Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2011 DHS Financial Statement Audit

OIG-12-56

March 2012

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

March 20, 2012

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This report presents the information technology (IT) management letter for the U.S. Citizenship and Immigration Services (USCIS) component of the fiscal year (FY) 2011 DHS consolidated financial statement audit as of September 30, 2011. It contains observations and recommendations related to information technology internal control weaknesses that were summarized in the *Independent Auditors' Report* dated November 11, 2011 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at the USCIS component in support of the DHS FY 2011 consolidated financial statement audit and prepared this IT management letter. KPMG is responsible for the attached IT management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

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

February 17, 2012

Acting 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, 2011 and the related statement of custodial activity for the year then ended (referred to herein as the "fiscal year (FY) 2011 financial statements"). The objective of our audit was to express an opinion on the fair presentation of these financial statements. We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended, based on the criteria established in Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Internal Control*, Appendix A. In connection with our audit, we also considered DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the FY 2011 financial statements.

Our *Independent Auditors' Report* issued on November 11, 2011, describes a limitation on the scope of our audit that prevented us from performing all procedures necessary to express an unqualified opinion on DHS' FY 2011 financial statements and internal control over financial reporting. In addition, the FY 2011 DHS *Secretary's Assurance Statement* states that the Department was unable to provide assurance that internal control over financial reporting was operating effectively at September 30, 2011.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 11, 2011, included internal control deficiencies identified during our audit, that individually, or in aggregate, represented a material weakness or a significant deficiency. This letter represents the separate limited distribution report mentioned in that report.

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to DHS' financial systems general Information Technology (IT) controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. We also noted that in some cases, financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also described in the *General IT Control Findings and Recommendations* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), 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 DHS financial systems within the scope of the FY 2011 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 and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General (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

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2011

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our audit of DHS' balance sheet as of September 30, 2011 and the related statement of custodial activity for the year then ended, we performed an evaluation of general information technology controls (GITC) at USCIS, to assist in planning and performing our audit. The DHS – Immigration and Customs Enforcement (ICE) hosts key financial applications for USCIS. As such, our audit procedures over information technology (IT) general controls for USCIS included testing of the ICE's Active Directory\Exchange (ADEX) network and the Federal Financial Management System (FFMS) policies, procedures, and practices, as well as USCIS policies, procedures and practices at USCIS Headquarters.

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 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 audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the GITC 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 also performed technical security testing for key network and system devices, as well as testing over key financial application controls in the ICE environment. The technical security testing was performed both over the Internet and from within select ICE facilities, and focused on test, development, and production devices that directly support USCIS general support systems.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2011, USCIS initiated corrective action plans to address some prior year IT control deficiencies. As a result, improvement was made in the area of effective safeguards over physical access to sensitive facilities and resources. In addition, we continued to identify general IT control deficiencies that could potentially impact USCIS's financial data. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System (FFMS) and ICE's ADEX configuration and patch management, and deficiencies within the personnel exit clearance process. 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 (AICPA). 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* (FFMIA).

Of the 17 findings identified during our FY 2011 testing, four 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 strong password management and 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 financial applications. 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 KPMG should be considered by USCIS, it is the responsibility of USCIS management to ultimately determine the most appropriate method(s) for addressing the control deficiencies identified based on their system capabilities and available resources.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2011 DHS financial statement audit, we identified the following USCIS IT and financial system control deficiencies that in the aggregate contribute to the material weakness at the Department level.

Configuration Management

- Security configuration management control deficiencies on ADEX. These control deficiencies included inadequate patch management and default installation and configurations on the Cisco routers.
- 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 Control

- The following account management control deficiencies over ADEX, CLAIMS 3 LAN, and CLAIMS 4:
    - The lack of recertification of CLAIMS 3 LAN and CLAIMS 4 system users.
    - User access is not documented and maintained for ADEX, CLAIMS 3 LAN, and CLAIMS 4.
    - CLAIMS 3 LAN and CLAIMS 4 password configurations do not meet DHS requirements.
    - Lack of policies and procedures for separated CLAIMS 3 LAN user accounts.
- Lack of processes in place for sanitization of equipment and media.
- Lack of policies and procedures for maintaining and reviewing CLAIMS 3 LAN and CLAIMS 4 audit logs.
- The lack of recertification of individuals with physical access to the Technology Engineering Consolidation Center (TECC).
- Virtual Private Network (VPN) access request forms are not properly maintained.

Segregation of Duties

- Segregation of duties controls over CLAIMS 4 user roles has not been established.
- Segregation of duties controls over CLAIMS 3 LAN user roles has not been established.

Security Management

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

Recommendations:

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

For Configuration Management

Unless specifically noted where USCIS needs to take specific corrective action, we recommend that the USCIS Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the ICE Office of Chief Financial Officer and the ICE Office of the Chief Information Officer**,** make the following improvements to ICE's information technology:

- Improve patch management by implementing FFMS database and network patches.
- Examine default configurations and system services installed on FFMS network devices and remove unnecessary system services.
- Ensure configuration baseline parameters are consistent with DHS guidelines.

For USCIS, we recommend

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

As of June 2011, USCIS migrated from ADEX and no longer use it as their Active Directory. Therefore, no recommendation will be provided for the ADEX weaknesses.

For Access Controls

- Develop, authorize, and implement the following access control policies and procedures to:
  - Ensure that CLAIMS 3 LAN system administrator and user accounts are recertified annually.
  - Improve account management for maintaining network, VPN, CLAIMS 3 LAN, and CLAIMS 4 access request forms for all active users.
  - Comply with NIST guidance for managing equipment and media.
  - Maintain and recertify access to the TECC.
- Ensure that access is removed for separated CLAIMS 3 LAN accounts upon departure from the agency.

- Implement policies and procedures for CLAIMS 3 LAN and CLAIMS 4 audit logs to ensure compliance with DHS and National Institute of Standards and Technology (NIST) guidance.

USCIS remediated the CLAIMS 3 LAN and CLAIMS 4 password configuration weaknesses during our fieldwork. Based on the corrective action taken, no recommendation will be offered.

For Segregation of Duties

- Develop, authorize, and implement procedures for CLAIMS 4 segregation of duties.
- Define the segregated roles and responsibilities of CLAIMS3 LAN users in the System Security Plan (SSP).

For Security Management

- Monitor the implementation plan to assure the exit clearance procedures have been implemented.
- Continue 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.

APPLICATION CONTROLS

As a result of the control deficiencies noted above in the General Information Technology Controls, manual compensating controls were tested in place of application controls.

.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2011

Appendix A

Description of Key USCIS Financial Systems and IT Infrastructure within the Scope of the FY 2011 DHS 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, and Administrative Appeals Office. CLAIMS 3 LAN interfaces with the following systems:

- Citizenship and Immigration Services Centralized Oracle Repository (CISCOR)
- CLAIMS 3 Mainframe
- Integrated Card Production System (ICPS)
- CLAIMS 4
- E-filing
- Benefits Biometric Support System (BBSS)
- Refugee, Asylum, and Parole System (RAPS)
- National File Tracking System (NFTS)
- Integrated Card Production System (ICPS)
- Customer Relationship Interface System (CRIS)
- USCIS Enterprise Service Bus (ESB)

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, D.C. 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 (RNACS)
- CLAIMS 3 LAN and Mainframe
- RAPS
- Enterprise Performance Analysis System
- NFTS
- Asylum Pre-Screening System
- USCIS ESB
- BBSS
- Enterprise Citizenship and Immigration Service Centralized Operational Repository
- CRIS
- 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 users, and a National Finance Center (NFC) payroll interface. FFMS currently interfaces with the following systems:

- Direct Connect for transmission of DHS payments to Treasury
- Fed Traveler
- The Biweekly Examination Analysis Reporting and Controlling Accounting Data Inquiry (CADI), for the purpose of processing NFC user account and payroll information.
- The Debt Collection System
- Bond Management Information System Web

ICE Network (until June 2011)

The ICE Network, also known as the Active Directory/Exchange (ADEX) E-mail System, is a major application for ICE and other DHS components, such as the USCIS. The ADEX servers and infrastructure for the headquarters and National Capital Area are in Washington, DC. ADEX currently interfaces with the Diplomatic Telecommunications Service Program Office ICENet infrastructure.

CIS1 Network (as of June 2011)

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.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2011

Appendix B
FY 2011 Notices of IT Findings and Recommendations at USCIS

Notice of Findings and Recommendations (NFR) – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditors' Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist the DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
CIS-IT-11-01	Equipment and media policies and procedures are not current	Access Controls	2		X
CIS-IT-11-02	Weak password configuration controls for CLAIMS 4	Access Controls	2		X
CIS-IT-11-03	Policies and procedures for CLAIMS 3 LAN and CLAIMS 4 audit logs	Access Controls	2		X
CIS-IT-11-04	Policies and procedures for separated CLAIMS 3 LAN accounts	Access Controls	2		X
CIS-IT-11-05	Periodic user access reviews are not performed for CLAIMS 3 LAN users	Access Controls	2		X
CIS-IT-11-06	Procedures for transferred/terminated personnel exit processing are not finalized	Security Management	2		X
CIS-IT-11-07	Incomplete or inadequate access request forms for CLAIMS 3 LAN and CLAIMS 4 system users	Access Controls	2		X
CIS-IT-11-08	ICE resource server and inadequate patch management weaknesses impact USCIS operations	Access Controls	3		X
CIS-IT-11-09	Weak password configuration controls for CLAIMS 3 LAN	Access Controls	2	X	
CIS-IT-11-10	Weak logical access controls exist over CLAIMS 4	Access Controls	2		X
CIS-IT-11-11	Ineffective safeguards over physical access to sensitive facilities and resources	Access Controls	2	X	
CIS-IT-11-12	VPN access request forms are not properly maintained	Access Controls	2	X	
CIS-IT-11-13	Lack of Segregation of Duties for CLAIMS 3 LAN	Segregation of Duties	2		X
CIS-IT-11-14	ADEX access request forms are not properly maintained	Access Controls	1		X
CIS-IT-11-15	Lack of Computer Security Awareness Training Compliance	Security Management	2		X
CIS-IT-11-16	Lack role-based training for key security personnel	Security Management	2	X	
CIS-IT-11-17	FFMS Vulnerability Weaknesses effect USCIS Operations	Configuration Management	3		X

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2011

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, 2011

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
CIS-IT-10-01	Inefficient Definition and Documentation of Access Roles at the National Benefits Center for CLAIMS 3 LAN		11-13
CIS-IT-10-02	Periodic User Access Reviews are not Performed for CLAIMS 3 LAN Users.		11-05
CIS-IT-10-03	Incomplete or Inadequate Access Request Forms for CLAIMS 3 LAN and CLAIMS 4 System Users.		11-07
CIS-IT-10-04	Procedures for Transferred/Terminated Personnel Exit Processing are not Finalized.		11-06
CIS-IT-10-05	Equipment and Media Policies and Procedures are not Current.		11-01
CIS-IT-10-06	FFMS Vulnerability Weaknesses Impact USCIS Operations		11-17
CIS-IT-10-07	Weak Password Configuration Controls for CLAIMS 4.		11-02
CIS-IT-10-08	Ineffective Safeguards over Physical Access to Sensitive Facilities and Resources.	X	
CIS-IT-10-09	Lack of Policies and Procedures for CLAIMS 3 LAN and CLAIMS 4 Audit Logs		11-03
CIS-IT-10-10	Weak Logical Access Controls exist over CLAIMS 4		11-10
CIS-IT-10-11	Lack of Policies and Procedures for Separated CLAIMS 3 LAN Accounts		11-04
CIS-IT-10-12	IT Security Awareness Training Compliance is not Monitored		11-15
CIS-IT-10-13	ADEX Access Request Forms are not Properly Maintained		11-14
CIS-IT-10-14	Default Installation and Configuration of Cisco routers on ICE Network Impact USCIS Operations		11-08

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2011

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Director, USCIS
DHS Chief Information Officer
DHS Chief Financial Officer
Associate Director-Management, USCIS
Acting Chief Financial Officer, USCIS
Acting Chief Information Officer, USCIS
Chief Information Security Officer
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
USCIS Audit Liaison

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 report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to Department of Homeland Security programs and operations:

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

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