Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit – Office of Financial Management and Office of Chief Information Officer

OIG-14-108

June 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 24, 2014

MEMORANDUM FOR: Luke McCormack
Chief Information Officer

Chip Fulghum
Acting Chief Financial Officer

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit – Office of Financial Management and Office of Chief Information Officer*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit – Office of Financial Management and Office of Chief Information Officer.* 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,
Chief Information Officer and Chief Financial Officer,
U.S. Department of Homeland Security

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 Office of Financial Management (OFM) and the Office of the Chief Information Officer (OCIO).

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 OFM's and OCIO'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.

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

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of the Chief Information Officer
September 30, 2013

TABLE OF CONTENTS

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 DHS Office of the Chief Financial Officer (OCFO) Office of Financial Management (OFM) and the DHS Office of the Chief Information Officer (OCIO) to assist in planning and performing our audit engagement.

Scope

DHS Treasury Information Executive Repository (DHSTIER) is the system of record for the DHS consolidated financial statements and is used to track, process, and perform validation and edit checks against monthly financial data uploaded from each of the DHS components' core financial management systems. DHSTIER is administered jointly by the OCFO Resource Management Transformation Office and the OCFO OFM and is hosted on the DHS OneNet at the Stennis Data Center in Mississippi.

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.

    - In conjunction with our test work of security management GITCs, limited after-hours physical security testing at select OFM and OCIO facilities was conducted to identify potential control deficiencies in non-technical aspects of IT security.

- *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.

- *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.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Summary

During FY 2012, OFM and OCIO took corrective action to address certain prior year IT control deficiencies. For example, OFM and OCIO made improvements over strengthening controls around system security authorization and configuration management. However, during FY 2013, we continued to identify GITC deficiencies that could potentially impact DHS' financial data related to controls over security management, access control, and contingency planning for DHS' core financial system.

Collectively, the IT control deficiencies limited DHS' 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 DHS' financial reporting and its operations.

Of the four IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, two were repeat findings from the prior year, and two were new findings. The four IT NFRs issued represent deficiencies in three of the five FISCAM GITC categories.

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

While the recommendations made by us should be considered by DHS, it is the ultimate responsibility of DHS management to determine the most appropriate method(s) for addressing the deficiencies identified.

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following OFM and OCIO GITC control deficiencies.

Security Management

After-Hours Physical Security Testing

On June 19, 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 DHS 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 DHS facility in Washington, DC, that processes, maintains, and/or has access to financial data.

We observed 40 instances where passwords, sensitive IT information (such as server names or IP addresses), unsecured or unlocked credit cards and laptops, and printed materials marked "For Official Use Only" or containing sensitive personally identifiable information were accessible by individuals without a "need to know".

Access Controls

- Physical access to the interior rooms within DHS Enterprise Data Centers DC-1 and DC-2 hosting key DHS financial systems was not consistently recertified.

Contingency Planning

- DHSTIER backup logs were not consistently maintained or rotated to an offsite storage facility.

Recommendations

We recommend that the DHS OCIO and DHS OCFO**,** make the following improvements to DHS' financial management systems and associated IT security program.

Security Management

- Continue to conduct DHS security awareness training and increase monitoring activities to enforce compliance with the criteria established by the DHS rules of behavior related to safeguards against unauthorized physical access of sensitive DHS information.

Access Controls

- Fully define and document responsibility for, and consistently implement controls related to the periodic review of physical access to the interior rooms within DC-1 and DC-2 hosting key DHS financial systems.

Contingency Planning

- Continue to sustain the corrective action implemented during FY 2013 to enforce existing policies and procedures related to DHSTIER backups to ensure that logs are consistently maintained and rotated to an offsite storage facility.

IT APPLICATION CONTROLS

We conducted testing over certain DHSTIER application controls supporting in-scope processes during the OFM and OCIO component of the FY 2013 DHS financial statement audit and did not identify any control deficiencies.

FY 2013 IT NOTICES OF FINDINGS AND RECOMMENDATIONS AT OFM AND OCIO

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-13-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at DHS	Security Management		X
OCIO-IT-13-01	Inadequate Recertification of DC-2 Physical Access	Access Controls		X
OCIO-IT-13-02	Backup Log Rotation Not Consistently Performed	Contingency Planning	X	
OCIO-IT-13-03	Inadequate Recertification of DC-1 Physical Access	Access Controls	X	

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.