Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Citizenship and Immigration Services Component of the FY 2012 Department of Homeland Security Financial Statement Audit

OIG-13-81

April 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 24, 2013

MEMORANDUM FOR: Mark Schwartz
Chief Information Officer
U.S. Citizenship and Immigration Services

Joseph Moore
Chief Financial Officer
nd Immigration Services

FROM: [signature]
r General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Citizenship and Immigration Services 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 Citizenship and Immigration Services 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 (DHS) 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.

Attachment

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
U.S. Citizenship and Immigration Services

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

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, and segregation of duties with respect to USCIS' 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 USCIS financial systems and IT infrastructure 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 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 (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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our financial statement audit 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 USCIS to assist in planning and performing our audit. The DHS Immigration and Customs Enforcement (ICE) hosts a key financial application for USCIS. As such, our audit procedures over GITCs for USCIS included testing of ICE's Federal Financial Management System (FFMS) policies, procedures, and practices, as well as USCIS policies, procedures and practices at USCIS' Headquarters.

Federal Information System Control Audit Manual (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 or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.

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

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

- *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 procedures, we assessed corrective actions implemented to address prior year findings over technical security testing for key network and system devices and key financial application controls in the ICE environment. In addition, we enhanced our GITC scope to include additional vulnerability testing at USCIS.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2012, USCIS initiated corrective action plans to address some prior year IT control deficiencies. As a result, improvement was made in the area of effective password configurations over two financial systems. In addition, we continued to identify GITC deficiencies that could potentially impact USCIS's financial data. The most significant findings were related to the FFMS configuration and patch management, and deficiencies in security awareness. Collectively, the IT control deficiencies limited USCIS'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 control deficiencies negatively impacted the internal controls over USCIS' financial reporting and its operations 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 ICE contributes to the DHS' noncompliance with the requirements of the *Federal Financial Management Improvement Act of 1996*.

Of the 19 findings identified during our FY 2012 testing, eight were new IT findings. These findings represent control deficiencies in four of the five FISCAM key control areas: configuration management, access controls, segregation of duties, and security management. Specifically, these control deficiencies include:

1. A lack of audit logging within the financial applications;
2. Security management issues involving staff security training and exit processing procedure weaknesses;
3. Inadequately designed and operating configuration management; and
4. The lack of effective segregation of duties controls within the network and a financial application.

These control 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 financial data used by management as reported in DHS' consolidated 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 weaknesses identified.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following USCIS GITC control deficiencies that in the aggregate contribute to the IT material weakness at the Department level.

Configuration Management

- Security configuration management over FFMS included several configuration and patch management weaknesses with the configuration of the FFMS Oracle databases, FFMS servers, and Cisco routers and switches.

Access Controls

- The following account management control deficiencies over CIS1, CLAIMS 3 Local Area Network (LAN), and CLAIMS 4:
  - Lack of recertification of CLAIMS 3 LAN/CLAIMS 4 system users and CIS 1 network administrators.
  - User access is not documented and maintained for CLAIMS 4.
  - Temporary users for the CIS1 network did not obtain supervisory approval.
  - Lack of policies and procedures for separated CLAIMS 3 LAN user accounts.
- Lack of processes in place for sanitization of equipment and media.
- Audit logs are not captured for CLAIMS 4. However, audit logs are captured for CLAIMS 3 LAN; yet, USCIS has not implemented a process to review the logs on a periodic basis.
- Visitor access to the Vermont Service Center (VSC) was not appropriately controlled.

Segregation of Duties

- CIS1 network administrator access privileges were not appropriately segregated. Thirty-nine administrators retained access to one or more administrator access groups, which is not required to perform administrator job functions.
- Segregation of duties controls over CLAIMS 3 LAN user roles has not been established.

Security Management

- Procedures for transferred/terminated personnel exit processing have not been fully implemented.
- Lack of Computer Security Awareness Training compliance.
- Role-based IT Security training is not monitored.

- Two financial systems failed to obtain Authority to Operate (ATO) for several quarters of the fiscal year:

  Sixteen high risk vulnerabilities were identified in CLAIMS 4.

  Forty-two high risk vulnerabilities were identified in CLAIMS 3 LAN.

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 included physical access to media and equipment that housed financial data and information residing within an USCIS employee's or contractor's work area, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at the USCIS headquarters location that processes and/or maintains financial data. The specific results are listed as shown in the following table:

Exceptions Noted	Exceptions Noted at 111 Mass. Ave – Lower Level	Exceptions Noted at 111 Mass. Ave – 5th Floor
Passwords	21	21
For Official Use Only	3	12
Keys	5	3
Personally Identifiable Information	8	8
Unlocked Laptop	1	4
Server Names/IP Addresses	2	5
Credit Cards	3	1
Total Exceptions at USCIS	**43**	**54**

Additionally, KPMG was able to access the facility by providing an expired non- DHS government badge to the security guard.

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 deception for the purpose of information gathering, or gaining computer system access, as shown in the following table:

Total Called	Total Answered	Number of people who provided a username and/or password
45	15	3 – Both User Name and Password

Recommendations:

We recommend that the USCIS Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the DHS Office of Chief Financial Officer (OCFO) and the DHS Office of the Chief Information Officer (OCIO), make the following improvements to USCIS's financial management systems and associated information technology security program.

Configuration Management

Unless specifically noted where USCIS needs to take specific corrective action, we recommend that the USCIS CIO and CFO, in coordination with the ICE OCFO and the ICE OCIO, make the following improvements to ICE's information technology:

- Examine the default configuration installations and system services installed on FFMS network devices and remove unnecessary system services.
- Ensure that password configuration settings are properly and effectively applied.
- Assess the patch deployment and testing processes and develop a process for patching applications across the enterprise.
- Implement appropriate FFMS database and network server patches and configuration baseline parameters consistent with DHS guidelines.

We recommend that USCIS:

- Monitor the ICE Mission Action Plan for the FFMS vulnerabilities that impact USCIS operations.

Access Controls

- Develop, approve, and implement access control policies and procedures to ensure that CLAIMS 3 LAN, CIS 1 and CLAIMS 4 system administrator and user accounts are documented, approved, and recertified annually.
- Develop, approve, and implement access control policies and procedures to ensure that management of equipment and media is in accordance with National Institute of Standards and Technology guidance.
- Ensure that access is removed for separated CLAIMS 3 LAN accounts upon departure from the agency.
- Finalize the audit and accountability policy and procedures which enforce regular review of system activity logs.
- Update VSC physical security policies and procedures to stipulate the requirements of visitor entry to sensitive facilities.

Segregation of Duties

- Complete the account recertification process on CIS1 system/domain administrator accounts.

- Develop, authorize, and implement procedures and operations manuals for CLAIMS 3 LAN segregation of duties.

Security Management

- Monitor the implementation plan to assure the exit clearance procedures have been implemented for Federal employees and contractors.
- Finalize the implementation of the Information Security Training Program and ensure all USCIS employees receive information security training commensurate to their job duties and in compliance with Federal regulations.
- Develop and enforce policies and procedures to ensure that staffs are complying with information, physical, and privacy security policies.

USCIS obtained an ATO for CLAIMS 3 LAN in March 2012 and CLAIMS 4 in July 2012. Therefore, no recommendation will be provided for the ATO weaknesses.

APPLICATION CONTROLS

As a result of the GITC control deficiencies noted above, manual compensating controls were tested in place of application controls.

Appendix A

Description of Key USCIS Financial Systems and IT Infrastructure within the Scope of the FY 2012 DHS Financial Statement Audit

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 2012 financial statement audit.

CLAIMS 3 Local Area Network (LAN)

CLAIMS 3 LAN provides USCIS with a decentralized, geographically dispersed LAN based mission support case management system, with participation in the centralized CLAIMS 3 mainframe data repository. CLAIMS 3 LAN supports the requirements of the Direct Mail Phase I and II, Immigration Act of 1990 (IMMACT 90) and USCIS forms improvement projects. The CLAIMS 3 LAN is located at the following service centers and district offices: Nebraska, California, Texas, Vermont, Baltimore District Office, National Business Center, and Administrative Appeals Office. CLAIMS 3 LAN interfaces with the following systems:

- Citizenship and Immigration Services Centralized Oracle Repository
- CLAIMS 3 Mainframe
- Integrated Card Production System
- CLAIMS 4
- E-filing
- Benefits Biometric Support System
- Refugee, Asylum, and Parole System
- National File Tracking System
- Integrated Card Production System
- Customer Relationship Interface System
- USCIS Enterprise Service Bus

CLAIMS 4

The purpose of CLAIMS 4 is to track and manage naturalization applications. Claims 4 is a client/server application. The central Oracle Database is located in Washington, DC while application servers and client components are located throughout USCIS service centers and district offices. CLAIMS 4 interfaces with the following systems:

- Central Index System (CIS)
- Reengineered Naturalization Automated Casework System
- CLAIMS 3 LAN and Mainframe
- Refugee, Asylum, and Parole System
- Enterprise Performance Analysis System
- National File Tracking System
- Asylum Pre-Screening System

- USCIS Enterprise Service Bus
- Biometrics Benefits Support System
- Enterprise Citizenship and Immigration Service Centralized Operational Repository
- Customer Relationship Interface System
- FD 258 Enterprise Edition and Mainframe
- Site Profile System

Federal Financial Management System (FFMS)

The FFMS is a CFO designated financial system and certified software application that conforms to OMB 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 financial reporting system. It includes the core system used by accountants, FFMS Desktop that is used by average users, and a National Finance Center payroll interface. The FFMS mainframe component and 14 servers are hosted at the DHS DC2 facility located in Virginia. FFMS currently interfaces with Treasury, BMIS Web, and FedTraveler.

CIS1 Network

The USCIS network, also known as 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 Virginia and Nebraska.

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

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-12-01	Policies and Procedures for CLAIMS 3 LAN and CLAIMS 4 Audit Logs	Access Controls		X
CIS-IT-12-02	Inadequate Access Request Forms for CLAIMS 4 System Users	Access Controls		X
CIS-IT-12-03	Weak Logical Access Controls exist over CLAIMS 4	Access Controls		X
CIS-IT-12-04	Security Awareness Issues Identified during After-Hours Walkthrough	Security Management	X	
CIS-IT-12-05	Lack of Segregation of Duties for CLAIMS 3 LAN	Access Controls		X
CIS-IT-12-06	Periodic User Access Reviews are not Performed for CLAIMS 3 LAN Users	Access Controls		X
CIS-IT-12-07	FFMS Vulnerability Weaknesses Impact USCIS Operations	Configuration Management		X
CIS-IT-12-08	Security Awareness Issues were Identified during Social Engineering	Security Management	X	
CIS-IT-12-09	Procedures for Transferred/Terminated Personnel Exit Processing are not Finalized	Access Controls		X
CIS-IT-12-10	Lack of Policies and Procedures for Separated CLAIMS 3 LAN Accounts	Access Controls		X
CIS-IT-12-11	Equipment and Media Policies and Procedures are not Current	Access Controls		X
CIS-IT-12-12	Lack of Computer Security Awareness Training Compliance	Security Management		X
CIS-IT-12-13	Lack Role-Based Training for Key Security Personnel	Security Management		X
CIS-IT-12-14	Lack of ATO for CLAIMS 3 LAN	Security Management	X	
CIS-IT-12-15	Lack of ATO for CLAIMS 4	Security Management	X	
CIS-IT-12-16	Lack of Segregation of Duties Controls Exist over CIS 1	Segregation of Duties	X	
CIS-IT-12-17	Visitor Access Controls are Inadequate at the VSC	Access Controls	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-12-18	Inadequate CIS 1 Access Request Forms for Temporary Users	Access Controls	X	
CIS-IT-12-19	Incomplete Recertification for CIS 1 Network Administrators	Access Controls	X	

Appendix C

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

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2012

NFR #	Description	Disposition	
		Closed	Repeat
CIS-IT-11-01	Equipment and media policies and procedures are not current		X
CIS-IT-11-02	Weak password configuration controls for CLAIMS 4	X	
CIS-IT-11-03	Policies and procedures for CLAIMS 3 LAN and CLAIMS 4 audit logs		X
CIS-IT-11-04	Policies and procedures for separated CLAIMS 3 LAN accounts		X
CIS-IT-11-05	Periodic user access reviews are not performed for CLAIMS 3 LAN users		X
CIS-IT-11-06	Procedures for transferred/terminated personnel exit processing are not finalized		X
CIS-IT-11-07	Incomplete or inadequate access request forms for CLAIMS 3 LAN and CLAIMS 4 system users		X
CIS-IT-11-08	ICE resource server and inadequate patch management weaknesses impact USCIS operations	X	
CIS-IT-11-09	Weak password configuration controls for CLAIMS 3 LAN	X	
CIS-IT-11-10	Weak logical access controls exist over CLAIMS 4		X
CIS-IT-11-11	Ineffective safeguards over physical access to sensitive facilities and resources	X	
CIS-IT-11-12	VPN access request forms are not properly maintained	X	
CIS-IT-11-13	Lack of Segregation of Duties for CLAIMS 3 LAN		X
CIS-IT-11-14	ADEX access request forms are not properly maintained	X	
CIS-IT-11-15	Lack of Computer Security Awareness Training Compliance		X
CIS-IT-11-16	Lack role-based training for key security personnel		X
CIS-IT-11-17	FFMS Vulnerability Weaknesses effect USCIS Operations		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
Acting 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 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.