



Department of Homeland Security Office of Inspector General

**Information Technology Management
Letter for the U.S. Citizenship and
Immigration Services Component of the
FY 2010 DHS Financial Statement Audit**





Homeland
Security

APR 13 2011

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 FY 2010 U.S. Citizenship and Immigration Services (USCIS) component of the DHS financial statement audit as of September 30, 2010. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors' Report* dated November 12, 2010 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 2010 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 18, 2011, 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.

A handwritten signature in black ink, appearing to read "Frank Deffer".

Frank Deffer

Assistant Inspector General
Information Technology Audits



KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

March 18, 2011

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
U.S. Citizenship and Immigration Services

Ladies and Gentlemen:

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS or Department), as of September 30, 2010 and the related statement of custodial activity for the year then ended (herein after referred to as “financial statements”). We were also engaged to examine the Department’s internal control over financial reporting of the balance sheet as of September 30, 2010 and the statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources as of September 30, 2010 (hereinafter referred to as “other fiscal year (FY) 2010 financial statements”), or to examine internal control over financial reporting over the other FY 2010 financial statements.

Because of matters discussed in our *Independent Auditors’ Report*, dated November 12, 2010, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements or on the effectiveness of DHS’ internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended. Additional deficiencies in internal control over financial reporting, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the financial statements or on the effectiveness of DHS’ internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended; and had we been engaged to audit the other FY 2010 financial statements, and to examine internal control over financial reporting over the other FY 2010 financial statements.

A control deficiency 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 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. A material weakness is a deficiency, or a 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.

The United States Citizenship and Immigration Services (USCIS) is a component of DHS. During our audit engagement, we noted certain matters in the areas of information technology (IT) configuration management, access controls, segregation of duties, and security management with respect to USCIS’ financial systems information technology (IT) general controls, which we believe contribute to an IT material weakness at the DHS level. These matters are described in the *IT General Control Findings and Recommendations* section of this letter.

Information Technology Management Letter for the USCIS Component of the FY 2010 DHS Financial Statement Audit



The material weakness described above is presented in our *Independent Auditors' Report*, dated November 12, 2010. This letter represents the separate limited distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through a Notice of Finding and Recommendation (NFR).

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. We aim to use our knowledge of USCIS gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies. 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 our engagement to audit the FY 2010 DHS financial statements in Appendix A; a listing of the FY 2010 IT Notices of Findings and Recommendations (NFR) at USCIS in Appendix B; and the status of the prior year NFRs and a comparison to current year NFR's at USCIS in Appendix C. Our comments related to certain additional matters have been presented in a separate letter to the Office of Inspector General and the USCIS Chief Financial Officer.

USCIS' written response to our comments and recommendations has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of DHS and USCIS management, DHS Office of Inspector General, Office of Management and Budget (OMB), U.S. Government Accountability Office, 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, 2010

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	1
Summary of Findings and Recommendations	2
IT General Control Findings and Recommendations	
Configuration Management	3
Access Controls	3
Segregation of Duties	4
Security Management	4
Application Control	6
Management Comments and OIG Response	6

APPENDICES

Appendix	Subject	Page
A	Description of Key USCIS Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit Engagement	7
B	FY 2010 Notices of IT Findings and Recommendations at USCIS	10
	• Notice of Findings and Recommendations – Definition of Severity Ratings	11
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at USCIS	19
D	Management Comments	21

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit DHS' balance sheet as of September 30, 2010 and the related statement of custodial activity for the year then ended, we performed an evaluation of information technology general controls (ITGC) 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 Government Accountability Office (GAO), formed the basis of our ITGC evaluation procedures. The scope of the ITGC 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 ITGC 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 those 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 ITGC 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. In addition to testing ICE's general control environment, we tested controls around the FFMS migration to the Clarksville Data Center (DC2) in Clarksville, VA.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2010, USCIS took corrective action to address some prior year IT control deficiencies. For example, USCIS made improvements over ADEX system administrator recertification, physical controls at the Manassas Data Center, and access controls over security software. However, during FY 2010, we continued to identify IT general control deficiencies that could potentially impact USCIS's financial data. The most significant findings from a financial statement audit perspective were related to the FFMS configuration and patch management, and deficiencies within Computer Linked Application Information Management System (CLAIMS) 3 LAN and CLAIMS 4 user account management. 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 operation 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 did not fully comply with the requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the 14 findings identified during our FY 2010 testing, three 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 ultimate responsibility of USCIS management to determine the most appropriate method(s) for addressing the control deficiencies identified based on their system capabilities and available resources.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

IT GENERAL CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2010 DHS financial statement audit, we identified the following USCIS IT and financial system control deficiencies that in the aggregate significantly contribute to the material weakness at the Department level.

Configuration Management

- Security configuration management control deficiencies on ADEX. These control deficiencies included default installation and configuration settings on the Cisco routers.
- Security configuration management over FFMS included:
 - Network and servers were installed with default configuration settings and protocols.
 - Mainframe production databases were installed and configured without baseline security configurations.
 - Servers have inadequate patch management.

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.
 - Inefficient definition and documentation of CLAIMS 3 LAN and CLAIMS 4 access roles were noted.
 - User access is not documented and maintained for ADEX, CLAIMS 3 LAN, and CLAIMS 4.
 - CLAIMS 4 password configurations do not meet DHS requirements.
 - Terminated personnel still have active user accounts within CLAIMS 3 LAN and CLAIMS 4.
- Lack of processes in place for sanitization of equipment and media.
- Ineffective safeguards over physical access to sensitive facilities and resources at the DC2 and the USCIS Vermont Service Center.
- Lack of policies and procedures for maintaining and reviewing CLAIMS 3 LAN and CLAIMS 4 audit logs.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

Segregation of Duties

- Segregation of duties controls were not enforced through access authorizations in CLAIMS 4.

Security Management

- Procedures for transferred/terminated personnel exit processing are not finalized.
- IT Security training is not mandatory nor is compliance monitored.

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 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 CIO and 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:

- Ensure that password configuration settings are properly and effectively applied.
- Implement the appropriate FFMS database and network server patches in order to ensure patch management compliance.

For USCIS, we recommend

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

For Access Controls

- Finalize the CLAIMS 3 LAN and CLAIMS 4 account management procedures that address account identification, set-up, recertification, and termination and access request form maintenance.
- Review CLAIMS 3 LAN accounts that have been inactive for 45 days and remove users on the Office of Human Capital and Training (HCT) attrition bi-weekly list.
- Finalize the CLAIMS 3 LAN Account Management procedures that address account identification, set-up, recertification, and termination and access request form maintenance.
- Recertify CLAIMS 3 LAN accounts and ensure a current and valid access request form is maintained.
- Finalize and issue the USCIS management directive on Information System Account management.
- Evaluate the risk imposed on the CLAIMS 4 system by not modifying the password history from 6 to 8. If it is deemed that the risk is low, USCIS should submit a Waivers and Exceptions Request Form to the DHS Chief Information Security Officer (CISO). If the risk is deemed medium or high, USCIS should implement the password changes to meet DHS requirements.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

- Finalize and implement the CLAIMS 4 Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance.
- Finalize the USCIS Media Protection Management Directive and the USCIS Media Protection Procedures and ensure they are readily available to USCIS personnel.
- Finalize the Media Protection Procedures for the Vermont Service Center (VSC). In addition, USCIS should test VSC's Office of Information Technology (OIT) Visitor Policy and Procedures to ensure they address physical security.
- Finalize the USCIS Audit and Accountability Management Directive and implement enterprise audit logging software.

For Segregation of Duties

- Finalize the CLAIMS 4 account management procedures that address account identification, set-up, recertification, and termination and access request form maintenance.

For Security Management

- Implement and enforce exit clearance policies and procedures to be followed in the event of transfer, termination or separation of federal and contract personnel. Resources should be made available to communicate the updated procedures to personnel, train mission support staff who have a critical role in the updated process, and enforce and monitor compliance with the exit procedures and policies.
- Update and provide IT security training materials utilized during the New Employee Orientation Program (NEOP).
- Maintain a monthly report of all new hires and the information security awareness training date completion.
- Continue utilization of the Department of State (DOS) Computer Security Awareness Training (CSAT) tool to provide annual information security awareness training to all USCIS employees.

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

APPLICATION CONTROLS

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

MANAGEMENT COMMENTS AND OIG RESPONSE

The OIG received written comments on a draft of this report from USCIS management. Generally, USCIS management agreed with all of our findings and recommendations. USCIS management has developed a remediation plan to address these findings and recommendations. A copy of the comments is included in Appendix D.

OIG Response

We agree with the steps that USCIS management is taking to satisfy these recommendations.

**Department of Homeland Security
United States Citizenship and Immigration Services**
Information Technology Management Letter
September 30, 2010

Appendix A

**Description of Key USCIS Financial Systems and IT Infrastructure
within the Scope of the FY 2010 DHS Financial Statement Audit**

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

CLAIMS 3 Local Area Network (LAN)

CLAIMS3 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 executes on Dell 220 S (EMC), RAID Controller, Disk Storage servers protected by firewalls, and Windows 2003, MS Sp2 as the operating system and Pervasive database software and is used to enter and track immigration applications. 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. CLAIMS 4 runs off of Sunfire 890, 490, Solaris 9, and Oracle 9iR2 servers with Oracle 9i, Windows NT, and Windows 2000 Server operating systems and are protected by firewalls. The central Oracle Database that runs off Oracle Enterprise 9i 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 (RNACS)
- CLAIMS 3 LAN and Mainframe
- Refugee, Asylum, and Parole System (RAPS)
- Enterprise Performance Analysis System (ePAS)
- National File Tracking System (NFTS)
- Asylum Pre-Screening System (APSS)
- USCIS Enterprise Service Bus (ESB)
- Biometrics Benefits Support System (BBSS)
- Enterprise Citizenship and Immigration Service Centralized Operational Repository (eCISOR)
- Customer Relationship Interface System (CRIS)
- FD 258 Enterprise Edition and Mainframe
- Site Profile System (SPS)

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

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 and is built on Oracle 9i Relational Database Management System running off an IBM 9672 Mainframe with ZOS 1.4 platform. The FFMS operating system operates off an IBM ZOS, Version 1.4 Mainframe Server and Microsoft Windows 2000 report servers protected by firewalls. It includes the core system used by accountants, FFMS Desktop that is used by average users, and a National Finance Center (NFC) payroll interface. As of July 2010, the FFMS mainframe component and two network servers are hosted at the DHS DC2 facility located in Clarksville, Virginia. Prior to July, the system was housed at Department of Commerce located in Springfield, VA. FFMS currently interfaces with the following systems:

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

ICE Network

The ICE Network, also known as the 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 located on the third floor of the Potomac Center North Tower in Washington, DC. The ICE Network utilizes a hybrid mesh/hub and mesh network design to maximize redundancy throughout the network. ICE operates off of Dell PowerEdge 2950, HP ProLiant DL 385 Server, HP ProLiant BL45p Server Blade, HP BL 25P Blade Server, and EMC Symmetrix DM. ADEX has implemented Microsoft Windows 2003 Enterprise Server operating system to provide directory, domain control, and network services to clients. For security purposes, ADEX has implemented firewalls and a logical Layer-3 encrypted overlay network through the use of Generic Routing Encapsulation (GRE) and IPSec tunneling. ADEX currently interfaces with the following systems:

- Diplomatic Telecommunications Service Program Office (DTSPO) ICENet Infrastructure

**Department of Homeland Security
United States Citizenship and Immigration Services**
Information Technology Management Letter
September 30, 2010

Appendix B
FY 2010 Notices of IT Findings and Recommendations at USCIS

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

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 Department of Homeland Security (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, 2010

Notice of Findings and Recommendations – Detail

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-10-01	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that the access roles at the National Benefits Center (NBC) for CLAIMS3 LAN have not been defined and documented. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS Office of Information Technology (OIT) will finalize the CLAIMS 3 LAN Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. These procedures reflect how all CLAIMS 3 LAN accounts will be managed at each facility that utilizes the CLAIMS 3 LAN.		X	3
CIS-IT-10-02	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that the weakness has not been remediated for CLAIMS3 LAN periodic user access reviews. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to review CLAIMS 3 LAN accounts for those that have been inactive for 45 days manually and to remove user's that appear on the Office of Human Capital and Training (HCT) attrition bi-weekly list. OIT will finalize the CLAIMS 3 LAN Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work with the OIT Account Management Group, the IT Project Manager and each installation site to recertify CLAIMS 3 LAN accounts and ensure a current and valid access request form is filed. OIT will continue to work with HCT to ensure their exit clearance process includes procedures to promptly notify OIT when employees leave or transfer. OIT will also finalize the USCIS Account Management, Management Directive (Agency Policy).		X	3
CIS-IT-10-03	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of the prior year NFR and learned that the weakness still	The USCIS OIT will finalize the CLAIMS 3 LAN and CLAIMS 4 Account Management Procedures that address account identification, set-up,		X	2

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	exist for incomplete or inadequate access request forms for CLAIMS 3 LAN and CLAIMS 4. USCIS has begun some corrective action; however, these issues have not been fully remediated.	recertification, and termination and access request form maintenance. OIT will continue to work with the OIT Account Management Group, the IT Project Manager and each installation site to recertify CLAIMS 3 LAN and CLAIMS 4 accounts and ensure a current and valid access request form is filed.			
CIS-IT-10-04	In FY 2009, KPMG performed an inspection of a sample of personnel that had terminated/transferred from their employment with USCIS during the fiscal year. KPMG requested evidence that exit clearance forms were completed for each employee to determine USCIS management's compliance with termination/transfer procedures. Of the 28 terminated/transferred USCIS personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 19 employees. During the FY 2010 financial statement audit, we learned that USCIS Human Resource Division revised the existing terminated/transferred procedures for exit processing; however, the procedures have not been approved nor implemented.	We recommend USCIS management issue and adhere to exit clearance policies and procedures to be followed in the event of transfer, termination or separation of federal and contract personnel. Resources should be made available to communicate the updated procedures to personnel, train mission support staff who have a critical role in the updated process, and enforce and monitor compliance with the exit procedures and policies.		X	2
CIS-IT-10-05	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that equipment and media policies and procedures are not current. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will finalize the USCIS Media Protection Management Directive and the USCIS Media Protection Procedures and ensure they are readily available to USCIS personnel. OIT will continue to work with the Office of Administration to ensure there is a standardize process to label, track, sanitize, refurbish, and/or destroy USCIS media using approved equipment and software.		X	1
CIS-IT-10-06	During KPMG's internal vulnerability assessment of FFMS performed in August 2010, KPMG identified	USCIS will monitor the Mission Action Plans (MAP) of the associated ICE NFRs: IT-10-12, IT-	X		3

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
 September 30, 2010

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	several High/ Medium Risk vulnerabilities, related to the following: - FFMS mainframe production databases were installed and configured without baseline security configurations, including the USCIS Oracle instance - FFMS servers have missing or inadequate patches In addition, we found physical safeguard weaknesses at the Clarksville Data Center (DC2), which impact USCIS operations. Specifically, we determined the following: - Re-entry procedures after an emergency have been implemented; however, the procedures are not documented. - FFMS server is inappropriately marked with a label that identifies the application/data on the server.	10-13, IT-10-14, IT-10-15 and request periodic status updates.			
CIS-IT-10-07	During the FY 2009 financial statement audit, KPMG performed inspection of the CLAIMS 4 password configuration settings. Per our inspection, KPMG determined that CLAIMS 4 has been configured to prohibit password reuse for 6 generations, which does not meet the DHS 4300A requirement of 8 password generations. During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that the weakness has not been remediated for CLAIMS4 password configuration. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to evaluate the risk imposed on the CLAIMS 4 system by not changing the password history from 6 to 8. If it is deemed that the risk is low, OIT will submit a Waivers and Exceptions Request Form to the DHS CISO. If the risk is deemed medium or high, OIT will continue to implement the password changes as outlined in the FY09 USCIS OIT Mission Action Plan (MAP).		X	2

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-10-08	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that ineffective safeguards still exist over physical access to sensitive facilities and resources. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to finalize the Media Protection Procedures for the Vermont Service Center. OIT will test VSC's OIT Visitor Policy and Procedures to ensure they address the physical security concerns listed in the condition statement.		X	1
CIS-IT-10-09	In FY 2009, we determined that the USCIS lacks policies and procedures over audit logging of application and server audit logs for CLAIMS 3 LAN and CLAIMS 4 system. Specifically, we learned that CLAIMS3 LAN generates audit logs; however, the USCIS does not require that the logs are reviewed or maintained. In addition, we determined that the USCIS does not have policies or procedures in place for maintaining and reviewing the audit logs. For CLAIMS4, we noted that CSC contractors capture and review the logs of user access to CLAIMS4; however, no reviews of significant changes in the application or to system files are conducted. Additionally, no policies or procedures have been established for conducting and monitoring the audit log reviews.	The OIT will continue to finalize the USCIS Audit and Accountability Management Directive and implement enterprise audit logging software. OIT will ensure CLAIMS 3 LAN and CLAIMS 4 audit logs are provided to the enterprise audit logging software for analysis. Once the integration of CLAIMS 3 LAN and CLAIMS 4 and the enterprise audit logging software is complete, develop CLAIMS 3 LAN and CLAIMS 4 audit and accountability procedures.		X	2
CIS-IT-10-10	During the FY 2010 financial statement audit, we learned that USCIS has begun some corrective action; however, these issues have not been fully remediated. Therefore, this finding is being reissued. During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that weak logical access controls still exist over CLAIMS 4. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will finalize the CLAIMS 4 Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work with the OIT Account Management Group, the IT Project Manager and each installation site to recertify CLAIMS 4 accounts and ensure a current and valid access		X	2

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		request form is filed. OIT will also finalize the USCIS Account Management, Management Directive (Agency Policy). OIT will continue to review CLAIMS 4 accounts for those that have been inactive for 45 days manually and to remove users that appear on the Office of Human Capital and Training (HCT) attrition bi-weekly list. OIT will continue to work with HCT to ensure their exit clearance process includes procedures to promptly notify OIT when employees leave or transfer. The HCT must finalize Exit Clearance Process policies and procedures and ensure that these documents are disseminated agency-wide. Specifically, ensure that contracting officers, contacting officers' technical representatives, managers and supervisors are informed about these documents and understand their importance.			
CIS-IT-10-11	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that CLAIMS3 LAN still lacks policy and procedures for separated employees. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to review CLAIMS 3 LAN accounts for those that have been inactive for 45 days manually and to remove user's that appear on the HCT attrition bi-weekly list. OIT will finalize the CLAIMS 3 LAN Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work with HCT to ensure their exit clearance process includes procedures to promptly notify OIT when employees leave or transfer. OIT will also finalize the USCIS Account Management Directive (Agency Policy). The HCT must finalize Exit Clearance Process policies and procedures and ensure that these		X	2

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
 September 30, 2010

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		documents are disseminated agency-wide. Specifically, ensure that contracting officers, contacting officers' technical representatives, managers and supervisors are informed about these documents and understand their importance.			
CIS-IT-10-12	During the FY 2010 financial statement audit, we learned that the IT security awareness training weakness has not been remediated, therefore, this finding was reissued.	For initial information security awareness training, OIT will continue to update and provide training materials for the HCT New Employee Orientation Program (NEOP). The HCT should continue to implement the NEOP agency-wide. HCT must provide OIT a monthly report of all new hires and the date they completed initial information security awareness training during NEOP. For annual information security awareness refresher training, OIT will continue to use the Department of Status (DOS) Computer Security Awareness Training (CSAT) tool to provide information security awareness training to all USCIS employees with access to agency information systems.		X	2
CIS-IT-10-13	During roll forward testing for the FY 2010 financial statement audit, KPMG performed inspection of ADEX access request forms. Per our inspection, KPMG determined that one out of the forty-five access forms requested was not provided. Additionally, three out of the forty-five access forms requested were created on the same day of the request.	OIT will finalize and issue the USCIS MD on Information System Account Management. The MD stipulates policies on records management of access requests and standardizes the USCIS Network Access Request Form.	X		2
CIS-IT-10-14	ICE - During KPMG's internal vulnerability assessment efforts of ICE's ADEX network servers and devices performed in August 2010, KPMG identified a default installation and configurations for the Hot Standby Router Protocol (HSRP) on the Cisco routers.	USCIS will monitor the Mission Action Plan (MAP) of the associated NFR# ICE-IT-10-16 and request periodic status updates.		X	3

Appendix B

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

NFR #No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	<u>USCIS</u> - Although USCIS does not have direct responsibility for the controls over ADEX and ICE financial applications, USCIS does have a responsibility to proactively manage its service provider relationship with ICE. USCIS should require ICE to provide a detailed Corrective Action Plan (CAP) containing the planned remediation of the security vulnerabilities affecting USCIS data integrity.				

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2010

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, 2010

		Disposition	
NFR No.	Description	Closed	Repeat
CIS-IT-09-01	Inefficient definition and documentation of access roles at the National Benefits Center for CLAIMS3 LAN		10-01
CIS-IT-09-02	Periodic user access reviews are not performed for CLAIMS3 LAN users.		10-02
CIS-IT-09-03	Incomplete or inadequate access request forms for CLAIMS3 LAN and CLAIMS4 system users.		10-03
CIS-IT-09-04	Periodic Active Directory Exchange system administrator access reviews are not performed at USCIS.	X	
CIS-IT-09-06	Weak data center access controls exist	X	
CIS-IT-09-07	Equipment and media policies and procedures are not current.		10-05
CIS-IT-09-08	Weak access controls for security software exist within the Password Issuance and Control System.	X	
CIS-IT-09-09	Weak access controls exist in CLAIMS3 LAN.	X	
CIS-IT-09-10	Weak password configuration controls around CLAIMS4.		10-07
CIS-IT-09-11	Background investigations are not conducted in a timely manner.	X	
CIS-IT-09-12	Procedures for transferred/terminated personnel exit processing are not finalized		10-04
CIS-IT-09-13	Ineffective safeguards over physical access to sensitive facilities and resources		10-08
CIS-IT-09-14	Weak access controls exist within FFMS	X	
CIS-IT-09-15	Lack of policies and procedures for CLAIMS 3 LAN and CLAIMS 4 audit logs		10-09
CIS-IT-09-16	Weak logical access controls exist over CLAIMS 4		10-10
CIS-IT-09-17	Training for IT security personnel is not mandatory	X	
CIS-IT-09-18	Lack of policies and procedures for separated CLAIMS3 LAN accounts		10-11
CIS-IT-09-19	IT Security Awareness Training compliance is not monitored		10-12
CIS-IT-09-20	Default installation and configuration of Cisco routers on ICE Network Impact USCIS Operations.		10-14

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Chief Information Officer
Washington, DC 20529



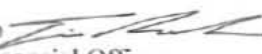
**U.S. Citizenship
and Immigration
Services**

February 24, 2011

Memorandum

TO: Frank Deffer
Assistant Inspector General for Information Technology Audits
U.S. Department of Homeland Security

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

 Timothy Rosado
Acting, Chief Financial Officer
U.S. Citizenship and Immigration Services

SUBJECT: Information Technology Management Letter for the USCIS Component of
the FY 2010 DHS Financial Statement Audit

We would like to thank you for the opportunity to review and comment on the Information Technology (IT) Management Letter for the U.S. Citizenship and Immigration Services (USCIS) Component for the FY 2010 Department of Homeland Security (DHS) Financial Statement Audit. USCIS requests that your Office make the following changes to the Independent Auditor's Report.

Except for the items noted below, USCIS agrees and accepts all finding, comments, and conclusions expressed in this report.

**FINDINGS CONTRIBUTING TO A MATERIAL WEAKNESS IN IT AT THE
DEPARTMENT LEVEL**

Conditions: During the FY 2010 DHS Financial Statement Audit, we identified the following USCIS IT and financial system control deficiencies that in the aggregate significantly contribute to the material weakness at the Department level.

Configuration Management

- Security configuration management control deficiencies on ADEX. These control deficiencies included default installation and configuration settings on the Cisco routers.

www.uscis.gov

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

Information Technology Management Letter for the USCIS Component of the FY 2010 DHS
Financial Statement Audit
Page 2

USCIS Suggested Change:

- Security configuration management control deficiencies on ADEX. These control deficiencies included default installation and configuration settings on ICE's Cisco routers.

Rational: The independent auditors only performed network and device testing on ICE's equipment using software scanning tools. USCIS does not have the oversight to manage ICE's installation of equipment used for shared services.

Access Control

- The following account management control deficiencies over ADEX, CLAIMS 3 LAN, and CLAIMS 4:
 - User access is not documented and maintained for ADEX, CLAIMS 3 LAN, and CLAIMS 4.
- Lack of processes in place for sanitization of equipment and media.

USCIS Suggested Change:

- The following account management control deficiencies over ADEX, CLAIMS 3 LAN, and CLAIMS 4:
 - User access request forms are not consistently maintained for ADEX, CLAIMS 3 LAN, and CLAIMS 4.
- Outdated documented processes for sanitization of equipment and media.

Rational: For all three information systems, USCIS provided roughly 90 percent of all forms requested by the independent auditor. User access requests are documented on USCIS Forms G-1160 and G-872. USCIS agrees that it needs to improve the maintenance process of these forms so that they are ready available upon request.

The Office of Information Technology (OIT) purchased approximately 100 degaussers and media sanitization software to ensure media is sanitized and degaussed when appropriate. OIT has draft USCIS Media Protection policies and procedures that support the implementation of DHS and National Institute of Standards and Technology policies, procedures, and standards. USCIS has media protection processes; however, our documentation has not been finalized.

Security Management

- IT Security training is not mandatory nor is compliance monitored.

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

Information Technology Management Letter for the USCIS Component of the FY 2010 DHS
Financial Statement Audit
Page 3

USCIS Suggested Change:

- IT Security Awareness training completions are not consistently monitored.

Rational: USCIS' Office of Human Capital and Training (HCT) maintains a Learning Management System (LMS) that:

- maintains all training records for USCIS employees and contractors,
- provides computer-based training courses, and
- maintains employees mandatory training plans.

The LMS is configured to have the USCIS Computer Security Awareness Training (CSAT) course on every employee's mandatory training plan. On April 9, 2010, the USCIS Acting Chief Information Officer issued the Mandatory CSAT policy requiring all USCIS employees and contractors to complete CSAT and enforcing the removal of network and email access for those that do not comply with the policy.

On June 23, 2010, OIT implemented the Department of State CSAT web-based tool to handle all tracking and monitoring of CSAT completions. This product automatically monitors and notifies employees when to complete CSAT. Employees are sent weekly email reminders until the training is completed.

Prior to the implementation of the DOS CSAT, the USCIS Academy monitored and tracked CSAT completions in the LMS. Training Coordinators throughout the agency were responsible for ensuring all employees completed CSAT in the LMS. The DOS CSAT product eliminates the manual tracking of CSAT completions by Training Coordinators.

USCIS is committed to resolving all control deficiencies and weaknesses identified in the audit and have prepared Mission Action Plans and Plan of Action and Milestones to resolve and improve the Agency's information technology controls.

USCIS appreciates the cooperation and respect that your staff provided during the course of the audit and looks forward to continuing our strong working relationship with your office.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

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 visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

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