STATEMENT OF JOHN E. MCCOY II

DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY, AND FINANCIAL MANAGEMENT

U.S. HOUSE OF REPRESENTATIVES

October 27, 2011

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you on behalf of the Department of Homeland Security (DHS) Office of Inspector General (OIG). My testimony today will focus on information technology (IT) issues discovered during the fiscal year (FY) 2010 financial statement audit. The information provided in this testimony is based on the report: *Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit (OIG-11-103).*

We engaged the independent accounting firm of KPMG, LLC to perform an integrated financial audit of the DHS, which included an evaluation of the following IT controls and issues:

- General controls of DHS' financial processing environment as defined by the Federal Information System Controls Audit Manual (FISCAM).
- Technical security for development and production devices that directly support key general support systems.
- Application controls on a limited number of DHS' financial systems and applications. Application controls are the structure, policies, and procedures that apply to supporting systems, such as inventory and payroll.
- Financial system functionality.
- Physical security, e.g. physical access to media and equipment that could be used to gain unauthorized access to financial systems.

DHS Financial Systems Progress and Challenges

DHS made some progress in remediating the IT findings reported in FY 2009, which resulted in the closure of approximately 30 percent of the prior year IT findings. In FY 2010, KPMG identified 161 findings, of which approximately 65 percent are repeated from FY 2009. In addition, DHS' financial systems have many functional limitations that affect the Department's ability to implement and maintain internal controls.

IT General Control Issues

From a financial statement perspective, DHS' five most significant weaknesses are: (1) Access Controls, (2) Configuration Management, (3) Security Management, (4) Contingency Planning, and (5) Segregation of Duties.

Access Controls protect information from unauthorized modification, loss, and disclosure by limiting access to data, programs, and facilities. At several DHS components KPMG noted excessive potential for unauthorized access to key financial applications. For example, system administrator access to financial applications was not properly restricted and strong password requirements were not enforced. KPMG observed ineffective safeguards over physical access to sensitive facilities and resources such as government credit cards, passwords, and laptops. KPMG also used social engineering to attempt to manipulate individuals into divulging sensitive information or

allowing computer system access. During the audit, some DHS employees provided their system user names and passwords to an auditor posing as a help desk employee.

Configuration Management controls help ensure that systems are operating securely. At several components, KPMG observed configuration management controls that were not fully defined, followed, or effective. For example, KPMG found a lack of documented policies and procedures to prevent users from having concurrent access to the development, test, and production environments of financial systems. In addition, configuration, vulnerability, and patch management plans were not implemented, or did not comply with DHS policy.

Security Management controls provide a framework for managing risk, developing security policies, and monitoring the adequacy of computer-related security controls. At several DHS components KPMG noted that financial systems as well as general support systems were not properly certified and accredited. KPMG also found scenarios where roles and responsibilities were not clearly defined, and a lack of policies and procedures and compliance with existing policies. For example, procedures for exit processing of contractors had not been established, and procedures for IT-based specialized security training were not in place.

Contingency Planning controls involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur. KPMG noted instances of incomplete or outdated business continuity plans and systems with incomplete or outdated disaster recovery plans. Some plans were not adequately tested and did not contain current system information, emergency processing priorities, or procedures for backup and storage.

Segregation of Duties controls constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations. At several DHS components, KPMG noted a lack of proper segregation of duties for roles and responsibilities within financial systems. For example, financial system users had conflicting access rights as the Originator, Funds Certification Official, and the Approving Official. In addition, policy and procedures to define and implement segregation of duties were not implemented.

Collectively, these IT control deficiencies limited DHS' ability to ensure the confidentiality, integrity, and availability of critical financial and operational data. KPMG considers them to collectively represent a material weakness for DHS under standards established by the American Institute of Certified Public Accountants and the Government Accountability Office.

Financial System Functionality Issues

Many of the Department's financial systems have not been substantially updated since the creation of DHS. In some cases, financial system functional limitations are negatively affecting DHS' ability to implement and maintain strong internal controls,

especially in the areas of financial data processing and reporting. For example, some components cannot modify IT system core software or install controls to prevent duplicate payments. This contributed to duplicate payments made by Immigration and Customs Enforcement (ICE) in FYs 2009, 2010, and 2011. These and other IT System limitations also lead to extensive manual and redundant procedures to process transactions, verify the accuracy of data, and prepare financial statements.

Component IT Financial Systems

For FY 2010, we issued separate IT management letter reports for the United States Citizenship and Immigration Services (USCIS), the United States Coast Guard (Coast Guard), Customs and Border Protection (CBP), the Federal Emergency Management Agency (FEMA), the Federal Law Enforcement Training Center (FLETC), ICE, and the Transportation Security Administration (TSA). We also issued an overall consolidated IT management letter report that summarized the IT issues for all seven components. Each management letter addressed component-level IT security issues and provided individual findings and recommendations. KPMG recommended that the components' chief information officers and chief financial officers work with the DHS chief information and chief financial officers to address the issues noted in the reports.

USCIS

During FY 2010, USCIS took corrective action to address prior year IT control deficiencies such as physical controls at the Manassas Data Center, and access controls over security software. However, during FY 2010, KPMG continued to identify IT general control deficiencies that could potentially impact USCIS' financial data. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System configuration and patch management, and deficiencies within the Computer Linked Application Information Management System (CLAIMS) 3 LAN and CLAIMS 4 user account management. Collectively, the IT control deficiencies limited USCIS's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability.

Of the 14 findings identified during our FY 2010 testing, 3 were new IT findings. These findings represent control deficiencies in four of the five FISCAM key control areas: configuration management, access controls, segregation of duties, and security management. Specifically, these control deficiencies include: (1) a lack of strong password management and audit logging within the financial applications, (2) security management issues involving staff security training and exit processing procedure weaknesses, (3) inadequately designed and operating configuration management, and (4) the lack of effective segregation of duties controls within financial applications.

Coast Guard

During FY 2010, KPMG determined that the Coast Guard remediated eight IT findings identified in previous years. Specifically, the Coast Guard took actions to improve aspects of its user recertification process, data center physical security, and scanning for system vulnerabilities. The Coast Guard's remediation efforts have enabled KPMG to expand test work into areas that were not practical to test previously, considering management's acknowledgment of the existence of control deficiencies.

During FY 2010, KPMG identified 28 IT findings, 10 of which were repeat findings from the prior year and 18 were new findings. Most of the new findings relate to IT systems that were added to the examination scope this year. Collectively, these findings represent deficiencies in four of the five key control areas, including security management, access control, segregation of duties, and configuration management.

KPMG also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems are not compliant with the *Federal Financial Management Improvement Act* and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control weaknesses and strengthening the control environment at the Coast Guard. The majority of the findings indicate a lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS Sensitive System Policy Directive 4300A requirements and National Institute of Standards and Technology guidance. Since key Coast Guard financial systems house TSA financial data, deficiencies identified in the Coast Guard's IT environment also impact TSA.

CBP

During FY 2010, CBP remediated 13 IT findings identified in previous years and took corrective action to address prior year IT control weaknesses. For example, CBP made improvements over various system logical access processes and system security settings, and system administrator access processes and procedures. CBP also performed more consistent tracking of contractors and system user rules of behavior agreements. However, during FY 2010, KPMG identified 23 IT findings, of which 16 were repeat findings from the prior year and 7 were new findings. Collectively, these findings represent deficiencies in security management, access control, and segregation of duties, as well as deficiencies related to financial system functionality. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and CBP financial data could be exploited, thereby compromising the integrity of financial data used by management and reported in CBP's financial statements.

FEMA

During FY 2010, FEMA took corrective action to address certain prior year IT control weaknesses. For example, FEMA made improvements over implementing certain logical and physical access controls over National Flood Insurance Program information

systems, as well as development and maintenance of the inventory of FEMA Chief Financial Officer-designed financial management systems. However, during FY 2010, KPMG continued to identify weaknesses that could potentially impact FEMA's financial data. Some of the most significant weaknesses from a financial statement audit perspective related to controls over security management, access control, configuration management, and contingency planning, as well as weaknesses over physical security and security awareness. Collectively, these weaknesses limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. Of the 63 findings identified during our FY 2010 testing, 50 were repeat findings, either partially or in whole from the prior year, and 13 were new IT findings. In FY 2010, disagreements with management's self assessment on the status of repeat findings occurred almost entirely at FEMA. As reported by KPMG during audit status briefings to the OIG and management, this condition did not repeat in FY 2011.

FLETC

During FY 2010, FLETC took corrective action to address prior year IT control weaknesses, such as improvements over configuration management in Momentum and the Glynco Area Network and management review over Momentum auditing logs. However, during FY 2010, KPMG continued to identify IT general control weaknesses that could potentially impact FLETC's financial data. The most significant weaknesses were related to the Glynco Area Network logical access controls and weaknesses over physical security and security awareness. Collectively, the IT control weaknesses limited FLETC's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. Of the six findings identified during our FY 2010 testing, one was a new IT finding. These findings represent control deficiencies in configuration management, security management, and access controls.

ICE

During FY 2010, ICE took corrective action to address some prior year IT control weaknesses. For example, ICE made improvements over physical controls at facility entrances, and Active Directory Exchange user account lockout settings and recertifications. However, during FY 2010, KPMG continued to identify IT general control weaknesses that could potentially impact ICE's financial data. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System configuration, patch management and user account management and weaknesses over physical security and security awareness. Collectively, the IT control deficiencies limited ICE's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability.

Of the 16 findings identified during our FY 2010 testing, 9 were new IT findings. These findings represent control deficiencies in 4 of the 5 key control areas: configuration management, access controls, security management, and segregation of duties.

TSA

During FY 2010, TSA took corrective action to address prior year IT control deficiencies. For example, TSA made improvements in its policies and procedures over its configuration management monitoring controls related to the development, implementation, and tracking of scripts at Coast Guard's Financial Center. However, during FY 2010, KPMG continued to identify IT general control deficiencies that impact TSA's financial data. Of the four findings issued during FY 2010 testing, three were repeat findings and one was a new IT finding. These findings represent deficiencies in three of the five FISCAM key control areas. Specifically, the deficiencies were: (1) unverified access controls through the lack of comprehensive user access privilege re-certifications, (2) security management issues involving the terminated employee process, and (3) physical security and security awareness issues.

KPMG also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems that house TSA financial data are not compliant with the *Federal Financial Management Improvement Act* and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control deficiencies.

DHS Financial Systems Modernization

DHS has made several attempts to modernize its financial systems. It's most recent initiative was the Transformation and Systems Consolidation, or TASC. This initiative was intended as an enterprise-wide solution that would consolidate financial, asset and acquisition management systems for all of DHS. In March 2011, the TASC project was cancelled after the Government Accountability Office sustained one of the protests and recommended that DHS reevaluate its requirements with regard to the scope of work covered by the solicitation, and if appropriate, issue a revised request for proposals to appropriately reflect the Department's actual requirements. In September, the Under Secretary of Management announced that the Department would pursue a decentralized approach instead of an enterprise-wide solution like TASC. The new approach will prioritize system modernization for components with the most critical need. The implementation of a new financial systems solution combined with improving IT security controls should allow the Department to achieve greater effectiveness in its financial management.

We will continue our positive working relationship with the Department by taking a proactive approach to overseeing DHS' financial management improvement efforts. We look forward to continuing our audit efforts and providing the results and solutions to the Secretary and the Congress.

Mr. Chairman, this concludes my prepared statement. Thank you for this opportunity and I welcome any questions from you or Members of the Subcommittee.

John E. McCoy, II
Deputy Assistant Inspector General for Audits
Department of Homeland Security
Office of Inspector General

John E. McCoy II was selected in December 2010 as the Deputy Assistant Inspector General for Audits for the Department of Homeland Security (DHS), Office of Inspector General (OIG). From March 2007 to December 2010 he served as the Director, Financial Management for DHS OIG. Prior to his arrival at the OIG, John was the Chief of the Financial Services Branch at the Federal Emergency Management Agency for four years. From 1994 through 2002, John worked for Certified Public Accounting firms and managed and performed financial statement audits, performance audits, and provided consulting services to federal and commercial clients. From 1993 to 1994 John worked for the Commonwealth of Virginia as a sales tax auditor and from 1991 to 1993 John worked for the Air Force Audit Agency. He served four years in the United States Marine Corps. John is a Certified Public Accountant and a Certified Information Systems Auditor. He has a Masters Degree in Accounting from George Mason University and Bachelor of Science degrees in Accounting and Business Information Systems from Illinois State University.