Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Transportation Security Administration Component of the FY 2011 DHS Financial Statement Audit

OIG-12-47

March 2012

Office of Inspector General

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

March 9, 2012

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.

This report presents the information technology (IT) management letter for the Transportation Security Administration (TSA) component of the fiscal year (FY) 2011 DHS consolidated financial statement audit as of September 30, 2011. It contains observations and recommendations related to information technology internal control weaknesses that were summarized in the *Independent Auditors' Report* dated November 11, 2011 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at the TSA component in support of the DHS FY 2011 consolidated financial statement audit and prepared this IT management letter. KPMG is responsible for the attached IT management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Office of Information Technology

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

February 16, 2012

Acting Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
Transportation Security Administration

We have audited the balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2011 and the related statement of custodial activity for the year then ended (referred to herein as the "fiscal year (FY) 2011 financial statements"). The objective of our audit was to express an opinion on the fair presentation of these financial statements. We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended, based on the criteria established in Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Internal Control*, Appendix A. In connection with our audit, we also considered DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the FY 2011 financial statements.

Our *Independent Auditors' Report* issued on November 11, 2011, describes a limitation on the scope of our audit that prevented us from performing all procedures necessary to express an unqualified opinion on DHS' FY 2011 financial statements and internal control over financial reporting. In addition, the FY 2011 DHS *Secretary's Assurance Statement* states that the Department was unable to provide assurance that internal control over financial reporting was operating effectively at September 30, 2011.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 11, 2011, included internal control deficiencies identified during our audit, that individually, or in aggregate, represented a material weakness or a significant deficiency. This letter represents the separate limited distribution report mentioned in that report.

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to DHS' financial systems general Information Technology (IT) controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. We also noted that in some cases, financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also described in the *General IT Control Findings and Recommendations* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and are intended For Official Use Only. We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key DHS financial systems within the scope of the FY 2011 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls (comments not related to IT) have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General (OIG), U.S. Office of Management and Budget (OMB), U.S. Government Accountability Office (GAO), and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2011

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit DHS' balance sheet as of September 30, 2011, and the related statement of custodial activity for the year then ended, we performed an evaluation of general information technology controls (GITC) at TSA, to assist in planning and performing our audit. The U.S. Coast Guard's (Coast Guard) Finance Center (FINCEN) hosts key financial applications for TSA. As such, our audit procedures over GITC for TSA included testing of the Coast Guard's FINCEN policies, procedures, and practices, as well as TSA policies, procedures and practices at TSA Headquarters. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A.

The FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the general IT controls environment.

- *Security Management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.

- *Access Control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.

- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.

- *Segregation of Duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.

- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit, we also performed technical security testing for key network and system devices. The technical security testing was performed both over the Internet and from within select Coast Guard facilities, and focused on test, development, and production devices that directly support TSA's financial processing and key general support systems.

In addition to GITC testing, application controls were tested for the year ending September 30, 2011, which were identified as key controls by the financial audit team.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2011, TSA took corrective action to address prior year IT control deficiencies. For example, TSA made improvements in its own policies and procedures over its recertification of the user accounts process. During FY 2011, we continued to identify IT general control deficiencies that impact TSA's financial data. The key issue from a financial statement audit perspective related to controls over the development, implementation, and tracking of scripts at Coast Guard's FINCEN. Collectively, these deficiencies negatively impacted the internal controls over TSA's financial reporting and its operation, and we consider them to contribute to a material weakness at the Department level under standards established by the American Institute of Certified Public Accountants. In addition, based upon the results of our test work, we noted that TSA did not fully comply with the Department's requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the six findings issued during our TSA FY 2011 testing, four were repeat findings, and two were new IT findings. 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) access control issues involving password complexity settings, 3) use of generic 'admin' user id and password, 4) security management issues involving the new employee process, and 5) physical security and security awareness issues.

In addition, we determined that the following deficiencies identified at the Coast Guard IT environment also impact TSA financial data: 1) inadequately designed and operating IT script change control policies and procedures, 2) security management issues involving civilian and contractor background investigations, 3) lack of consistent contractor, civilian, and military system account termination notification processes, 4) physical security and security awareness issues, and 5) procedures for role-based training for individuals with elevated responsibilities is not fully implemented. We 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 FFMIA and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control deficiencies, and strengthening the control environment at FINCEN.

These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and TSA financial data could be exploited thereby compromising the integrity of financial data used by management and reported in TSA's financial statements.

While the recommendations made by us should be considered by TSA, it is the ultimate responsibility of TSA management to determine the most appropriate method(s) for addressing the deficiencies identified based on their system capabilities and available resources.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2011 DHS Financial Statement Audit, we identified the following TSA IT and financial system control deficiencies that in the aggregate are considered management letter comments. Our findings are divided into two groupings: 1) financial systems controls, and 2) IT system functionality.

Related to IT Controls:

Configuration Management

The Coast Guard's core financial system configuration management process controls are not operating effectively, and continue to present risks to TSA financial data confidentiality, integrity, and availability. Financial data in the general ledger may be compromised by automated and manual changes that are not adequately controlled. For example, the Coast Guard uses an IT scripting process to make updates, as necessary, to its core general ledger software to process financial data. We noted that some previously noted weaknesses were remediated, while other control deficiencies continued to exist. The remaining control deficiencies that were present throughout FY 2011 vary in significance; however four key areas that impact the Coast Guard Script control environment are: 1) Script Testing Requirements, 2) Script Audit Logging, 3) Script Approvals and Recertifications, and 4) Script Record Documentation Review.

- Script Testing Requirements: There are no detailed requirements over the review and testing of functional changes to the data including functional test plans.
- Script Audit Logging: Controls over audit logs in the production databases are not consistently implemented to log privilege user actions and scripts run. A review was implemented in May 2011 to reconcile between the scripts run in the production databases and the changes made to the database tables. However, this review only occurred one day a month which only consisted of 5% of scripts run a month.
- Script Approvals and Recertifications: Dimensions (automates the process for executing scripts into the CAS suite database) users were not being reviewed and Mashups listings were not completed as they did not include the script runners and system administrators for Dimensions. Additionally, documentation retained in support of the reviews was not adequately completed per FINCEN policy throughout the year.
- Script Record Documentation Review: Fields in the Mashups tool (automated approval workflow which enforces rules defined in the system from approvals and will retain all the records within the online database for audit purposes) are not always accurately recorded and no final review is performed to ensure that they are accurate. Additionally, there are certain fields that should reconcile, and any discrepancies are not always consistently documented and explained.

In addition, we noted weaknesses in the script change management process at the USCG as it relates to the Internal Control over Financial Reporting process (e.g., the financial statement impact of the changes to FINCEN core accounting system through the script change management process).

Access Control

- Access review procedures for key financial applications do not include the review of all user accounts to ensure that all terminated individuals no longer have active accounts; inactive accounts are locked; and privileges associated with each individual are still authorized and necessary.

- Password settings for one key financial application were not configured to enforce DHS/CG password length or complexity.
- Administrative access to one key financial application is granted to members of the Database Administration (DBA) team through the use of a generic user ID and shared password.

Security Management

- The computer access agreement for TSA employees is not being completed; and
- During our after-hours physical security and social engineering testing we identified exceptions in the protection of sensitive user account information. The tables below detail the exceptions identified at the locations tested.

After-Hours Physical Security Testing:

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a TSA employee's / contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at TSA Headquarters.

Exceptions Noted	**Total Exceptions at TSA HQ by Type**
Unsecured Laptop	4
PII	3
DHS/TSA Badge	1
Keys that unlocked laptops	2
Total Exceptions at TSA HQ	**10**

Social Engineering Testing:

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or gaining computer system access.

Total Called	**Total Answered**	**Number of employees who provided their user ID and password**
40	20	4

Related to Financial System Functionality:

We noted that financial system functionality limitations are contributing to control deficiencies reported elsewhere in Exhibit I in the *Independent Auditor's Report, dated November 11, 2011*, and inhibiting progress on corrective actions impacting TSA. These functionality limitations are preventing the TSA from improving the efficiency and reliability of its financial reporting processes. Some of the financial system limitations lead to extensive manual and redundant procedures to process transactions, verify accuracy of data, and to prepare financial statements. Systemic conditions related to financial system functionality include:

- As noted above, Coast Guard's core financial system configuration management process is not operating effectively due to inadequate controls over the IT script process. The IT script process was instituted as a solution primarily to compensate for system functionality and data quality issues;
- For one financial system that was configured by the vendor, Coast Guard and TSA do not have the ability to modify the vendor established password settings;
- Production versions of operational financial systems are outdated, no longer supported by the vendor, and do not provide the necessary core functional capabilities (e.g., general ledger capabilities); and
- Issues with current technology are preventing TSA management from reviewing account recertification reports timely.

Recommendations: We recommend that TSA:

- Work with the DHS Chief Financial Officer (CFO), DHS Chief Information Officer (CIO), and the Coast Guard CFO and CIO to ensure the following planned corrective actions take place in a timely manner:
  - Continue to update the procedures, tools, and associated training to better address script record documentation reviews and provide training to impacted staff.
  - Continue to improve and better document the script audit logging processes and associated technical implementations in compliance with Coast Guard software development lifecycle (SDLC) and CM policies and procedures.
  - Continue to improve and better document script approvals; define and implement script management and execution tool user access/account recertification procedures; and update associated training and provide that training to impacted staff.
  - Continue to improve and better document script testing requirements and associated technical implementations and test environments in compliance with Coast Guard SDLC and CM policies and procedures.
  - Continue to improve the script change management process and other associated internal controls as these relate to the financial statement impact of the changes to the Core Accounting System (CAS) Suite financial databases.
  - Continue to implement policy regarding approval of scripts that impact financial statements.
- Office of Property Management Systems should closely monitor and follow-up with Deputy Property management Officials to ensure requests are implemented timely for Sunflower.
- As part of the ongoing efforts to strengthen internal controls over access to TSA financial systems, in the second quarter of FY 2011, the Financial Systems Branch added an additional level of quality

assurance (QA) review to the quarter review process. The QA step will help minimize human errors in regards to Markview.

- Monitor FINCEN on the status of the Markview developer to incorporate the ability to provide for stronger password controls in the Markview system as required by the DHS Sensitivity System Policy Directive 4300A.

  By early September 2011, the Markview developer should complete an analysis of the level of effort involved to update the product to be in compliance with IT security requirements, i.e., password to be 8 characters in length; contain a combination of alpha, numeric, and special characters; not be the same as previous 8 password; stored in the encrypted form; account locked after 3 failed login attempts; initial login prompts users to change initial password; and passwords changed every 90 days.

  TSA should work with FINCEN to develop a schedule to test and implement these changes after the vendor has delivered the new version that incorporates the compliant password controls.

- Implement an automated e mail notification process so that all new Markview users are reminded of the requirements of adhering to strong password controls as identified in the DHS 4300A Sensitivity Policy.

- Establish a procedure to change the ADMIN password every 90 days as required by the DHS Sensitivity System Policy Directive 4300A. This will minimize the risk of unauthorized access to the Markview system.

- Implement a unique user id and password for all DBAs as required by the DHS Sensitivity System Policy Directive 4300A. Establishing a unique user account that will create accountability and system changes will be easily identifiable and traced to an individual DBA.

- Convert the manual process of keeping hardcopies of the computer access agreement (CAA) to an electronic and computer-based process where employees will be instructed to review the CAA online via TSA's Online Learning Center.

- Update the policy on the CAA to coincide with this process, so that temporary access to a TSA computer is permitted, making completing the CAA online possible, ensuring compliance with policy and ease of reviewing and maintaining this form.

- Continue to execute the IT Security Awareness Training Program.

- Conduct internal physical security walkthroughs on a semi-annual basis.

- Conduct internal social engineering testing on a quarterly basis.

- Conduct a one-on-one training with individuals failing physical security after-hours testing and social engineering attempts.

- Take administrative actions, if needed, on a case-by-case basis.

- Conduct a communications campaign to address the effects of improper handling of physical security, and

- Conduct a communications campaign via broadcasts warning against social engineering.

APPLICATION CONTROLS

Application controls were tested for the year ending September 30, 2011, and we found no issues.

Appendix A

Description of Key TSA Financial Systems within the Scope of the FY 2011 DHS Financial Statement Audit

Below is a high-level description of significant financial management systems included in the scope of the engagement to perform the financial statement audit.

Core Accounting System (CAS)
CAS is the core accounting system that records financial transactions and generates financial statements for the United States Coast Guard. CAS is hosted at the Coast Guard's FINCEN in Virginia, (VA) and is managed by the United States Coast Guard. The FINCEN is the Coast Guard's primary financial system data center. CAS interfaces with other systems located at the FINCEN, including Financial and Procurement Desktop (FPD).

Financial Procurement Desktop (FPD)

The FPD application is used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is hosted at the FINCEN in VA and is and managed by the United States Coast Guard.

Sunflower

Sunflower is a customized third party commercial off the shelf product used for TSA and Federal Air Marshals property management. Sunflower interacts directly with the Office of Finance Fixed Assets module in CAS. Additionally, Sunflower is interconnected to the FPD system and is hosted at the FINCEN in VA and is managed by the United States Coast Guard.

MarkView

MarkView is imaging and workflow software used to manage invoices in CAS. Each invoice is stored electronically and associated to a business transaction so that users are able to see the image of the invoice. MarkView is interconnected with the CAS system and is located at the FINCEN in VA and is managed by the United States Coast Guard.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2011

Appendix B

FY 2011 Notices of IT Findings and Recommendations at TSA

Notice of Findings and Recommendations – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditors Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist the DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Appendix B

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
TSA-IT-11-01	Markview – Password Settings	Access Controls	2	X	
TSA-IT-11-02	Markview – Administrator Account	Access Controls	2	X	
TSA-IT-11-03	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing	Access Controls	1		X
TSA-IT-11-04	TSA Computer Access Agreement Process	Access Controls	1		X
TSA-IT-11-05	Sunflower and Markview User Account Recertifications	Access Controls	2		X
TSA-IT-11-06	Configuration Management Controls Over the Coast Guard Scripting Process	Configuration Management	2		X

APPENDIX C

Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at TSA

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2011

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
TSA-IT-10-01	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		X
TSA-IT-10-02	CAS, FPD, and Sunflower Access Recertifications		X
TSA-IT-10-03	TSA Computer Access Agreement Process		X
TSA-IT-10-04	Configuration Management Controls Over the Coast Guard Scripting Process		X

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2011

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Administrator, TSA
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, TSA
Chief Information Officer, TSA
Chief Information Security Officer
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
DHS GAO/OIG Audit Liaison
Chief Information Officer, Audit Liaison
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

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