Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Transportation Security Administration Component of the FY 2013 Department of Homeland Security Financial Statement Audit

OIG-14-97

May 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 28, 2014

MEMORANDUM FOR: Stephen Rice
Chief Information Officer
Transportation Security Administration

David Nicholson
Chief Financial Officer
Transportation Security Administration

FROM: [redacted]ne
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Transportation Security Administration Component of the FY 2013 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the Transportation Security Administration of the FY 2013 Department of Homeland Security Financial Statement Audit.* This report contains comments and recommendations related to information technology internal control deficiencies that were not required to be reported in the Independent Auditors' Report.

We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit of Department of Homeland Security fiscal year 2013 consolidated financial statements. The contract required that KPMG perform its audit according to generally accepted government auditing standards and guidance from the Office of Management and Budget and the Government Accountability Office. KPMG is responsible for the attached management letter dated March 11, 2014, and the conclusion expressed in it.

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

Attachment

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

March 11, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Department of Homeland Security Transportation Security Administration

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated December 11, 2013, included internal control deficiencies identified during our audit 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 we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and communicated through Notices of Findings and Recommendations (NFRs), are intended to improve internal control or result in other operating efficiencies and are summarized as described below.

With respect to TSA's financial systems' IT controls, we noted certain matters in the areas of security management, access controls, and contingency planning. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The Table of Contents identifies each section of the letter. We have provided a description of key TSA financial systems and IT infrastructure within the scope of the FY 2013 DHS financial statement audit in Appendix A, and a listing of each IT NFR communicated to management during our audit in Appendix B.

During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of DHS' organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"). In connection with our audit of the FY 2013 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and IT application controls at the Transportation Security Administration (TSA) to assist in planning and performing our audit engagement.

Scope

The scope of our GITC and IT application control test work is described in Appendix A, which provides a description of the key TSA financial systems and IT infrastructure within the scope of the TSA component of the FY 2013 DHS consolidated financial statement audit.

Approach

General Information Technology Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office, formed the basis of our GITC evaluation procedures.

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 categories to be essential to the effective operation of GITCs and the IT environment:

- *Security Management* – 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* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.

- *Configuration Management* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.

    - We performed technical information security testing for key TSA network and system devices. The technical security testing was performed from within select DHS facilities and focused on production devices that directly support DHS' and TSA's financial processing and key general support systems.

- *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.

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

IT Application Controls

We performed testing over selected key IT application controls on financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions. FISCAM defines application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS

During FY 2012, TSA took corrective action to address certain prior year IT control deficiencies. For example, TSA made improvements over configuration management controls relative to the scripting process. However, during FY 2013, we continued to identify GITC deficiencies related to controls over security management (including deficiencies over physical security and security awareness), access control, and contingency planning for TSA core financial and feeder systems.

Collectively, the IT control deficiencies limited TSA‘s ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted the internal controls over TSA financial reporting and its operations. In addition, based upon the results of our test work, we noted that TSA contributes to the Department's non-compliance with the relevant federal financial management systems requirements of the *Federal Financial Management Improvement Act of 1996.*

Of the seven IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, all were repeat findings, either partially or in whole from the prior year. The seven IT NFRs issued represent deficiencies in three of the five FISCAM GITC categories.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, requirements and National Institute of Standards and Technology (NIST) guidance. Specifically, the findings stem from:

1. Inadequately designed and ineffective access control policies and procedures relating to the management of logical access to financial applications, databases, and support systems;
2. Insufficient logging of system events and monitoring of audit logs; and
3. Inconsistently implemented backup management controls.

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 TSA financial data used by management and reported in TSA's and DHS' 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 FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following TSA GITC deficiencies.

Security Management

After-Hours Physical Security Testing

On September 4, 2013, we performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to printed or electronic media, equipment, or credentials residing within a TSA employee's or contractor's work area or shared workspaces which could be used by others to gain unauthorized access to systems housing financial or other sensitive information. The testing was performed at a TSA facility in Arlington, Virginia (VA) that processes, maintains, and/or has access to financial data.

We observed 17 instances where passwords, sensitive IT information (such as server names or IP addresses), keys, unsecured or unlocked external media, and printed materials containing sensitive Personally Identifiable Information were accessible by individuals without a "need to know".

Social Engineering

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.

On July 11, 2013, we performed social engineering testing from a DHS facility to identify risks related to TSA personnel awareness of responsibilities for protecting sensitive IT information, including personal system access credentials, from disclosure to unauthorized personnel. We noted two instances where individuals divulged their TSA network account password to KPMG auditors.

Access Controls

- DHS requirements for password complexity were not fully implemented for accounts on the Electronic Time Attendance and Scheduling application (eTAS).

- Audit logs for components of the eTAS environment (including the operating system and database) and supporting system software were not consistently reviewed by management, and audit logs for the eTAS application do not include activity related to changes to user accounts and associated profiles, in accordance with DHS and TSA policy.

- eTAS account management activities, including enforcement of training requirements, implementation of account inactivity controls, authorization of new or modified application access, and periodic recertification of access, were not consistently or timely documented or implemented in accordance with DHS and TSA policy.

Contingency Planning

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

Recommendations

We recommend that the TSA Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO), in coordination with the DHS OCIO and the DHS OCFO**,** make the following improvements to TSA‘s financial management systems and associated IT security program.

Security Management

- Develop and deliver training and awareness materials to TSA staff and supervisors to address IT security policies and procedures related to properly securing sensitive DHS and TSA data within physical workspaces, initiate periodic after-hours reviews of TSA workspaces, and implement appropriate TSA policies and guidance in addressing identified security violations.

- Continue existing implementation of TSA’s IT Security Awareness Training Program, including performing periodic internal social engineering testing, delivering individualized training and implementing administrative actions, as appropriate, and communicating reminders concerning social engineering risks and awareness.

Access Controls

- Implement technical controls to ensure that passwords for eTAS accounts are configured in accordance with DHS. If necessary and justified by operational and business requirements, ensure that documented requests for exceptions from DHS password requirements identify all affected accounts subject to deviations from standard control requirements and follow established processes for DHS exceptions.

- Implement technical and monitoring controls to ensure that eTAS operating system and database audit logs include all required auditable events, are being reviewed by management on a periodic basis, are documented, and audit log review evidence is maintained in accordance with DHS and TSA requirements.

- Implement technical controls to enforce DHS and TSA requirements related to implementation of account inactivity controls.

- Implement monitoring controls over the account management process to ensure that all users are granted access to eTAS, including timely completion of required training and documentation of access authorizations, and that all accounts are recertified no less than annually, in accordance with DHS and TSA requirements.

Contingency Planning

- Perform and document annual testing to ensure the integrity and reliability of eTAS backup media in accordance with DHS and TSA requirements and NIST minimum baseline control guidance.

IT APPLICATION CONTROLS

We conducted testing over certain Core Accounting System (CAS), Financial Procurement Desktop (FPD), and Sunflower application controls supporting in-scope processes during the TSA component of the FY 2013 DHS financial statement audit and did not identify any control deficiencies.

Appendix A

Description of Key TSA Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit

Below is a description of significant TSA financial management systems and supporting IT infrastructure included in the scope of the TSA component of the DHS FY 2013 financial statement audit.

Core Accounting System (CAS)

CAS is the core accounting system that records financial transactions and generates financial statements for TSA. CAS is hosted at the U.S. Coast Guard Financial Center (FINCEN) in VA. CAS interfaces with other systems located at the FINCEN, including FPD and Sunflower. CAS is used by financial management individuals as CAS is the main system of record for financial information. CAS is comprised of a Hewlett-Packard (HP) UNIX operating system and an Oracle database.

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 interfaces with the CAS system and is hosted at the FINCEN in VA. FPD is comprised of an HP UNIX operating system and an Oracle database.

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 and interfaces with the FPD system. Sunflower is hosted at the FINCEN in VA. Sunflower is comprised of a Red Hat Linux operating system and an Oracle database.

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 and 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. eTAS is comprised of a Windows 2003 operating system and an Oracle database, and is located at the DHS Enterprise Data Center in VA. The Office of Human Capital is responsible for eTAS.

Appendix B

FY 2013 IT Notices of Findings and Recommendations at TSA

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-13-01	Weakness in eTAS user recertification	Access Controls		X
TSA-IT-13-02	Weakness in eTAS password complexity	Access Controls		X
TSA-IT-13-03	Weakness in eTAS Restoration Testing of Backups	Contingency Planning		X
TSA-IT-13-04	Weakness in eTAS review of audit logs	Access Controls		X
TSA-IT-13-05	eTAS System User Access	Access Controls		X
TSA-IT-13-06	Security Awareness Issues Identified During Social Engineering Testing at TSA Headquarters	Security Management		X[1]
TSA-IT-13-07	Physical Security and Security Awareness Issues Identified During After Hours Testing at TSA Headquarters	Security Management		X1

[1] FY 2012 NFR TSA-IT-12-01 was split into two findings for FY 2013 to report separately on the results of each set of enhanced information security testing procedures performed at TSA.

Appendix A
Report Distribution

Department of Homeland Security

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

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@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:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

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