Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the USCIS Component of the FY 2013 DHS Financial Statement Audit

OIG-14-80

April 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 25, 2014

MEMORANDUM FOR: Mark Schwartz
Chief Information Officer
United States Citizenship and Immigration Services

Joseph Moore
Chief Financial Officer
United States Citizenship and Immigration Services

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

SUBJECT: *Information Technology Management Letter for the United States Citizenship and Immigration Services 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 United States Citizenship and Immigration Services Component 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, U.S. Citizenship and Immigration Services

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 U.S. Citizenship and Immigration Services (USCIS).

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 USCIS' financial systems' IT controls, we noted certain matters in the areas of security management, access controls, configuration management, segregation of duties, 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 USCIS 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

Department of Homeland Security
Information Technology Management Letter
U.S. Citizenship and Immigration Services
September 30, 2013

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 U.S. Citizenship and Immigration Services (USCIS) 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 USCIS financial systems and IT infrastructure within the scope of the USCIS 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.
    - In conjunction with our test work of security management GITCs, limited after-hours physical security testing and social engineering at select USCIS 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.

- We performed technical information security testing for key USCIS 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 USCIS' 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, USCIS took corrective action to address certain prior year IT control deficiencies. For example, USCIS made improvements over strengthening controls around security awareness training compliance and privileged system access monitoring. 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 configuration management for the USCIS core financial system and associated General Support System environments.

Collectively, the IT control deficiencies limited USCIS' 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 USCIS' internal controls over financial reporting and its operations. We consider these deficiencies, in aggregate, to contribute to the IT 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 USCIS contributes to the Department's non-compliance with the relevant federal financial management systems requirements of the *Federal Financial Management Improvement Act of 1996*, mainly because USCIS' application tracking systems are not designed to support the financial reporting process.

Of the five IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, four were repeat findings, either partially or in whole from the prior year, and one was a new finding. The five 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 guidance. Specifically, the findings stem from inadequately designed and ineffective access control policies and procedures relating to the management of logical access to financial applications, databases, and support systems; and patch, configuration, and vulnerability management control deficiencies within systems.

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

While the recommendations made by us should be considered by USCIS, it is the ultimate responsibility of USCIS 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 USCIS GITC deficiencies that, in the aggregate, contribute to the IT material weakness at the Department level.

Security Management

After-Hours Physical Security Testing

On August 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 USCIS 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 USCIS facility in Washington, DC, that processes, maintains, and has access to financial data.

We observed 24 instances where passwords, sensitive IT information (such as server names or IP addresses), unsecured or unlocked laptops and external media, and printed materials marked "For Official Use Only" or 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 17, 2013, we performed social engineering testing from a DHS facility to identify risks related to USCIS personnel awareness of responsibilities for protecting sensitive IT information, including personal system access credentials, from disclosure to unauthorized personnel. We noted eight instances where individuals divulged their Federal Financial Management System (FFMS) application account password to KPMG auditors.

Access Controls

- Account management activities on FFMS, including revocation of access from separated or transferred Federal employees and contractors, were not consistently or timely documented or implemented in accordance with DHS and USCIS policy.

- DHS requirements for password complexity were not fully implemented for accounts on the USCIS network.

Configuration Management

- Security patch management and configuration deficiencies were identified during the vulnerability assessment on hosts supporting FFMS.

Recommendations

We recommend that the USCIS 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 USCIS's financial management systems and associated IT security program.

Configuration Management

- Continue to monitor the Service Provider's efforts to remediate and implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during our vulnerability assessment.

Security Management

- Develop and implement monitoring controls to assess employee compliance with information, physical, and privacy security policies with respect to protecting personal system access credentials from disclosure to unauthorized personnel.

- Enhance information, physical, and privacy security awareness efforts to remind employees of responsibilities to protect government data and equipment, and develop and implement a process to conduct periodic after-hours reviews of USCIS workspaces to assess compliance with information, physical, and privacy security policies.

Access Controls

- Implement monitoring controls over the exit clearance process to ensure that all separated and transferred Federal employees and contractors' access to USCIS systems is revoked in a timely manner in accordance with USCIS and DHS requirements.

- Implement technical controls to ensure that passwords for accounts on the USCIS network are configured in accordance with DHS requirements.

IT APPLICATION CONTROLS

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

Appendix A

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

Department of Homeland Security
Information Technology Management Letter
U.S. Citizenship and Immigration Services
September 30, 2013

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

Federal Financial Management System (FFMS)

FFMS is a CFO designated financial system and certified software application that conforms to Office of Management and Budget Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS is a commercial off-the-shelf (COTS) financial reporting system, which has an IBM z/OS operating system and an Oracle database. It includes the core system used by accountants, FFMS Desktop that is used by end-users, and a National Finance Center payroll interface. The FFMS mainframe component and servers are hosted at the DHS Enterprise Data Center located in Virginia (VA). U.S. Immigration and Customs Enforcement is the system owner and manages FFMS for USCIS.

USCIS Network (CIS1)

CIS1 is the Active Directory Domain Services Platform used within the USCIS that contains all of USCIS's Active Directory and Exchange resources. CIS1 is a part of the Enterprise Infrastructure Services accreditation boundary and all Active Directory information, including the Active Directory database itself, is hosted on specified servers called Domain Controllers. These 52 Active Directory Domain Controllers are located throughout the country, with the majority of them being located in VA and Nebraska.

Appendix B

FY 2013 IT Notices of Findings and Recommendations at USCIS

Department of Homeland Security
Information Technology Management Letter
U.S. Citizenship and Immigration Services
September 30, 2013

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-13-01	Security Awareness Issues Identified During Social Engineering Testing at USCIS	Security Management		X
CIS-IT-13-02	Deficiencies in transferred/terminated employee exit processing	Access Controls		X
CIS-IT-13-03	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-13-04	Weakness in CIS1 Password Complexity	Access Controls	X	
CIS-IT-13-05	FFMS Vulnerability Weaknesses Impact USCIS Operations	Configuration Management		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.