability and responsibility that are critical to complementing the contracting authorities already in place. Together, the draft directive and instruction confirm the chain of contracting authority from the OCPO to the Heads of Contracting Activity (HCA), and then to the contracting officers. In addition, these documents stipulate the establishment of the DHS HCA Council, which supports the OCPO by providing senior officials with support and guidance on the state of contracting within the Department.

Directive 252-07, "Acquisition Line of Business Integration and Management." Directive 252-07 will:

- Clarify acquisition responsibilities of the Under Secretary for Management;
- Establish a programmatic line of authority via a "Component Acquisition Executive (CAE)"; and
- Clarify and delineate respective responsibilities of HCAs and CAEs.

Directive 102-01 sets forth the acquisition roles and responsibilities of Headquarters and Component personnel. It also defines program threshold levels, the decision authorities for those respective threshold levels and when a program needs to be reviewed. This acquisition management framework is also defined in context of the other key institutional management frameworks, such as strategic requirements determination and the Department's Planning, Programming, Budgeting, and Execution system. In this way, the acquisition management process is interlinked with the other key decision processes such that decisions in any one process are informed by knowledge gained by the others. This is an essential aspect of Department integration.

This year, the USM/Chief Acquisition Officer kicked off the first CAE Council meeting. The CAE is the senior acquisition official within a Component responsible for implementation, management, and oversight of their Component's acquisition processes, and coordinates those processes with the contracting and procurement processes of the Component's HCA. The HCA Council meets on a monthly basis to discuss key issues of concern to OCPO and/or the contracting activities. These meetings are a key ingredient in assuring a coordinated contract effort across DHS. In addition, each year OCPO issues priority letters to the HCAs that set forth their key goals for the upcoming year, including areas such as competition, small business, and Federal Procurement Data System (FPDS) accuracy and program management certifications.

Additionally, eight CAEs have been appointed in accordance with Directive 102-01, "Acquisition Management," to provide structure and accountability to the programmatic aspects of Acquisition. The establishment of the CAE structure will be further institutionalized when Directive 252-07 is approved and issued. Finally, additional directives and instructions are being established to provide further guidance and controls over the acquisition process.

The Acquisition Review Board (ARB) is the cross-Component board that assesses a program's progress and brings essential issues to the Acquisition Decision Authority. In FY 2010 DHS conducted 34 ARBs. These ARBs included Program Reviews and Program Decisions by the Acquisition Decision Authority, as well as, active oversight of Departmental *American Recovery and Reinvestment Act* (ARRA) initiatives.

To complement the ARB process, Component Portfolio Reviews were implemented in 2009 as a means for the Department to review and collaborate with each major program on an annual basis as well as gaining insight on the Components' acquisition oversight processes and staff. This process, jointly executed by the Component and the Department, supports management of the Component's acquisition portfolio and strengthens Departmental governance and oversight. DHS conducted 10 Portfolio Reviews in FY 2010.

Initiatives Underway and Planned

Building upon the 2010 and prior years' accomplishments and momentum, the OCPO will continue to improve organizational alignment and leadership in the following manner:

- Issuance and implementation of Directive 252-07, "Acquisition Line of Business Integration and Management."
- Conduct up to 36 ARBs in FY 2011. Plans are to also increase the number of Service Acquisition ARBs. Additionally, 10 Portfolio Reviews are planned.

- CAE Council meetings will be held as well as the designation of more CAE's throughout the Department where appropriate.

Policies and Processes

DHS made "moderate" progress in developing and strengthening acquisition management policies and processes. The Department has put a great deal of effort into improving its processes and controls over awarding, managing, and monitoring contract funds.

OCPO plans to amend the Homeland Security Acquisition Manual (HSAM) to require that acquisition personnel include Advanced Acquisition Plan (AAP) numbers in procurement files, when applicable.

As reported last year, DHS needs to further develop methods for evaluating the effectiveness of an award fee as a tool for improving contractor performance, and FEMA needs to accelerate its planned acquisition process improvements for awarding, managing, monitoring, tracking, and closing-out contracts.

FY 2010 Accomplishments

On August 23, 2010, OCPO issued an amendment to the HSAM Chapter 3007, Acquisition Planning, and the DHS Acquisition Planning Guide (HSAM Chapter 3007, Appendix H). Included in HSAM Notice 2010-08 was an amendment to HSAM 3007.103(d)(2)(i), which requires that a copy of each AAP and its reference number obtained through the AAP Database be included in the contract file as evidence of acquisition planning. The amendment to HSAM 3007.103(d)(2)(i) was effective upon issuance.

OCPO amended the HSAM 3016.401 to, among other things, require reporting from the Components of key information on each award fee and incentive contract that is awarded as well as reporting key information after the fact on the effectiveness of each award fee and performance incentive. These reports are to be used to evaluate the effectiveness of award fees and performance incentives and to develop best practices. We believe this will result in a process of continual improvement of DHS award fee and incentive contracting. OCPO issued supplemental guidance on June 10, 2010, detailing specific steps to be taken to ensure each award fee contract would be consistent with new Government-wide policy. We believe the combination of the amended Federal Acquisition Regulation (FAR) and the supplemental OCPO guidance, along with the training, will significant increase adherence to award fee policies.

OCPO's revised Acquisition Planning Guide (HSAM 3007, Appendix H, page H-20) requires acquisition planners, where appropriate, to describe "the type of incentive, the rationale for the selection of an incentive, and plans for managing the incentive contract (i.e., award fee plan)." Where appropriate, planners are also required to "discuss relevant agency data collected on award fees and incentive paid to contractors and include performance measures to evaluate such data to determine the effectiveness of award and incentive fees as a tool for improving contractor performance and achieving desired program outcomes (FAR 16.401(f))."

In addition to amending policies, OCPO has developed and launched Award Fee training for the Components. OCPO has also developed a two-hour award fee training course on the new FAR and

OCPO guidance. The course has been presented to DHS contracting personnel during FY 2010 and will continued to be offered in FY 2011.

To assure compliance with HSAM, Homeland Security Acquisition Regulation (HSAR), and Department of Defense (DOD) directives, OCPO performs program management and procurement management reviews. As previously noted, for program management, during FY 2010, there were 34 ARBs and 10 portfolio reviews performed. For procurement oversight, OCPO performed three Component specific reviews (OPO, ICE, and USSS), as well as seven DHS-wide reviews (Indefinite Delivery Indefinite Quantity (IDIQ) contracts, noncompetitive contracts, acquisition plans, contract pricing, time and material contracting, locating contract files, and firm fixed price level of effort contracts).

Initiatives Underway and Planned

Building upon the 2010 and prior years' accomplishments and momentum, the OCPO will continue to improve its policies and processes in the following manner:

- Continue to provide Award Fee training to DHS Components.
- Monitor reporting from the Components of key information on each award fee and incentive contract awarded to evaluate the effectiveness of award fees and performance incentives and develop best practices.
- In collaboration with the Office of General Counsel–Ethics, launch mandatory Procurement Ethics training for DHS acquisition workforce through a variety of mediums, e.g., on-site training, webinars.
- Maintain currency and accuracy of the HSAR and HSAM.
- Issue as an Appendix to HSAM 3015, a DHS Debriefing Guide to standardize processes within DHS as a means of strengthening DHS's commitment to transparency.
- Conduct up to 36 ARBs in FY 2011. Plans are to also increase the number of Service Acquisition ARBs. Additionally, ten Portfolio Reviews are planned.
- In addition to the oversight review on award fees, OCPO plans to conduct three Component specific reviews (CBP, USCG, and TSA), and at least four DHS-wide reviews (invoicing, interagency contracting, ARRA funds, and contract closeout).

Acquisition Workforce

Within OCPO, the acquisition workforce branch focuses on the numbers and skills of staff needed to carry out the functions of managing complex programs and effectively contracting for the products and services necessary to execute those programs. Achieving an effective acquisition workforce includes a corporate commitment to sound human capital management integrated with and aligned to organizational goals. Challenges DHS faces in this area are related to:

- A shortage of acquisition professionals to support the mission needs of the Department, creating a challenge for recruiting, developing, certifying and retaining a highly skilled workforce.
- Recruiting staff with the necessary skills for ensuring an effective acquisition program across multiple acquisition career fields.
- Identifying the appropriate number of acquisition personnel across Component contracting activities in a dynamic operational environment.

2010 Accomplishments

Common to the Federal Government, DHS has a shortage of trained and credentialed acquisition professionals. OCPO has made progress in building a skilled acquisition workforce in the following manner:

- We have continued the expansion of the Acquisition workforce office within the OCPO, providing staff and resources in recognition of the fact that workforce planning and management is critical to the success of the Department.
- Requested FY 2011 centralized funding to continue the acquisition intern program, known as the Acquisition Professional Career Program, to grow the DHS acquisition workforce by an additional 100 participants. In FY 2010 we successfully hired and placed 105 participants, culminating in a total of 200 participants in the program. Concurrently, we expanded from hiring for three acquisition disciplines (contracting, program management, systems engineering) to hiring for six acquisition disciplines, adding participants in logistics, business cost estimating, and information technology. Furthermore, we have begun the geographic expansion of the program to include hiring four participants for the U.S. Coast Guard in Norfolk, Virginia and recruiting for candidates to fill program requirements in Glynco, Georgia (for FLETC) and Mt. Weather, Virginia (for FEMA).
- Increased the size of the contracting/procurement workforce for a net gain of 76 contracting professionals from 1,326 in FY 2009 to 1,402 (as of 10/31/2010).
- Issued 843 Program Manager (PM) certifications (all levels) in FY 2010, increasing the total number of PM certifications to 2,486 (from program inception through FY 2010).
- Issued 1,933 Contracting Officers Technical Representative (COTR) certifications in FY 2010, increasing the total number of COTR certifications issued to 10,213 (from inception through FY 2010).
- In addition to the courses received from the Federal Acquisition Institute and the Defense Acquisition University, the DHS centralized acquisition training program provided 52 separate course titles, 300 course offerings, with 8,900 seats. Also completed the program management courseware for the three levels of PM certification in support of DHS policies and the PM professional competencies.
- Expanded the acquisition workforce by finalizing DHS certification programs for the following career fields: Test and Evaluation, Logistics, and Business Cost Estimating and Acquisition Financial Management.
- Developed the Department's first full acquisition human capital plan, providing a baseline for annual plans to help identify the recruitment, hiring, training, and certification needs of the acquisition workforce.
- FEMA has focused on ways to strengthen its acquisition workforce for catastrophic disasters and has developed two new specialized acquisition teams to focus on areas of critical need. FEMA proposed the establishment of a Disaster Acquisition Response Team (DART) and a Local Business Transition Team (LBTT) to offer critical support during disaster response efforts. To date, FEMA has established a unique structure that will allow these specialized teams to function as a national asset while being embedded in Regions IV, VI, and IX. In addition to these regions, the LBTT will also be present in Region V. The DART will focus on the administration and closeout of disaster contracts. The LBTT will focus on the implementation of Section 307 of the Robert T. Stafford Act, which addresses increased use of local vendors to satisfy contracting needs.

Initiatives Underway and Planned

Building upon the 2010 and prior years' accomplishments and momentum, the OCPO will continue to build a skilled acquisition workforce in the following manner:

- Requested FY 2011 centralized funding to continue to build the acquisition intern program, known as the Acquisition Professional Career Program, by 100 full-time equivalents for a cumulative total of 300 by the end of FY 2011.
- Assist the Component acquisition offices in filling existing vacancies through centralized, targeted recruitment efforts.
- Continue to increase the knowledge, skills and abilities and close the competency gaps of the acquisition workforce through training and development. The DHS centralized acquisition training program will provide 70 separate course titles, 325 course offerings, with 10,000 seats available for certification and recertification, professional career development, and continuous learning opportunities. These classes will be in addition to those received from the Federal Acquisition Institute and the Defense Acquisition University.
- Establish a DHS consolidated Training and Development Center for conducting certification and recertification, professional career development, and continuous learning classes.
- Build the courseware for the three levels of the Test and Evaluation (T&E) certification program in support of DHS policies and the T&E professional competencies.
- Expand the acquisition workforce by finalizing the DHS certification program for the systems engineering career field.

Knowledge Management and Information Systems

DHS made "modest" progress in deploying an enterprise acquisition information system and tracking key acquisition data, and is in the process of deploying a Department-wide (enterprise) contract management system that interfaces with the financial system. Many procurement offices continue to operate using legacy systems that do not interface with financial systems. With ten procurement offices and more than $17 billion in annual acquisitions and procurement, DHS needs a consolidated acquisition system to improve data integrity, reporting, performance measurement, and financial accountability. In FY 2009, of the $14.2 billion in contract awards reported to FPDS, the contract writing systems interfaced to financial systems accounted for 64 percent of the dollars awarded and 76 percent of the actions awarded. For the one contract writing system lacking a financial system interface, internal controls for reconciliation monitoring have been implemented.

Additionally, the Department has made moderate progress to improve the accuracy and completeness of contract data in Federal Procurement Data System – Next Generation (FPDS-NG). This system is the only consolidated information source for analyzing competition on procurements and is relied on for reporting to the public and Congress. This year, we reviewed the integrity of reported acquisition data in FPDS-NG and found that the system earned a 94.5 percent accuracy rate.

FY 2010 Accomplishments

DHS has implemented a quarterly operational report with automated dashboards that provide data on areas such as competition, small business, workforce certifications, late payments, protests, claims, and undefinitized contract actions.

DHS OCPO developed a Procurement Enterprise Reporting Application (ERA). ERA provides near real-time reporting, produces dashboards and quality control metrics and facilitates data analysis of DHS contract data down to individual contract line items. ERA is presently interfaced with FPDS and Enterprise PRISM.

The OCPO initiated a data integrity project that proactively checks FPDS-NG data for anomalies. Once anomalies are identified, Components are notified and they take corrective action. This effort is improving overall data integrity and has been implemented in addition to the FPDS annual certification by OCPO, and the FPDS training provided by OCPO to the Components during FY 2010.

DHS OCPO implemented the Enterprise Procurement Information Center (EPIC), a collaboration portal that facilitates document, task, calendar, announcement, and link management. EPIC also provides business process automation through custom workflows and provides team and project sites for collaboration and training.

The OCPO completed migration from the National Institute of Health's Contractor Performance System (CPS) to DOD's Contractor Performance Assessment Reporting System (CPARS). Over 4,800 Federal DHS personnel were trained on contractor performance policies and regulations and CPARS system navigation and use.

The OCPO initiated a data integrity project that proactively checks FPDS-NG data for anomalies. Once anomalies are identified, Components are notified and they take corrective action. This effort is improving overall data integrity and has been implemented in addition to the FPDS annual certification by OCPO, and the FPDS training provided by OCPO to the Components during FY 2010.

OCPO will continue to expand EPIC functionality; institute a contractor performance assessment reporting verification and validation process; support the Transformation and Systems Consolidation (TASC) effort; institute additional data integrity checks in the Enterprise PRISM contract writing system; and, further automate the quarterly operational report so that, rather than a quarterly report, all data is real-time for use by the contracting activities and OCPO to monitor key areas and take proactive corrective action where needed.

Initiatives Underway and Planned

The OCPO has the following initiatives planned or underway:

- FPDS-NG data integrity reports will be run more frequently in search of anomalies and automatic notification of errors will be emailed to Component points of contact.
- OCPO will continue to expand EPIC functionality.
- OCPO will institute a contractor performance assessment reporting verification and validation process.
- The DHS Chief Financial Officer has initiated TASC to acquire an integrated financial, acquisition, and asset management solution to DHS. The TASC program office is finalizing all planning documents according to the Acquisition MD 102-01. The original Life Cycle Cost Estimate is being refined and a staffing plan was developed and continues to be refined to include the certifications, qualifications, and work experience levels of all staff required

to manage a program of the size and complexity of TASC. OCPO will continue to support the TASC effort.

Challenge #2: Information Technology Management

DHS has completed many activities in FY 2010 to significantly reduce many of the major information technology (IT) management challenges in creating a unified IT infrastructure for effective integration and agency-wide management of IT assets. The challenge for the Chief Information Officer (CIO) will be to continually review and update these and other activities based on improved governance, new technologies, revised management practices and guidance pertaining to IT Security Controls, IT Infrastructure Integration, Privacy Concerns, and Budget Oversight/Capital Planning and Investment Control.

Information Security Controls

FY 2010 Accomplishments
The DHS Chief Information Security Officer (CISO) completed the FY 2010-2014 Information Security Strategic Plan. It outlines how the Department will continue to provide information security to support DHS's mission and objectives and articulates the goals for the next five years. The strategic plan was developed collectively with the DHS Components, and outlines the goals, objectives, priorities, and initiatives at the enterprise and the Component levels. The plan emphasizes the use of improved governance and communications to mature the DHS information security program into a cohesive, coordinated, Department-wide "Team Security" program. It expands beyond Federal Information Security Management Act (FISMA) compliance to embrace enterprise services and improved business processes for developing and delivering enterprise security for the Department's mission technology.

The DHS Information Security Program focuses on enterprise security and collaboration between information security functions at all DHS Components. The Security Program goes beyond just Headquarters and the Information Security Office, encompassing Component security programs through the DHS Chief Information Security Officer (CISO) Council, serving as the governing body. The CISO Council consists of the DHS Headquarters, National Security Systems and eight DHS Components (CBP, FEMA, FLETC, ICE, TSA, USCG, USCIS and USSS).

The DHS CISO has designated four DHS Strategic Goals. These four goals are strategically and operationally the most important to achieve the overall DHS information security mission in the near term. These are:

- Goal 1: Strengthen Information Security Governance Framework;
- Goal 2: Improve Compliance Activities;
- Goal 3: Embrace Enterprise Services; and
- Goal 4: Enhance Business Acumen and Resource Allocation.

The Department continued to show improvements in FISMA compliance for the 677 operational systems in use in the Department, particularly in the areas of security controls testing, Privacy, Plan-of-Action and Milestones (POA&M) management, and focused security operations.

DHS improved the Department's classified cyber threat information processing capability and improved overall analytical capability to understand and respond to sophisticated threats. The CISO conducted in-depth technical reviews of the Department's IT systems to assess quality assurance and validate compliance with DHS security requirements. Additionally, the CISO implemented weakness remediation plan for operations systems by focusing on POA&M management.

Initiatives Underway and Planned

In FY 2011, continued improvement in the Department's classified cyber threat information processing capability and analytical capability is planned, as well as conducting in-depth technical reviews of the Department's IT systems. Implementation of the Information Security Strategic Plan will continue and provide the Department a secure and trusted computing environment based on risk management principals to effectively share information.

IT Infrastructure Integration

FY 2010 Accomplishments

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 (backup) 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 (TIC) 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 (OneNet) and demonstrates significant progress towards OMB's Trusted Internet Connection goals. All Continental United States OneNet Wide Area Network Circuits were transitioned to Networx.

Initiatives Underway and Planned

The Department has the following initiatives planned or underway:

- In FY 2011, DHS will add new infrastructure capabilities and continue the consolidation to the DHS Enterprise Data Centers and OneNet. In June 2011, DHS will deploy Policy Enforcement Points as a way of ensuring Component security information requirements are maintained while migrating all the Components behind the TIC infrastructure. A High-Assurance Gateway will be used to handle exemptions needed to enforce a strict security policy. Consolidating Network Switching Nodes into the data centers and adding a reverse proxy capability as a means for protecting applications outside the TIC are also part of the FY 2011 plan for OneNet.
- Email infrastructure is also undergoing a major transformation as DHS creates two Enterprise Secure Message Gateways, one at each Enterprise Data Center, and

decommissions the single gateway currently servicing the DHS. The dual gateways will provide the necessary capacity and redundancy (backup) to ensure this important application serves the DHS customer needs for the foreseeable future. In FY 2011, DHS Components will begin migrating to the DHS Email as a Service (EaaS) offering. EaaS provides a cost-effective, scalable and fully redundant infrastructure capable of supporting the entire Department's email requirements.

- DHS Office of the Chief Information Officer (OCIO) will continue to upgrade and modernize key business applications, and establish a secure, utility computing environment for deploying mission and enterprise capabilities. This approach is consistent with private sector and OMB's direction to move toward cloud services to improve IT security and gain operational efficiencies.
- Additionally, DHS will continue to address Component disaster recovery capabilities within and between enterprise data centers.

Information Sharing with Partners

FY 2010 Accomplishments
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 (NIEM) 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.

Since FY 2008, DHS has been serving as the lead Program Management Office and Executive Director of the NIEM program for the U.S. Government and its state, local, tribal and private sector partners. As the current steward for the NIEM program office, DHS is deeply committed to the institutionalization of NIEM across the Department and with its international, state, local, tribal and private sector partners. DHS's significant growth in the utilization of standards and data sharing is consistent with the President's National Strategy for Information Sharing.

The Enterprise Data Management program continues to provide the architecture and governance for the understanding of data assets within and across the Department. This program supports the development of the Department-wide roadmap for data to improve mission effectiveness and efficiency, eliminating existing stovepipe data systems, and increasing interoperability and information sharing. Data architecture is the key governance tool to assure that mission needs drive technology investments. Additionally, through the use of data architecture practices Data Reference Model, the Enterprise Data Management Office (EDMO) is expected to recommend realignment of IT investments or acquisitions through the identification of targets at an estimated reduction of $10 million in annual IT costs by reducing the systems under maintenance, or driving common requirements for the development of centralized services.

EDMO's program plans integrate information sharing requirements and enable access across all levels of government, first responders, and stakeholders in the private sector through the use of the NIEM, a common vocabulary and process for the development of Information Exchanges such as the Nationwide Suspicious Activity Initiative Report standard. The development of these information exchanges requires collaboration with DHS Components and external partners and articulates clear business rules and user access guidelines that ensure secure information sharing.

Initiatives Underway and Planned

DHS will continue expansion and use of NIEM for data exchanges with state and local partners, and roll out a formal NIEM training curriculum to the Department to meet the needs of diverse stakeholders. Additionally, DHS plans to increase the rate of NIEM adoption to 90 percent for all new development in the major DHS IT Level 1 and 2 Programs.

Privacy Concerns

FY 2010 Accomplishments

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 CISO works closely with the Privacy Office to monitor the privacy requirements under the 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 (PIA) and/or System of Records Notice (SORN) records. The privacy metrics are designed to provide the status of completed PIAs or SORNs for those systems requiring such information. The metric is not applied to systems other than those designated by the Chief Privacy Officer as sensitive 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 PIAs on 26 percent of the IT systems that required PIAs and 66 percent of the IT systems were covered by a SORN. As of August 31, 2010, DHS improved its FISMA privacy numbers to 70 percent for PIAs and 94 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, 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.

The Privacy Office is also working with the Screening Coordination Office, Office of the CIO, Office of General Counsel and Intelligence and Analysis to conceptualize the framework requirements for a more secure and controlled Information Sharing Environment. This Information Sharing working group conducted assessments of SORNs for ten highly requested data sets as well as a series of fact finding interviews for the users of these same data sets in order to develop a set of policy and technology recommendations. These recommendations will help drive additional privacy and security controls for information sharing to DHS and external partners and provide input to the DHS Information Sharing Governance Board for continuing this effort and piloting a proof of concept for the Controlled Homeland Security Information Environment.

Accessibility Concerns
Ensuring that employees and customers with disabilities have equal access to information and data is important to meeting the DHS mission. Integration of Section 508 compliance into IT governance activities and decision-making processes is the key strategy DHS is currently using to ensure that moving forward, all IT systems are, in fact, accessible according to the Section 508 Electronic and Information Technology Standards.

Accessibility is also being integrated into the FISMA processes so that a full compliance picture can be developed. Additionally, quarterly Web compliance reporting, standardized accessibility testing procedures, associated educational products, and subject matter expert technical assistance services have been implemented to guide all information and data-related products towards full Section 508 compliance.

Initiatives Underway and Planned
In FY 2010, DHS plans to continue efforts to ensure electronic information and data are fully accessible to members of the public and employees with disabilities by developing an enterprise-wide tracking system for accessibility-related activities and information. DHS will continue efforts to define additional privacy and security controls for improved information sharing for DHS and external partners to highly requested DHS data sets.

Additionally, in FY 2011 DHS plans to assist the Program Manager for the Information Sharing Environment with the development of a NIEM-based functional standards for the process of automating and standardizing Request-for-Information/Request-for-Action) as well as the identification of Privacy Attributes for Personally Identifiable Information within NIEM.

Budget Oversight/Capital Planning and Investment Control

FY 2010 Accomplishments
In FY 2010, DHS developed NIEM information exchanges for the OMB E-Government IT Dashboard to standardize Capital Planning and Investment Control data elements across Federal agencies. In FY 2010, DHS delivered to OMB NIEM exchanges for agency Exhibit 53 and Tech Stat submissions.

At the request of Deputy Secretary Lute, the DHS CIO initiated a Department-wide Portfolio Review of all major IT investments to support the FY 2012-2016 Program Budget Review. To promote effective alignment of IT resources, it is critical that the Department evaluate IT resource allocation plans from a portfolio perspective. There are Department-wide, systemic challenges in effectively managing existing large IT programs, balancing investments in new capabilities against infrastructure, and effective reuse of IT systems and capabilities across Components. With a candid, transparent, and open dialog amongst Components, we can better ensure that the budget will deliver value for the resources expended while trimming costs, streamlining operations, eliminating duplication, and leverage capabilities across the enterprise.

A series of reviews was held concentrating on similar Component investments over the month of July 2010 to address portfolios of IT programs. Component leadership participated and articulated the mission effectiveness and status for each existing or planned program. As a result of these reviews, Resource Allocation Decision recommendations were provided to DHS leadership.

The IT Acquisition Review process has resulted in 444 IT acquisition requests and over $6.3 billion in requests being 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 2010 support the Quadrennial Homeland Security Review (QHSR), are consistent with the direction expressed in OCIO Strategic Plan for FYs 2009–2013 and align with DHS mission priorities.

OMB recently identified three DHS programs for the Federal-wide High Risk List. OCIO assisted the programs with developing their Remediation Plans. Since the launch of the OMB IT Dashboard in July 2009, DHS has been updating the milestones on a monthly basis, and is developing a process for periodic review by the CIO during FY 2011 for all major IT programs.

Initiatives Underway and Planned

The DHS OCIO is working to ensure E-Government initiative alignment to the DHS Segment Architecture Methodology, the Program Management Center of Excellence standards and best practices, and the Enterprise Portfolio Governance Structure. Additionally, DHS through stewardship of the NIEM Program Objective Memorandum, will deliver a new standardized NIEM-based information exchange that allows for all Federal agencies to deliver information on the OMB Exhibit 300 in an efficient and easy to use manner.

Challenge #3: Emergency Management

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

Disaster Sourcing: Develop and implement Single Point Ordering process

FY 2010 Accomplishments

The Single Point Ordering (SPO) concept was field-tested during the 2007 California fires; however, it has not yet been fully implemented with formalized, standardized processes throughout FEMA. SPO is defined as an agency-wide integrated process to centralize, manage and track resource orders for disaster supplies, equipment, personnel, teams and services. After several Focus Groups, FEMA conducted a three-day pilot Single Point Order Tracking (SPOT) Practitioner's Course during April 27–29, 2010. The class was made up of 20 students representing FEMA Joint Field Office positions such as Ordering Unit Leader, Logistics Section Chief, Mission Assignment Coordinator, Finance/Administration Section Chief, Human Resources Specialist, and a U.S. Army

Corps of Engineers (ESF #3) and Mass Care (ESF #6) representative. This resulted in refinement of SPOT business processes and a draft SPOT FEMA Directive (FD 145-2).

Initiatives Underway and Planned
The SPOT FEMA Directive 145-2 is currently in staffing. Subsequent to issuance of the SPOT Directive, a SPOT Operating Manual will be staffed and published providing more detailed business processes. These defined business processes will drive and refine the requirement for automated support.

Emergency Management – Housing

FY 2010 Accomplishments
FEMA restructured the Annual Disaster Housing Plan incorporating a new strategic direction. Now titled The Disaster Temporary Housing Operational Guide, the document describes FEMA's approach to working with Federal partners, states, territories, tribes, voluntary agencies, local communities, and individual disaster survivors to prepare for and respond to disaster-related sheltering and temporary housing needs. This guide is based on key concepts that are further defined in the *National Disaster Housing Strategy* and supersedes the 2009 Disaster Housing Plan and all previous Disaster Housing Plans.

FEMA awarded contracts to five manufacturers to produce Motor Homes (MHs) and Park Models (PMs) meeting FEMA's stringent specifications. The first task order was issued in November 2009 to meet the minimum order obligation of the Government. These IDIQ contracts are composed of five one-year options with a contractual ceiling to manufacture up to 135,000 MHs and PMs. These units can be either standard units or Uniform Federal Accessibility Standards (UFAS) compliant units to meet the diverse needs of the disability community.

In FY 2010, FEMA continued to identify and evaluate alternative housing units through the Joint Housing Solutions Group (JHSG). The group is comprised of housing and building science experts from FEMA, the U.S. Department of Housing and Urban Development (HUD), the DHS Office of Health Affairs, and private sector partners, including the National Institute of Building Sciences. The JHSG completed an initial assessment of numerous candidate alternative units, culminating in the award of two competitive contracts for nine different models (six units in 2009 and three units in 2010).

During FY 2010 FEMA continued to work closely with HUD to evaluate the effectiveness of the Disaster Housing Assistance Program pilot as an alternative to long term direct housing. This pilot program leverages the local public housing agencies to help displaced eligible applicants locate rental housing in and around the damaged communities.

Initiatives Underway and Planned
In FY 2010 JHSG completed a one year report on the first six units against four critical factors: timeliness, livability, range of use and cost. In 2011, JHSG will be evaluating and providing a report on the performance of the three most recent units. These efforts continue to provide valuable information on housing units and operations, critical for our ability to recommend housing unit and operations solutions.

Through the JHSG and Uniform Federal Accessibility Standards Units, FEMA will finalize review and analysis of the current projects and work to identify benefits of these programs to incorporate into FEMA's current procurement strategies. These efforts will support the timely delivery of temporary emergency housing to disaster survivors.

Mitigation: Develop integrated national hazard mitigation strategy

FY 2010 Accomplishments
The Federal Insurance and Mitigation Administration (FIMA) initiated steps to develop a Federal Insurance and Mitigation Strategic Plan.

Initiatives Underway and Planned
FIMA will utilize ongoing activities to develop a National Mitigation Strategy. These activities will include the National Emergency Management Association (NEMA) White Paper on Mitigation, the FIMA Strategic Plan and the results of the National Flood Insurance Program (NFIP) Reform workgroup.

The Federal Insurance and Mitigation Strategic Plan will be based on the following Strategic Direction:

- FIMA will effectively use science, technology, social media and communication programs to provide timely, accurate and relevant information in order to enhance the credibility of FIMA's work and mission. These strategies must reflect FEMA's core values of integrity, respect, compassion and fairness.
- FIMA will clearly communicate as we deliver on our mission to engage the public, the private sector, Government agencies, and our FEMA colleagues in understanding the natural hazard risks and strategies to buy down those risks.
- FIMA will holistically integrate sustainable hazard mitigation in the context of other community environmental and economic sustainability objectives, both pre and post disaster. By improving efforts to orient our programs towards community mitigation engagement in the management of future development decisions, FIMA will foster long-term mitigation strategies to reduce losses and assist communities and the nation in protecting from unnecessary future disaster impacts.

Improve local hazard mitigation planning process

FY 2010 Accomplishments
The *Disaster Mitigation Act of 2000* (Pub. L. 106-390) amended the Stafford Act to establish specific requirements for state and local hazard mitigation plans. Today, most states, major counties, and cities have active mitigation plans in place. During FY 2010, the FIMA, Risk Analysis Division, accomplished the following: (a) increased resources committed to mitigation planning through contractual assistance for plan reviews, training and technical assistance; (b) integrated mitigation planning into the RiskMAP life cycle to provide direct technical assistance to local communities engaged in new flood mapping activities; (c) focused on risk awareness as a communication and outreach goal of RiskMAP for mitigation planning; and (d) published *Hazard Mitigation: Integrating Best Practices into Planning* with the American Planning Association to provide guidance to local community planners on mitigation in local comprehensive plans. FIMA

is also developing an online training course to expand reach of mitigation planning training to the 19,000+ communities that are due to update their plans in the next few years.

Initiatives Underway and Planned
FIMA is revising the plan review process to ensure consistency in plan reviews and to focus approved mitigation plans on measurable mitigation strategies and implementation. FIMA is also initiating FY 2011 RiskMAP projects to include mitigation planning technical assistance direct to communities engaged in new flood risk studies. A plan is also underway to develop a new metric to measure actions that result from RiskMAP projects for communities with mitigation plans that identify flood risks.

Improve hazard mitigation outcomes

FY 2010 Accomplishments
State and local mitigation plans have demonstrated continuous improvement in mitigation programs through regularly scheduled updates. Almost 18,000 jurisdictions (66 percent of the Nation's population) currently have approved mitigation plans, and all States either have completed or are on target to complete plan updates, including nine States that currently have Enhanced Mitigation Plans that demonstrate a higher level of commitment to mitigation. FEMA has reconciled and clarified over 140 policy memos issued since the early 1990s, and integrated them into a streamlined guidance document that provides annual program guidance for the five hazard mitigation assistance programs.

Initiatives Underway and Planned
In FY 2011, FEMA will review its plan review process to ensure consistency in plan reviews and to focus approved mitigation plans on measurable mitigation strategies and implementation. Newly initiated FY 2011 RiskMAP projects will include mitigation planning technical assistance direct to communities engaged in new flood risk studies. RiskMAP also will monitor mitigation actions in communities with mitigation plans that identify flood risks.

FEMA is assisting NEMA to help advance the key recommendation described in its White Paper, which is to initiate a National Mitigation Alliance. This alliance will identify impediments and solutions to implementation of mitigation strategies at the state, tribal, and local levels. The Alliance will begin meeting in November 2010.

Challenge #4: Grants Management

FEMA assists communities in responding to and recovering from terrorist attacks and disasters. FEMA provides disaster assistance to communities through the Public Assistance Grant Program, the Hazard Mitigation Grant Program, and the Fire Management Assistance Grant Program. FEMA also awards grants to state and local governments; territories; tribal governments; and private, public, profit, and nonprofit organizations to enhance preparedness, protection, response, recovery, and mitigation capabilities throughout the Nation. The challenge for FEMA is to improve FEMA's grants management and oversight infrastructure to ensure effective monitoring of grantees.

FY 2010 Accomplishments

In FY 2010, the Grant Programs Directorate (GPD) took the following actions in the area of grants management, increasing emphasis on the effective monitoring of FEMA's grants recipients as well as its oversight structure:

- Launched the multi-year Programmatic Grants Monitoring Improvement Initiative in FY 2010 in an effort to expand and enhance programmatic monitoring capacity. The initiative has expanded both the breadth and depth of monitoring activities, as well as forming comprehensive plans for the future growth of grants monitoring at FEMA.
- Expanded monitoring activities from three to seven grants programs in spring 2010. The programs monitored include:
    - Homeland Security Grant Program;
    - Transit Security Grant Program;
    - Emergency Management Performance Grant Program (EMPG);
    - Port Security Grant Program;
    - Intercity Bus Security Grant Program Intercity Passenger Rail (IPR – Amtrak) and Freight Rail Security Grant Program; and
    - Trucking Security Program.

In the area of systems development, GPD's Non-Disaster (ND) Grants system is complete for functionality that supports application submission through award package creation. GPD has conducted targeted communication and outreach activities to key stakeholder groups. In conjunction with the OCIO, GPD researched other grants management systems and documented lessons learned. Stakeholder feedback was gathered via one-on-one interviews and focus groups to design a system that would be flexible, user-friendly, and have functionalities needed to effectively manage stakeholders' grant programs.

GPD is enhancing its oversight infrastructure as well through increased regional management of grant awards. FEMA regions are currently responsible for all programmatic and business management functions for the EMPG, Drivers' License Security Grant Program, Emergency Operations Centers (EOC) and Regional Catastrophic Grant Program grants from award to closeout. The regionalization of these grants has improved the grantee's ability to quickly implement projects related to these awards, as these grantees have long established relationships with the FEMA regions from their work in Mitigation and Disaster Response and Recovery. The regions have also been responsive to the grantee's immediate needs in regards to programmatic and budget approvals, grant extensions, the completion of Grant Adjustment Notices and Environmental and Historic Preservation (EHP) reviews.

Initiatives Underway and Planned

GPD's monitoring plans envision grants monitoring as a systematic year-round effort that spans the grants lifecycle, is applied to all preparedness grant programs in GPD's portfolio, and is fully coordinated among program, financial and other monitoring activities. Implemented by both FEMA Headquarters and Regions, the lifecycle approach efficiently extracts monitoring-related information from existing year-round grants management activities and uses it to supplement more traditional, episodic monitoring activities (e.g., monitoring site visits). Using this approach, the initiative has designed a standard set of monitoring activities that can be prioritized and implemented based on grantee and program need. Data collected through these monitoring activities is combined and centrally stored to create a comprehensive monitoring record that can be examined to proactively resolve common challenges experienced by grantees and to uncover opportunities to improve GPD's own administrative effectiveness and efficiency.

In fall 2010, monitoring will be introduced for the:

- Tribal Homeland Security Grant Program, and the
- EOC Grant Program.

Thus, within the next month, GPD will have monitoring protocols and content in place to monitor 68.12 percent of the total grant funding expended from FY 2006–2009, as well as the foundation for facilitated expansion of monitoring to additional programs. We look to continue expanding our monitoring efforts into FY 2011 and beyond.

GPD's programmatic monitoring data is currently collected in a centralized Access database application that allows for cohesion among and data analysis across grant programs. The centralized nature of the database also allows for facilitated data sharing and analysis of data over time. In fall 2010, the Grants Monitoring Improvement Initiative will also begin to transition monitoring data to a web-based environment that will allow for greater ease of use, more sophisticated analytics, and greater data coordination with other reporting efforts. When fully implemented, this approach will enable a nimble, cost-effective, and well-integrated grants information management strategy that will facilitate proper grants management practices, verify that grant funds are administered in accordance with the guidance issued to grantees, mitigate improper use of grant funds, and provide valuable information to GPD as it seeks to maximize the value and effectiveness of its preparedness grants portfolio.

The functionality offered within ND Grants will provide FEMA with a flexible system that can quickly adapt to changing business needs. ND Grants will accomplish the following:

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

GPD plans to expand upon the progress that is underway while continuing to improve our grants monitoring infrastructure. Actions planned include:

- Continued expansion of monitoring activity to another two to three preparedness grant programs.
- Alignment of monitoring data with GPD internal controls and performance metrics to provide for accurate, ongoing evaluation of monitoring performance.

- Working to incorporate the monitoring database into the Grants Reporting Tool, allowing for greater cohesiveness with other grant administrative processes and a more holistic information management system.
- Updating monitoring content and protocols for all currently monitored programs and working to monitor these programs against expanded requirements (e.g., (EHP)).

Challenge #5: Financial Management

FY 2010 Accomplishments

DHS has made significant progress improving internal controls over financial reporting. From FY 2005–2010, DHS has reduced the number of audit qualifications from 10 to 1 and Department-wide material weaknesses in internal controls over financial reporting by more than half. The number of Component conditions contributing to material weaknesses has gone from 25 to 9.

In FY 2010, DHS ended the practice of conducting stand-alone audits at the Components—except for CBP because of its significant revenue activities—and is focused on getting a qualified audit opinion on the Consolidated Balance Sheet by FY 2011. Component standalone audits at the Department served their purpose in successfully demonstrating that strong controls exist within the individual reporting entities of DHS Financial Management. Moving forward, there will be tremendous long-term value to standardizing processes DHS-wide, rather than building individual Component financial reporting capabilities, and in focusing our efforts on managing risk.

We still face challenges, but made significant progress in strengthening internal controls and implementing corrective actions within several key financial management areas. In FY 2010, the Department:

- Performed targeted risk assessments to identify weaknesses in accounting and financial reporting and developed and implemented Mission Action Plans for those high-risk areas. Monitoring of implementation and effectiveness is ongoing.
- Has made significant progress in ensuring controls are in place to prevent Antideficiency Act violations related to FY 2010 activity.
- Addressed financial management and business process challenges and shared best practices and lessons learned by identifying subject matter experts in critical risk areas and leveraging their expertise through cross-Component working groups. In addition, DHS updated its "Component Requirements Guide," which contains approximately 40 standard financial reporting processes.
- Analyzed the skill sets of essential financial management personnel and developed a plan to improve core competencies in key financial management areas.
- Substantially completed the Financial Management Policy Manual, which is designed to ensure DHS maintains efficient and transparent operations and our resources are not vulnerable to waste, fraud, and mismanagement.
- Provided training to all new employees in the DHS financial management community to develop a common set of core competencies, including the responsibilities of all financial managers to support and reinforce strong internal controls and the principles of fiscal law.

Components have worked hard to implement corrective actions and as a result have made good progress in key financial management and internal control areas.

- In FY 2010, the U.S. Coast Guard can assert to the following balance sheet items: Investments, Legal Liabilities, Actuarial Pension Liabilities, Actuarial Medical Liabilities, Operational Materials & Supplies (OM&S), and Fund Balance with Treasury – Payroll. Most significant, U.S. Coast Guard can assert to more than $43 billion in actuarial pension and medical liabilities. U.S. Coast Guard will continue to execute its strategic plan to assert to all balance sheet items in FY 2011, with a focus on Accounts Receivable, Accounts Payable, Environmental Liabilities, FBwT and PP&E. These assertions will better position the Department to obtain a qualified balance sheet opinion in FY 2011.
- USCIS, ICE, and NPPD corrected—and CBP reduced the severity of—deficiencies that contributed to the Department's PP&E and OM&S material weakness condition by implementing new policies, better processes, and strong internal controls. Additional personnel and new processes also helped CBP correct its deficiency condition in Financial Management and Reporting.
- New controls and processes helped TSA eliminate its audit qualification for PP&E and reduce the severity of its material weakness condition in Financial Reporting. TSA remediated three prior deficiency conditions by improving the control environment for IT Controls, Actuarial and Other Liabilities, and Other Entity Level Controls.
- FEMA reduced the severity of its deficiency condition in Financial Management and Reporting by improving the accuracy of key estimates, completing data cleanup, and improving data entry and field issues within the Integrated Financial Management Information System. FEMA also developed control procedures for Treasury Information Executive Repository and General Ledger reconciliations.

The Department is proud of these accomplishments and acknowledges the resolve and leadership of our financial management community. Over the years, Department-wide efforts provide case studies with five consistent critical success factors for accomplishing corrective action results:

- Engaged leadership that involves staff at all levels across business lines of the organization in internal control.
- Developing a good corrective action plan with clearly defined outcomes and a critical path to those outcomes.
- Availability of adequate resources for the successful execution of corrective actions.
- Consistent execution supported by disciplined project management.
- Confidence that corrective actions are credible due to the verification and validation of results through test of design and operational effectiveness.

Initiatives Underway and Planned

While we have made progress, we recognize that significant internal control challenges remain, largely at U.S. Coast Guard. The Department's Chief Financial Officer is actively engaged with senior management and staff at each Component, overseeing corrective actions to ensure continued progress across the Department.

DHS is committed to good stewardship of taxpayer dollars, and to demonstrating that commitment by obtaining an opinion on the Consolidated Balance Sheet. In support of that goal, the Department will:

- Work with the U.S. Coast Guard as it implements the corrective actions in the Financial Strategy for Transformation and Audit Readiness planned for FY 2011 and beyond.
- Continue targeted risk assessments to identify and remediate weaknesses in accounting and financial reporting.
- Implement a modernized financial management system and establish standard business processes to ensure DHS sustains its progress. Progress that relies on manual processes may not be sustainable without a modernized system. In the interim, DHS will continue to implement compensating controls designed to help ensure completeness, accuracy, authorization, and validity of financial transactions.

Challenge #6: Infrastructure Protection

DHS works closely with Federal partners and the private sector to deter threats, mitigate vulnerabilities, and minimize incident consequences for all Critical Infrastructure and Key Resources (CIKR).

Furthermore, the protection of the Nation’s cybersecurity has been identified by the OIG as a challenge that requires the development of a comprehensive strategy and management plan that identifies areas needing improvement and the development of a comprehensive information sharing and collection environment.

Infrastructure Protection

FY 2010 Accomplishments

The National Infrastructure Protection Plan (NIPP) CIKR Sector Partnership has facilitated the regular meeting and operation of inter-agency, inter-modal, inter-discipline sector, and cross-sector working groups to address issues such as cybersecurity, surface transportation security risk assessments, and electric-telecommunications interdependencies and incident coordination. Many of these activities have been organized through the Government Coordinating Councils (GCC), which represent inter-agency forums for identification of common or overlapping issues or programs that require coordination. An increase in meetings and updating of charters confirm the commitment to the Partnership and the value of programs and initiatives supported by the Partnership councils. The following accomplishments were seen in FY 2010:

- 611 sessions, including the GCC/Sector Coordinating Councils (SCC), Critical Infrastructure Partnership Advisory Council (CIPAC) Plenary, and working group meetings were held.
- Seven Councils (GCC/SCC) updated their charters.
- The CIPAC charter was renewed for another two years.
- The National Infrastructure Advisory Council charter was renewed for another two years.
- The Energy Sector completed a roadmap to identify and set NIPP implementation goals and priorities.

Increasing the reach of the partnership enables CIKR partnerships to become an interlocking, well-coordinated network of mutually supportive and sustainable relationships containing all key CIKR stakeholder elements. In the reporting period, the partnership:

- Enhanced communication, targeting specific disciplines such as State Homeland Security Advisors, State Emergency Management Directors, and State Critical Infrastructure Protection Managers to facilitate two-way collaboration on Infrastructure Protection (IP) mission issues of common interest.
- In collaboration with The Conference Board, issued "Protecting Critical Infrastructure: A Cross-Border Action Plan" (November 2009), which proposes a plan for Canada-U.S. collaboration. It recognizes that both countries have extensive plans in place for protecting CIKR and supports a plan at a regional, cross-border level that is aligned with the national plans.
- In partnership with Verizon Business, the U.S. Secret Service published a study focusing on data theft, security breaches, and cyber-crime trends. The report provides an easy to understand study, containing metrics and statistics that underscore critical IT security and general risk-mitigation information. The main objective of the study is to help expand the collective understanding of breaches and continue to augment advanced detection and prevention efforts. Its list of key recommendations and lessons learned from both Secret Service cases and Verizon cases, spans the spectrum of both public and private sectors, and is applicable anywhere in the world. This report was released to the public on July 28, 2010.

<u>Initiatives Under Way and Planned</u>
IP has instituted a major initiative to incorporate the CIKR Information Sharing Environment into the Nation's fusion centers, with the pilot completed in northern California in the first quarter of calendar year 2010. This dovetails with continued effort to increase the reach of the partnership to enable CIKR partnerships to become an interlocking, well-coordinated network of mutually supportive and sustainable relationships containing all key CIKR stakeholder elements. Part of the effort included the creation of and continued sponsoring of the CIKR Alliance Network that leverages trade associations and subject matter experts to enhance communication in the field and increase participation on Sector Partnership activities.

NPPD received the OIG draft report "Protective Security Advisor Program Efforts to Build Effective Critical Infrastructure Partnerships: Oil and Natural Gas Subsector" in mid-August. An initiative underway during the audit fieldwork creates new performance metrics based on established program goals and objectives aligned with IP, NPPD, and DHS goals and objectives as articulated in the DHS QHSR and Bottom-Up Review.

Understanding that the Protective Security Advisor (PSA) Program has grown and matured since its inception to become a focal point for IP activities and interaction with state, local, tribal, territorial and private sector partners, new metrics have been developed to better capture the program's impact on securing the Nation's critical infrastructure. The Protective Security Coordination Division, which operates the PSA Program, is using 180-day assessment follow-up interviews to capture data on how the PSAs, IP, NPPD and DHS as a whole are "buying down risk" for the Nation's critical infrastructure owners and operators, and demonstrating progress in protecting critical infrastructure. This implementation data is being used to develop qualitative metrics for the PSA Program that demonstrate how PSA activities contribute to PSA Program, IP, NPPD, and DHS critical infrastructure protection and resilience goals and objectives.

Cybersecurity and Communications

FY 2010 Accomplishments

Recently, the United States Computer Emergency Readiness Team (US-CERT) developed and began distributing to an initial set of agencies a Department and Agency Cybersecurity Activity Report that helps each agency understand its EINSTEIN 2 activity in the context of the larger, consolidated dataset of ongoing attacks and threats across the Federal Executive Branch civilian agency enterprise. EINSTEIN is the automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal Government to improve our Nation's situational awareness. Moreover, a product that summarizes Government-wide EINSTEIN 2-related activity and other cyber information across Federal Executive Branch civilian agencies was developed and its distribution to all partner agencies began on a weekly basis in August 2010. To better perform its operations, US-CERT increased its staff to 56 people with another 28 people selected and currently in the hiring pipeline (i.e. the security clearance and suitability process). Hiring actions also have been taken with respect to another 14 US-CERT positions.

Initiatives Under Way and Planned

US-CERT is preparing a strategic plan and developing corresponding performance measures. Additionally, US-CERT is developing a comprehensive performance management plan which builds on the strategic plan's performance measures to ensure accountability while identifying successes and areas for improvement. US-CERT began using an operational draft concept of operations and will update this document upon approval of the strategic plan, as US-CERT implements lessons learned during ongoing exercises and as the National Cybersecurity and Communications Integration Center reaches full operational capability. In addition, US-CERT is developing a comprehensive information sharing and collaboration environment as part of the EINSTEIN program to support continuous communications concerning cybersecurity vulnerabilities and indicators. This portal, which will incorporate direct input from partners and constituents, is slated to provide access to near real-time analysis reports derived from EINSTEIN 2 data, incident handling services, data analysis tools, and collaboration mechanisms (e.g. wiki services, instant messaging, and virtual meeting capabilities). A prototype was demonstrated at the Government Forum of Incident Response and Security Teams National Conference held in San Antonio, Texas August 15-20, 2010, which brings together technical and tactical practitioners of security response teams responsible for securing Government information technology systems. In addition to the comprehensive information sharing and collaboration environment, a cyber threat correlation tool is being implemented for US-CERT to improve its ability to provide agencies with actionable cyber vulnerability analysis.

Challenge #7: Border Security

Strengthening security at the border with additional personnel and resources

FY 2010 Accomplishments

DHS prevents and investigates illegal movements across our borders, including the smuggling of people, drugs, cash, and weapons. The Southwest Border Initiative, which began in March 2009 and continued through 2010, is a series of unprecedented steps to crack down on Mexican drug cartels by deploying additional personnel and technology, increasing information sharing, working closely with the Mexican government, and improving Federal coordination with state, local and tribal law enforcement authorities.

Over the past twenty one months, DHS has dedicated historic levels of personnel, technology, and resources to the Southwest border. Today, the Border Patrol is better staffed than at any time in its 86-year history, having nearly doubled the number of agents from approximately 10,000 in 2004 to more than 20,500 in 2010. ICE has increased the number of Federal agents deployed to the Southwest border from 3,034 in FY 2008 to approximately 3,300 in FY 2010, and currently has a quarter of all its personnel in the Southwest border region—the most ever. Since March 2009, DHS has doubled the number of personnel assigned to Border Enforcement Security Task Forces; increased the number of ICE intelligence analysts working along the Southwest border focused on cartel violence; quintupled deployments of Border Liaison Officers; and begun screening 100 percent of southbound rail shipments for illegal weapons, drugs, and cash – for the first time ever. DHS has also deployed additional canine teams trained to detect drugs and weapons and non-intrusive inspection technology that helps to identify anomalies in passenger vehicles at the Southwest border. Furthermore, DHS has completed 649 miles of fencing out of nearly 652 miles mandated by Congress, including 299 miles of vehicle barriers and 350 miles of pedestrian fence, with the remaining 3 miles scheduled to be complete by the end of the calendar year.

These initiatives and investments have yielded impressive results. Seizures of contraband along the Southwest border have increased across the board under the Obama administration and illegal crossings continue to decline. In fiscal years 2009 and 2010, CBP seized more than $104 million in southbound illegal currency—an increase of approximately $28 million compared to 2007–2008. Further, in fiscal years 2009 and 2010, CBP and ICE seized more than $282 million in illegal currency, more than 7 million pounds of drugs, and more than 6,800 weapons along the southwest border—increases of more than $73 million, more than 1 million pounds of drugs and more than 1,500 weapons compared to 2007-2008. Additionally, nationwide Border Patrol apprehensions of illegal aliens decreased from nearly 724,000 in FY2008 to approximately 463,000 in FY2010, a 36 percent reduction, indicating that fewer people are attempting to illegally cross the border. Moreover, in fiscal years 2009 and 2010, ICE made over 20,102 criminal arrests along the Southwest border, an increase of approximately 12 percent compared to 2007–2008. Over 12,857 of these arrests were of drug smugglers and over 2,562 of these arrests were of human smugglers.

Initiatives Underway and Planned

The passage and signing of Southwest border security supplemental legislation will provide DHS additional capabilities to secure the Southwest border at and between our ports of entry and reduce the illicit trafficking of people, drugs, currency and weapons. Specifically, this bill provides

$14 million for improved tactical communications systems along the Southwest border; $32 million for two additional CBP unmanned aircraft systems; $176 million for an additional 1,000 Border Patrol agents to be deployed between ports of entry; $68 million to hire 250 new CBP officers at ports of entry and to maintain 270 officers currently deployed to ports of entry; $80 million for 250 new ICE agents; and $6 million to construct two forward operating bases along the Southwest Border to improve coordination of border security activities.

Improving policies, processes, and procedures that govern the management/care of detainee population

FY 2010 Accomplishments
In August 2009, Secretary Napolitano and Assistant Secretary of Immigration and Customs Enforcement John Morton announced a major overall of the nation's immigration detention system—prioritizing health, safety and uniformity among detention facilities while ensuring security, efficiency and fiscal responsibility. Reform efforts through FY 2010 include initiatives to centralize contracts under ICE headquarters supervision; develop an assessment tool to identify aliens suitable for alternatives to detention; house non-criminal non-violent populations at facilities commensurate with risk; expand legal support services programs; devise and implement a medical classification system; launch a public, Internet-based detainee locator tool to assist attorneys, family members, and other relevant parties in locating detained individuals in ICE custody; and more than double the number of Federal personnel providing onsite oversight at the facilities where the majority of detainees are housed to ensure accountability and reduce reliance on contractors.

Initiatives Underway and Planned
ICE has drafted the Performance Based National Detention Standards 2010, which will enhance the Detention Reform initiative begun in 2009.

ICE is developing new approaches to bed space management. The ICE Detention Facility Map aligns bed location with arrest activity, population characteristics, driving distances to offices and airports, access to families, legal resources and consulates, and provides for a "right-sized" system. This effort has already enabled ICE to reduce the number of facilities used from 341 to 270.

ICE is piloting new classification instruments for both bed space and medical classifications. These efforts will augment other bed space reforms to permit ICE DRO to improve planning for new bed space. The new Intake Risk Assessment and Classification Tool began its pilot in the Baltimore and Washington Field Offices in May 2010.

Challenge #8: Transportation Security

TSA faces the challenge of establishing effective security strategies, while maintaining quick and easy access for passengers and cargo. The OIG recognized that a continuing challenge facing TSA involves strengthening security for aviation, mass transit, and other modes of transportation.

Passenger Air Cargo Security

FY 2010 Accomplishments
TSA achieved the 100 percent domestic cargo screening requirement for passenger planes in August 2010 and requires the screening of 100% of high-risk international inbound air cargo.

TSA is creating modules that will ensure consistency in training across regulated parties. The modules will include training covering the following areas:

- Acceptance and transfer procedures;
- Cargo screening procedures;
- Chain of custody measures;
- Facility security;
- Security coordinator training; and
- Handling of Sensitive Security Information and Personally Identifiable Information.

Each module will include instructor and student guides and tests. TSA finalized the modules in October 2010 and will post the materials for industry comment.

Training modules are currently under development and include chapters covering screening protocols and the use screening technology. This training will ensure a consistent, high level of improvised explosive device (IED) and anomaly recognition training for personnel conducting screening and will increase industry's compliance with screening protocol requirements in the Security Programs. Screening training modules will include:

- Cargo Screening;
- Roles and Responsibilities for Screening Cargo;
- Physical Search;
- IED Recognition;
- Advanced Technology X-ray;
- Explosives Trace Detection;
- Explosives Detection System; and
- Electronic Metal Detection.

TSA has established Special Emphasis Inspections (SEIs) to focus on areas such as air cargo access control and Security Threat Assessments (STA). For the second straight year, TSA has conducted Headquarters (HQ) directed SEIs on these areas with more than 200 STA-based SEIs conducted in FY 2010 than in FY 2009. Additional SEIs involving access control, cargo acceptance and the Indirect Air Carrier program are underway and have shown signs of improved compliance rates. Improved compliance rates in FY 2010 have been seen in the following areas:

- Access Control SEI compliance rate increased from 94% to 96.5% from FY 2009 to FY 2010;
- Cargo Acceptance SEI compliance rate increased from 98.5% to 99.1%;
- Indirect Air Carrier based SEI compliance rate improved 1%; and the
- Overall compliance rate for all SEIs improved from 95.8% to 97.9%.

TSA has taken significant efforts to improve the national oversight and inspection program. In FY 2010, TSA implemented a risk-based approach to inspections, which employs a process that denotes the air cargo compliance risk of each entity in the supply chain, so that inspections can be carried out in a manner which is geared at minimizing this risk. From FY 2010 Quarter 1 to Quarter 3, High Risk entities were diminished by 5.9 percent, Moderate Risk entities were diminished by 8.4 percent and Low Risk entities increased by 17.6 percent. The average risk score across all entities was decreased by 13.54 points. Over 25,000 risk-based inspections and tests were conducted across the system by mid-year FY 2010.

TSA has also worked to provide additional tools to Transportation Security Inspectors (TSIs) and TSA field management to better analyze work results and focus oversight efforts. Primarily, the HQ-issued risk scores analyze three years worth of data to present to the field a risk score that represents where the need to inspect exists.

TSA established the first ever TSA-CBP liaison to the CBP National Targeting Center for Cargo (NTC-C). TSA has established a permanent member of the CBP NTC-C who resides on the NTC-C floor and shares data, intelligence, analyses, testing, and inspection results as necessary.

TSA has increased its TSI training sessions from quarterly to monthly in FY 2010. These training sessions have been focusing on conducting high-quality cargo screening inspections. TSA has also developed and implemented an air cargo screening lab, based at the Security Enforcement Training Academy. This lab uses actual screening equipment and processes to put TSIs through real world practical exercises to hone skills necessary for conducting air cargo screening location inspections.

TSA is also developing a domestic air cargo screening assessment program, in which TSIs will conduct tests and assessments of cargo screening methods, practices, and personnel on a regular and recurring basis.

<u>Initiatives Underway and Planned</u>

TSA will educate industry on the use of the modules in fall 2010. The training modules will initially be released as voluntary in order to receive user feedback. After receiving industry comments, TSA intends to re-issue the materials as a mandatory TSA training program to be incorporated into the standard security programs.

TSA plans to continue the use of SEIs and to track the compliance rates.

TSA will continue its risk-based approach to inspections in FY 2011. TSA plans to implement additional risk scores for all cargo air carriers and aircraft operators. Compliance Dashboards will be enhanced.

Additional roles and integration of the NTC-C liaison will be explored to include joint training and enhanced interaction in TSA operations such as SEIs and Cargo Strikes.

TSA plans to initiate a pilot program for the air cargo screening assessment program in FY 2011. The Office of Security Operations (OSO) is already coordinating this effort with various TSA organizations and is leveraging already existing process and protocols to the extent possible from the Aviation Screening Assessment Program.

TSA is exploring the development of additional TSI training to include advanced air cargo screening oversight and air cargo risk profiling.

TSA is in the process of obtaining additional screening equipment for the cargo lab and developing a cargo screening inspection course.

Rail and Mass Transit

FY 2010 Accomplishments

In July 2010, Secretary Napolitano launched the first phase of DHS' nationwide "If You See Something, Say Something" campaign and announced a new national information-sharing partnership with Amtrak as part of the nationwide Suspicious Activity Reporting (SAR) initiative—highlighting the public's role in keeping our country safe and the Obama administration's commitment to bolstering surface transportation security.

The "If You See Something, Say Something" campaign—originally implemented by New York City's Metropolitan Transit Authority and funded, in part, by $13 million from DHS' Transit Security Grant Program—is a simple and effective program to raise public awareness of indicators of terrorism, crime and other threats and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities.

The campaign complements the national SAR initiative—a partnership among Federal, state, and local law enforcement to establish a standard process for law enforcement to identify and report suspicious incidents or activity and share that information nationally so it can be analyzed to identify broader trends. The partnership with Amtrak is a new national information-sharing partnership in which DHS and the Department of Justice (DOJ) work with Amtrak to utilize the latest intelligence in law enforcement trainings on how to identify suspicious behaviors associated with new and evolving threats. Amtrak officers will also utilize an upgraded reporting system—made available by the Transportation Security Administration—to refer suspicious activity reports to DHS and the Federal Bureau of Investigation for analysis and follow-up.

TSA has also been working with the DHS's Science and Technology sponsored Transportation Security - Centers of Excellence program in developing a course to better train Bus Operators in security awareness related areas, called BOARD for Bus Operator Awareness Research and Development project.

The Bomb Squad Response to Transportation Systems training and exercise program has been very active this fiscal year with mass transit related training events in Phoenix, Arizona; Oakland, California; Miami, Florida; National Capital Region/DC; and Norfolk, Virginia. Between 50 and 150 bomb technicians have been trained at each of these events.

The Mass Transit and Passenger Rail Security Division has planned, coordinated and executed the deployment of marine mammal systems (MMS) from the Space and Naval Warfare Systems Center Pacific, Biosciences Division (Code 715) to support the protection of underwater critical infrastructure in mass transit (Bay Area Rapid Transit, San Francisco Bay Region) during “Golden Guardian 2010,” a state-level exercise focused on terrorism in west coast ports. The underwater detection capability, via the MMS, was also identified as a potential capability to facilitate re-opening a port, post attack.

During FY 2010, the effectiveness of the TSA’s Surface Transportation Security Inspection Program (STSIP) was enhanced through implementation of the following programs, initiatives, and organizational changes:

- The TSA, through the STSIP, concluded its first full year of inspections of freight, passenger, and transit rail operators to determine compliance with rail security regulations issued in 2009, (49 Code of Federal Regulations (CFR) Part 1580). These were TSA’s first compliance inspections performed in rail. In FY 2010, the STSIP completed over 4,000 such inspections to determine industry compliance with these requirements.
- In FY 2010, TSA further enhanced the effectiveness of surface inspectors through providing additional training to surface inspectors on new programs and processes intended to enhance the effectiveness of the workforce. The STSIP conducted a national training conference for all TSI-Surface and their supervisors (Assistant Federal Security Director (AFSD-Is)/AFSD-Surface/Supervisory TSIs) to provide the workforce with the latest guidance and updates on security programs such as 49 CFR Part 1580, inspections, freight rail risk reduction surveys, and Baseline Assessment for Security Enhancement reviews in mass transit. TSA also continued to provide railroad operations training to other TSA field elements (including Federal Security Directors, Deputy Federal Security Directors, Federal Air Marshals, Special Agents in Charge, Assistants to the Special Agent in Charge, Area Directors, Deputy Area Directors, etc.), in order to increase agency-wide awareness and expertise on issues involving surface transportation security.
- In an effort to provide more direct oversight of the surface transportation security program, a realignment of personnel devoted to surface transportation was accomplished in January 2010. TSA created six Regional Security Inspectors in an effort to create uniformity among field reporting lines.
- In FY 2010, the STSIP continued the build out and expansion of surface related training at the Transportation Technology Center in Pueblo, Colorado. The STSIP also facilitated completion of modifications to classroom space and dedicated personnel to the site to develop the TSI-Surface curriculum and to deliver training material. This team is also responsible for the future expansion of the TSA space at the Pueblo site and the development of expanded training courses that will cross all surface modes of transportation.

<u>Initiatives Underway and Planned</u>

The BOARD program will be rolled out to the transit bus operator community over the next two years. This effort may also be expanded to include the Bus Dispatch/Operations Centers and bus operator security management. An initial training effort for all transit bus operators will be conducted followed by a recurrent training effort.

We expect to expand the Intermodal-Security Training and Exercise Program training program with our stakeholders as expeditiously as resources will allow. We also intend to continue to coordinate with Department of Transportation/Federal Transit Administration on response and recovery issues to help identify existing gaps that we can target in our program.

TSA is working on a Mass Transit and Passenger Rail employee training rule to establish standards for employee training.

TSA will continue working with the American Public Transportation Association in the development of standards and guidance. These standards and guidance will inform the training process through the Baseline Assessment for Security Enhancement as well as training smart practices.

TSA will work with the mass transit and passenger rail law enforcement communities as well as Government agencies to develop and coordinate existing response plans.

TSA will advance its chemical and biological response and detection capabilities through additional research and development activities in conjunction with S&T.

TSA will work closely with transit agencies on the use of TSA resources (transportation security officers, behavior detection officers, surface inspectors, and Federal Air Marshals) to support passenger and baggage screening efforts; similar resources have been supporting Visible Intermodal Prevention and Response efforts since December 2005.

In FY 2011, the effectiveness of TSA’s STSIP will be enhanced through implementation of the following programs and initiatives:

The STSIP will continue expansion of the Surface Transportation Security Training Center in Pueblo, Colorado to provide training opportunities in all surface modes. The dedicated training center will allow TSA to train greater numbers of field employees and managers on surface transportation programs and issues, thus increasing the level of agency expertise in surface transportation. This is expected to continue to increase internal awareness of the mission of the surface inspector workforce and its utilization.

TSA expects to issue a Notice of Proposed Rulemaking that, when final, will require certain training requirements for mass transit, freight rail, intercity bus, and motor carrier entities as a result of the 9/11 Act. When these regulations are final, surface inspectors will be charged with monitoring industry compliance. In FY 2011, the TSA will begin to examine and develop compliance protocols for these regulations and related inspector training.

Training

FY 2010 Accomplishments

In 2010, TSA’s Operational and Technical Training Division (OTT), within the OSO has finalized a Strategic Plan for the management of the technical training program.

OTT recently developed a Curriculum Development roadmap tool that visually depicts the forecast for all curriculum-related activities on the horizon.

Initiatives Underway and Planned

TSA is exploring the feasibility of establishing a TSA Academy for Transportation Security Officers. An Integrated Project Team will be launched at the start of FY 2011, to develop a comprehensive alternatives analysis for senior leadership consideration.

While TSA has always had an On-the-Job Training (OJT) program, TSA is in the final stages of a more structured and formalized OJT Program, which will include a structured training curriculum for the TSOs who will sign up to serve as an OJT Instructor.

TSA has scheduled a pilot to be conducted in the second quarter of FY 2011, and if minimal and/or no changes are required as a result of the pilot conducted, TSA plans to implement this program system wide in the third quarter of FY 2011.

Challenge #9: Trade Operations and Security

CBP is at the frontline of protecting the nation from threats, including those posed by maritime cargo. CBP has implemented a multilayered approach to security, using a risk management approach to strategically apply resources to prioritized enforcement objectives and threats.

Targeting and Examining High Risk Cargo

FY 2010 Accomplishments

CBP's multilayered approach to security includes obtaining advance information about cargo; using targeting techniques to assess risk and building a knowledge base about the people and companies involved in the supply chain; fostering partnerships with the private sector and collaborating with other Federal agencies and departments; expanding enforcement efforts to points earlier in the supply chain than simply our borders; and maintaining robust inspection regimes, including non-intrusive inspection equipment and radiation detection technologies, at our ports of entry.

CBP requires advanced electronic cargo information, as mandated in the Trade Act of 2002 (24-Hour Rule, through regulations), for all inbound shipments in all modes of transportation. CBP requires the electronic transmission of additional data, as mandated by the SAFE Port Act, through the Importer Security Filing and Additional Carrier Requirements rule (Security Filing "10+2"), which became effective as an Interim Final Rule on January 26, 2009, and went into full effect on January 26, 2010. Under the Security Filing "10+2" rule, importers are responsible for supplying CBP with ten trade data elements 24 hours prior to vessel lading, and ocean carriers are required to provide their vessel stow plans no later than 48 hours after departure and their container status messages no later than 24 hours after creation or receipt. This advance data allows CBP targeting specialists to identify risk factors earlier in the supply chain.

The National Targeting Center – Cargo (NTC-C) analyzes this advance cargo information using the Automated Targeting System (ATS) before shipments reach the United States and identifies high-risk, shipments. This information is used by CBP and other agencies to support enforcement actions, such as seizures and arrests.

In addition to this advance information, CBP works with the trade community through the Customs Trade Partnership Against Terrorism (C-TPAT), a voluntary public-private sector partnership program in which CBP works with the principal stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers to ensure the highest possible levels of cargo security.

C-TPAT membership consists of 10,056 Certified Partners which includes 4,440 importers, 2,803 carriers, 859 brokers, 826 consolidators/3PLs, 58 marine port authority and terminal operators and 1,070 foreign manufactures. C-TPAT has conducted 16,242 on site validations of manufacturing and logistics facilities in 97 countries representing some of the most terrorist prone and high risk areas of the world. C-TPAT currently has 142 Supply Chain Security Specialists located in 7 operational field offices.

Initiatives Underway and Planned
CBP is continuing to work with the trade community to further leverage private sector resources to enhance supply chain security. Additionally, CBP is working with foreign partners to establish bi-national recognition and enforcement of C-TPAT.

Container Security Initiative

FY 2010 Accomplishments
CBP partners with foreign governments through the Container Security Initiative (CSI) to prevent and deter terrorist threats before they reach American ports. CSI enables CBP to identify and inspect high-risk U.S.-bound cargo containers at foreign ports prior to departure. Through CSI, CBP stations multidisciplinary teams of officers to work with host country counterparts to identify and examine containers that are determined to pose a high risk for terrorist activity. CSI, the first program of its kind, was announced in January 2002 and is currently operational in 58 foreign seaports—covering more than 80 percent of the maritime containerized cargo shipped to the United States.

CBP officers stationed at CSI ports, with assistance from CSI personnel at the National Targeting Center–Cargo (NTC–C), review 100 percent of the manifests originating and/or transiting those foreign ports for containers that are destined for the United States. In this way, CBP identifies and examines high risk containerized maritime cargo prior to lading at a foreign port and before shipment to the United States.

Initiatives Underway and Planned
As the CSI program has matured, CBP looked for opportunities to increase efficiencies and reduce costs by shifting functions to the NTC–C. CBP's ability to target high risk containers has progressed to the point that much of the work can be done from CBP's U.S. location rather than through a physical presence overseas. CBP is exploring opportunities to utilize emerging technology in some locations, which will allow the program to become more efficient and less costly. In January 2009, CBP began to reduce the number of personnel stationed overseas who perform targeting functions, increasingly shifting the targeting of high risk containers to personnel stationed at the NTC–C. This shift in operations reduces costs without diminishing the

effectiveness of the CSI program. CBP will remain operational in all 58 locations in fiscal year 2011 with sufficient personnel in country to conduct the examinations of high risk shipments with the host government and to maintain relationships with their host-country counterparts.

Scanning of Cargo

FY 2010 Accomplishments

The Secure Freight Initiative (SFI) is an effort to enhance the U.S. Government's ability to scan containers for nuclear and radiological materials at seaports worldwide and better assess the risk of inbound containers. SFI is currently deployed at five overseas pilot ports and reflects close collaboration with other Federal agencies, foreign governments, and the trade community. SFI provides carriers of maritime containerized cargo greater confidence in the security of the shipment they are transporting, and promotes the secure flow of commerce.

Initiatives Underway and Planned

CBP provided a report to Congress on April 13, 2010 entitled, "Risk-Based, Layered Approach to Supply Chain Security" in response to language in the House Report 111-157 and the Conference Report 111-298 accompanying the FY 2010 Department of Homeland Security Appropriations Act (Pub. L. 111-83). The act required that CBP provide a report on its strategy to achieve meaningful and effective cargo and supply chain security in lieu of 100-percent scanning of cargo. CBP agrees with Congress's conclusion in House Report 111-157 that, "at least for now, a 100-percent scanning goal is not feasible, and even if it were, would come at an unacceptably high cost monetarily and in the displacement of other efforts." CBP achieves meaningful cargo and supply chain security in the absence of the total scanning requirements by employing a risk-based, layered approach that includes collecting advanced information on cargo entering the United States, working with partners in the shipping industry to improve their security, and focusing on high-risk shipments. CBP has determined that this approach to enhancing security across all potential transit vectors is more efficient and cost effective than alternative approaches that focus exclusively on a single layer of defense.

Acronym List

Acronyms

AAP – Advanced Acquisition Plan

ADMP – Active Duty Military Payroll

AFG – Assistance to Firefighters Grants

AFR – Annual Financial Report

AMP – Asset Management Plan

ARB – Acquisition Review Board

ARRA – American Recovery and Reinvestment Act

ATA – American Trucking Association

BEST – Border Enforcement Security Task Force

BP – British Petroleum

BPD – Bureau of Public Debt

BUR – Bottom-Up Review

CAE – Component Acquisition Executive

CBP – U.S. Customs and Border Protection

CBRN – Chemical, Biological, Radiological, and Nuclear

CDL – Community Disaster Loan

CDP – Center for Domestic Preparedness

CDSOA – Continued Dumping and Subsidy Offset Act

CFO – Chief Financial Officer

CFR – Code of Federal Regulations

CIKR – Critical Infrastructure and Key Resources

CIO – Chief Information Officer

CIPAC – Critical Infrastructure Partnership Advisory Council

CISO – Chief Information Security Officer

COBRA – Consolidated Omnibus Budget Reconciliation Act of 1985

COTR – Contract Officer’s Technical Representative

COTS – Commercial Off-the-Shelf

CPARS – Contractor Performance Assessment Reporting System

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

DART – Disaster Acquisition Response Team

DC – District of Columbia

DHS – Department of Homeland Security

DHS FAA – Department of Homeland Security Financial Accountability Act

DNDO – Domestic Nuclear Detection Office

DNSSEC – Domain Name System Security

DOC – Department of Commerce

DOD – Department of Defense

DOL – Department of Labor

DRO – Detention and Removal Operations

EaaS – Email as a Service

EDMO – Enterprise Data Management Office

EDS – Explosive Detection System

EFSP – Emergency Food and Shelter Program

EHP – Environmental and Historic Preservation

EMI – Emergency Management Institute

EOC – Emergency Operations Centers

EMPG – Emergency Management Performance Grant Program

EPIC – Enterprise Procurement Information Center

ERA – Enterprise Reporting Application

ESCM – Entry Summary Compliance Measurement

FAR – Federal Acquisition Regulation

FBwT – Fund Balance with Treasury

FCRA – Federal Credit Reform Act of 1990

FECA – Federal Employees Compensation Act

FEMA – Federal Emergency Management Agency

FERS – Federal Employees Retirement System

FFMIA – Federal Financial Management Improvement Act of 1996

FFSR – Federal Financial Systems Requirements

FIMA – Federal Insurance and Mitigation Administration

FISMA – Federal Information Security Management Act

FLETC – Federal Law Enforcement Training Center

FMFIA – Federal Managers' Financial Integrity Act

FOSC – Federal On-scene Coordinators

FPDS – Federal Procurement Data System

FPDS-NG – Federal Procurement Data System-Next Generation

FPS – Federal Protective Service

FSIO – Financial Systems Integration Office

FY – Fiscal Year

GAAP – Generally Accepted Accounting Principles

GAO – Government Accountability Office

GCC – Government Coordinating Councils

GCCF – Gulf Coast Claims Facility

GPD – Grant Programs Directorate

GSA – General Services Administration

HCA – Heads of Contracting Activity

HQ – Headquarters

HSA – Homeland Security Act of 2002

HSAM – Homeland Security Acquisition Manual

HSAR – Homeland Security Acquisition Regulation

HSGP – Homeland Security Grant Program

HSPD – Homeland Security Presidential Directive

HUD – Housing and Urban Development

ICAO – International Civil Aviation Organization

ICCB – Internal Control Coordination Board

ICE – U.S. Immigration and Customs Enforcement

IDI – Injured Domestic Industries

IDIQ – Indefinite Delivery Indefinite Quantity

IED – Improvised Explosive Device

IEFA – Immigration Examination Fee Account

IHP – Individuals and Household Programs

IMP – Integrated Management Plan

INA – Immigration Nationality Act

IP – Improper Payment

IPERA – Improper Payments Elimination and Recovery Act

IPIA – Improper Payments Information Act of 2002

IT – Information Technology

JHSG – Joint Housing Solutions Group

JIATF – Joint Interagency Task Force

LBTT – Local Business Transition Team

LOI – Letters of Intent

MD – Management Directive

MD&A – Management's Discussion and Analysis

MERHCF – Medicare-Eligible Retiree Health Care Fund

MGMT – Management Directorate

MMS – Marine Mammal Systems

MRS – Military Retirement System

MTS – Metric Tracking System

ND – Non-Disaster

NEMA – National Emergency Management Association

NFIP – National Flood Insurance Program

NIEM – National Information Exchange Model

NIPP – National Infrastructure Protection Plan

NPFC – National Pollution Funds Center

NPPD – National Protection and Programs Directorate

NTC-C – National Targeting Center for Cargo

OCFO – Office of the Chief Financial Officer

OCIO – Office of the Chief Information Officer OCPO – Office of the Chief Procurement Officer

OHA – Office of Health Affairs

OIG – Office of Inspector General

OJT – On-the-Job Training

OMB – Office of Management and Budget

OM&S – Operating Materials and Supplies

OPA – Oil Pollution Act of 1990

OPEB – Other Post Retirement Benefits

OPM – Office of Personnel Management

ORB – Other Retirement Benefits

OSLTF – Oil Spill Liability Trust Fund

OSO – Office of Security Operations

OTT – Operational and Technical Training Division

PA – Public Assistance

PA&E – Program Analysis and Evaluation

PCS – Process Control Systems

PIA – Privacy Impact Assessment

PM – Program Manager

POA&M – Plan of Action and Milestones

PP&E – Property, Plant, and Equipment

PSA – Protective Security Advisor

Pub. L. – Public Law

PY – Prior Year

QHSR – Quadrennial Homeland Security Review

Recovery Act – The American Recovery and Reinvestment Act of 2009

RSSI – Required Supplementary Stewardship Information

SAT – Senior Assessment Team

SBI – Secure Border Initiative

SBInet – Secure Border Initiative Network

SBR – Statement of Budgetary Resources

SCC – Sector Coordinating Council

SEI – Special Emphasis Inspection

SFFAS – Statement of Federal Financial Accounting Standards

SFI – Secure Freight Initiative

SFRBTF – Sport Fish Restoration Boating Trust Fund

SMC – Senior Management Council

SPO – Single Point Ordering

SPOT – Single Point Order Tracking

S&T – Science and Technology Directorate

STA – Security Threat Assessment

STSIP – Surface Transportation Security Inspection Program

TAFS – Treasury Account Fund Symbol

TASC – Transformation and Systems Consolidation

TIC – Trusted Internet Connection

TME – Tactical Modeling

TSA – Transportation Security Administration

TSE – Transportation Security Equipment TSGP – Transit Security Grants Program

TSI – Transportation Security Inspector

T&E – Test and Evaluation

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

USSS – U.S. Secret Service

WHTI – Western Hemisphere Travel Initiative

WYO – Write Your Own

Homeland
Security