Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Transportation Security Administration Component of the FY 2012 Department of Homeland Security Financial Statement Audit

OIG-13-78

April 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

April 18, 2013

MEMORANDUM FOR: Dr. Emma Garrison-Alexander
Chief Information Officer
Transportation Security Administration

David Nicholson
Chief Financial Officer
Transportation Security Administration

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Transportation Security Administration Component of the FY 2012 Department of Homeland Security Financial Statement Audit*

Attached for your action is our final report, *Information Technology Management Letter for the Transportation Security Administration Component of the FY 2012 Department of Homeland Security Financial Statement Audit.* The independent accounting firm KPMG LLP (KPMG) performed the Department of Homeland Security's financial statement audit as of September 30, 2012, and prepared this information technology (IT) management letter.

KPMG is responsible for the attached IT management letter dated December 20, 2012, and the conclusion expressed in it. We do not express an opinion on DHS' financial statements or internal controls or conclusions on compliance with laws and regulations. The DHS management concurred with all recommendations.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Audit Division, at (202) 254-5451.

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

April 4, 2013

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, 2012, and the related statements of net cost, changes in net position, and custodial activity, and combined statement of budgetary resources for the year then ended (referred to as the "fiscal year (FY) 2012 financial statements"). We were also engaged to audit the Department's internal control over financial reporting of the FY 2012 financial statements. The objective of our audit engagement was to express an opinion on the fair presentation of the FY 2012 financial statements and the effectiveness of internal control over financial reporting of the FY 2012 financial statements.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 14, 2012, included internal control deficiencies identified during our audit engagement that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to the Transportation Security Administration (TSA).

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, and contingency planning with respect to TSA's financial systems general IT controls (GITC) which we believe contribute to a DHS Department-wide material weakness in IT controls and financial system functionality. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The comments described herein have been discussed with the appropriate members of management, or communicated through Notices of Findings and Recommendations (NFRs), 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 TSA financial systems within the scope of the FY 2012 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 (OIG) and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS OIG, U.S. Office of Management and Budget, 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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	**1**
Summary of Findings and Recommendations	**2**
General IT Control and Financial System Functionality Findings and Recommendations	**3**
Findings	**3**
Related to IT Financial Systems Controls	**3**
Configuration Management	**3**
Access Controls	**3**
Contingency Planning	**3**
Security Management	**3**
After – Hours Physical Security Testing	**4**
Social Engineering Testing	**4**
Related to Financial System Functionality	**4**
Recommendations	**5**
Application Controls	**6**

APPENDICES

Appendix	Subject	Page
A	Description of Key TSA Financial Systems and IT Infrastructure within the Scope of the FY 2012 DHS Financial Statement Audit	**7**
B	FY 2012 Notices of IT Findings and Recommendations at TSA	**9**
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at Transportation Security Administration	**11**

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit the financial statements of DHS as of and for the year ended September 30, 2012, we performed an evaluation of the general Information Technology (IT) controls (GITCs) at TSA and the U. S. Coast Guard (Coast Guard) (TSA's IT service provider for financial processes), to assist in planning and performing our audit engagement. The Coast Guard Finance Center (FINCEN) hosts key financial applications for TSA. As such, our audit procedures over GITCs 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 (HQ). 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.

FISCAM was designed to inform financial statement 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 statement audit. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of GITCs and the IT 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 GITC 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 and TSA facilities, and focused on test, development, and production devices that directly support TSA's financial processing and key general support systems. Limited social engineering and after-hours physical security testing was also included in the scope of the technical security testing.

In addition to GITC testing, application controls were tested for the year ending September 30, 2012, which were identified as key controls by the financial audit team.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2012, TSA took corrective action to address prior year IT control deficiencies. For example, TSA made improvements over its revalidation of user accounts for certain systems; strengthened password parameters; and ensured administrators had their own unique login id and password. During FY 2012, we continued to identify IT general control deficiencies that impact TSA's financial data. 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 of 1996 (FFMIA).

In FY 2012, our IT audit work identified nine IT findings, of which three were repeat findings from the prior year, and six were new findings. In addition, we determined that TSA remediated three IT findings identified in previous years. These findings represent deficiencies in four of the five FISCAM key control areas. Specifically the deficiencies were:

1. Unverified access controls through the lack of comprehensive user access privilege recertifications;
2. Access control issues involving password complexity settings;
3. Lack of review of audit logs;
4. Poorly designed controls over new user access to the network and an individual financial system;
5. Lack of testing of restoration of backups; and
6. 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 process;
4. Physical security and security awareness issues; and
5. Procedures for role-based training for individuals with elevated responsibilities 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.

GENERAL IT CONTROL AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS AND RECOMMENDATIONS

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following TSA IT and financial system control deficiencies. Our findings are divided into two groupings: 1) financial systems controls and 2) IT system functionality.

Related to IT Financial Systems 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, documented, and tested. 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, and we found inconsistencies of data within the script record documentation existed.

Access Controls

- The Computer Access Agreement process for TSA employees has not been consistently implemented and applied based on TSA policy.
- Access review procedures for one key financial application, Electronic Time Attendance and Scheduling (eTAS), does 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, eTAS, were not configured to enforce password length or complexity.
- New users obtained access to eTAS without all required training completed or new user access forms completed as required by TSA policy.
- Audit logs are not reviewed for inappropriate or unusual activity over eTAS.

Contingency Planning

- Restoration testing of backup media over eTAS is not performed to ensure integrity and reliability of data.

Security Management

- Formalized documented policies do not exist to ensure IT systems are properly evaluated for basic requirements by the appropriate offices and levels of management prior to the system implementation of eTAS.
- 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 HQ.

Exceptions Noted (1)	**Total Exceptions at TSA HQ by Type**
Passwords (2)	6
Keys	1
Personally Identifiable Information (PII) (3)	3
Unlocked Laptop	4
External Drive, Other Media, etc.	2
Total Exceptions at TSA HQ	**16**

(1) There were cases of multiple exceptions in a single workspace, but the type of exception was only noted as 1 exception. For example, one cubicle had multiple passwords, but this was only recorded as 1 exception.
(2) Attempts to login to the systems with the identified passwords were not performed. However, we assumed that the identified passwords were valid passwords. Also includes one password for a debit card account.
(3) Includes one health form containing sensitive PII.

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**
45	15	3

Related to Financial System Functionality:

We noted that financial system functionality limitations are contributing to control deficiencies, 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:

- Financial systems functionality limitations are preventing the TSA from establishing automated processes and application controls that would improve accuracy, reliability, and facilitate efficient processing of certain financial data such as:
  - Maintaining adequate posting logic transaction codes to ensure that transactions are recorded in accordance with generally accepted accounting principles; and
  - Tracking detailed transactions associated with intragovernmental business and eliminating the need for default codes such as Trading Partner Identification Number that cannot be easily researched.

Recommendations:

We recommend that TSA take the following corrective actions:

- Work with the DHS Chief Financial Officer (CFO), DHS Chief Information Officer, and Coast Guard HQ to ensure the following planned corrective actions take place in a timely manner:
  - Continue to provide training and update the procedures and tools if necessary, to better document and review the Test Strategy Field among the script analysts and script approvers to promote consistency.
  - Continue to conduct internal FINCEN Internal Control Branch (ICB) review over the script process, software development life cycle, and configuration management policies and procedures.
- Direct the Information Assurance Division to provide the Financial Management Division's ICB with the Quarterly Delinquency Report for IT Security Awareness Training.
- Direct the ICB to develop an internal control review on the delinquency rate of users who are beyond the 60 day requirement per the TSA Information Assurance Handbook.
- Ensure that Supervisors and Contracting Officer's Representatives within each program office in TSA require each employee and contractor complete IT Security Awareness Training within 60 days of being granted access to information systems, in accordance with the IT Security Policy Handbook.
- Update the eTAS policy to state that license audits will be conducted on a quarterly basis.
- Work with the airports once eTAS has marked its first year to conduct annual account recertifications in order to be in compliance with DHS 4300A.
- Enable the existing password complexity functionality within the eTAS application and require all users to change their passwords to contain a combination of all the following: alphabetic (lowercase and uppercase), numeric and special characters.
- Adhere to the policy regarding KRONOS training certificates and access forms.
- Instruct a TSA contractor to create a log parsing facility for the KRONOS Application logs which will generate a list of User Account changes (Creation, Deletion, Modification of Rights and Privileges) that occurred within the last month. This list of account changes will be compared against the Account Request forms for that month. The review will be conducted by the System Owner or designee.
- Work with the TSA Security Operations Center (SOC) to send all log files from the Windows servers as well as the ETA KRONOS application and web server itself to the TSA SOC where centralized logging, log correlation, audit reduction, real-time review and analysis can be conducted on a regular basis.

- Perform annual testing to ensure the integrity and reliability of the backup media in compliance with DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, the TSA Information Assurance Handbook, and National Institute of Standards and Technology Special Publication 800-53, revision 3.
- Dedicate resources to execute elements of the IT Security Awareness Training program related to social engineering, including conducting internal testing on a quarterly basis, conducting one-on-one training with individuals failing social engineering attempts, taking administrative actions, if needed, on a case-by-case basis in regards to social engineering, and conducting communications campaigns via broadcasts warning against social engineering.
- Ensure during New Employee orientation, the Office of Security will continue to advise new employees to secure their cubicles/offices, to include sensitive information, when not at their cubicles/offices.
- Ensure that when personnel are reassigned, that individual's Business Management Office (BMO) notify the Office of Security of their newly assigned office and floor. This will enable the Office of Security to assign the appropriate access to the employee's Personal Identity Verification (PIV) card and/or provide office keys to an individual with an office.
- Coordinate efforts between the Office of Security and BMOs and/or the office occupant to ensure that individuals authorized to have access to the office besides the office occupant are identified.
- Implement appropriate monitoring controls around personnel separation procedures to ensure that BMOs/Contracting Officer's Technical Representatives consistently notify the Office of Security in a timely manner when individuals depart TSA so that their PIV card access can be terminated.
- Implement appropriate monitoring controls around personnel separation procedures to ensure that limited physical access is granted by Office of Security to authorized personnel only in accordance with an official request.
- Coordinate efforts between the TSA CFO and the TSA Chief Information Security Officer (CISO) to develop a process to communicate potential financial systems to the CISO that would be used to update the Trusted Agent Federal Information Security Management Act tool.
- Implement appropriate monitoring controls around the evaluation of TSA systems and subsequent documentation and management of POA&Ms and auditor-identified weaknesses to ensure that all weaknesses are corrected.
- Coordinate efforts between the TSA CFO and the TSA CISO to ensure that the inventory submitted to the DHS CFO for CFO designated financial systems is complete and accurately represents the current IT environment.

APPLICATION CONTROLS

Application controls were tested for the year ending September 30, 2012, and we found no issues.

Appendix A

Description of Key TSA Financial Systems and IT Infrastructure within the Scope of the FY 2012 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.

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 Coast Guard.

Sunflower

Sunflower is a customized third-party commercial off-the-shelf product used for TSA and Federal Air Marshal Service 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 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 Coast Guard.

Electronic Time Attendance and Scheduling (eTAS)

eTAS is an automated and standardized labor management solution. The system provides an automated means to schedule employee work and leave hours, record hours worked / not worked, and provide bi-weekly time records to TSA's payroll provider, the National Finance Center. The system automates the workforce management process to reduce the amount of time, effort, and associated cost required for entry of data.

Appendix B
FY 2012 Notices of IT Findings and Recommendations at TSA

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2012

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-12-01	Physical Security and Security Awareness Issues identified during enhanced security testing	Access Controls		X
TSA-IT-12-02	Computer Access Agreements	Access Controls		X
TSA-IT-12-03	eTAS User Account Recertification	Access Controls	X	
TSA-IT-12-04	eTAS User Passwords	Access Controls	X	
TSA-IT-12-05	eTAS Restoration Testing of Media Backups	Contingency Planning	X	
TSA-IT-12-06	eTAS Audit Logs	Access Controls	X	
TSA-IT-12-07	eTAS System User Access	Access Controls	X	
TSA-IT-12-08	Configuration Management Controls Over the Coast Guard Scripting Process	Configuration Management		X
TSA-IT-12-09	eTAS Pre-Implementation Deficiencies	Security Management	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, 2012

NFR No.	Description	Disposition	
		Closed	Repeat
TSA-IT-11-01	Markview – Password Settings	X	
TSA-IT-11-02	Markview – Administrator Account	X	
TSA-IT-11-03	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		X
TSA-IT-11-04	TSA Computer Access Agreement Process		X
TSA-IT-11-05	Sunflower and Markview User Account Recertifications	X	
TSA-IT-11-06	Configuration Management Controls Over the Coast Guard Scripting Process		X

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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