Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Statement Audit

OIG-10-93

June 2010

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland
Security

JUN - 8 2010

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 2009 U.S. Citizenship and Immigration Services (USCIS) financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors' Report* dated January 15, 2010 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at USCIS in support of the DHS FY 2009 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 10, 2010, 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
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036

March 10, 2010

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 have audited the consolidated balance sheet of the U.S. Citizenship and Immigration Services (USCIS), a component of the U.S. Department of Homeland Security (DHS), as of September 30, 2009 and the related consolidated statements of net cost, changes in net position, and the combined statement of budgetary resources (hereinafter referred to as "consolidated financial statements") for the years then ended. In planning and performing our audit of the consolidated financial statements of USCIS, in accordance with auditing standards generally accepted in the United States of America, we considered USCIS's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements but not for the purpose of expressing an opinion on the effectiveness of USCIS's internal control. Accordingly, we do not express an opinion on the effectiveness of USCIS's internal control.

In planning and performing our fiscal year 2009 audit, we considered USCIS's internal control over financial reporting by obtaining an understanding of the design effectiveness of USCIS's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements. To achieve this purpose, we did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*. The objective of our audit was not to express an opinion on the effectiveness of USCIS's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of USCIS's internal control over financial reporting.

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 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.

Our audit of USCIS as of, and for the year ended, September 30, 2009 disclosed a material weakness in the areas of information technology (IT) configuration management, security management, access controls, and segregation of duties. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated January 15, 2010. This letter represents the separate restricted 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). Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. 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.

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 2009 USCIS consolidated financial statement audit 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 certain additional matters have been presented in a separate letter to the Office of Inspector General and the USCIS Chief Financial Officer dated January 15, 2010.

This communication is intended solely for the information and use of DHS and USCIS management, DHS Office of Inspector General, 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, 2009

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

Page

APPENDICES

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2009

OBJECTIVE, SCOPE AND APPROACH

We have audited the US Citizenship and Immigration Services (USCIS) balance sheet as of September 30, 2009. In connection with our audit of USCIS's balance sheet we performed an evaluation of information technology general controls (ITGC), to assist in planning and performing our audit. The U.S. Department of Homeland Security – Bureau of 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 audit. The scope of the USCIS IT general controls assessment is 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 general IT controls 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 general IT controls 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 the general control environment, we performed application control tests on a limited number of ICE's financial systems and applications. The application control testing was performed to assess the controls that support USCIS financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2009, we noted that USCIS made minimal progress in addressing its previously identified IT internal control weaknesses. Therefore, due to USCIS's lack of prioritization of the issues, all seven (7) were reissued. During our review, we continued to identify IT general control weaknesses that could potentially impact USCIS's financial data. The most significant weaknesses from a financial statement audit perspective related to controls over the FFMS and the weaknesses over physical security and security awareness. Collectively, the IT control weaknesses 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 weaknesses negatively impacted the internal controls over USCIS financial reporting and its operation and we consider them to collectively represent a material weakness for USCIS 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 USCIS did not fully comply with the requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the 19 findings identified during our FY 2009 testing, 12 were new IT findings. These findings represent weaknesses in four of the five FISCAM key control areas. Specifically, 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 weaknesses 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 and reported in USCIS's financial statements.

USCIS management should ensure that there is emphasis placed on the completion, monitoring and enforcement of IT security-related policies and procedures. On-going measures to improve the IT security considerations for key financial systems utilized by USCIS and implement effective access controls, segregation of duties and configuration management controls need to be completed.

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 weaknesses identified based on their system capabilities and available resources.

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

Findings Contributing to a Material Weakness Deficiency in IT

During the FY 2009 financial statement audit, we identified the following IT control deficiencies that are considered a material weakness:

1. Configuration Management – we noted:
   - Security configuration management weaknesses on the Active Directory Exchange (ADEX). These weaknesses included default configuration settings, inadequate patches, and weak password management.
2. Security Management – we identified:
   - Background investigations are not conducted in a timely manner.
   - Procedures for transferred/terminated personnel exit processing are not finalized.
   - IT Security training is not mandatory nor is compliance monitored.
3. Access controls – we identified:
   - Ineffective safeguards over physical access to sensitive facilities and resources.
   - The following account management weaknesses over ADEX, CLAIMS 3 LAN, and CLAIMS 4:
     - The lack of recertification of system administrators and 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 CLAIMS 3 LAN and CLAIMS 4.
     - CLAIMS 3 LAN and CLAIMS 4 password configurations do not meet DHS requirements.
     - Terminated personnel still have active user accounts within CLAIMS 3 LAN and CLAIMS 4.
     - Generic user accounts exist for the CLAIMS 3 LAN.
   - Lack of policies and procedures for maintaining and reviewing CLAIMS 3 LAN and CLAIMS 4 audit logs.
   - Lack of processes in place for sanitization of equipment and media.
4. Segregation of Duties– we identified:
   - Segregation of duties controls were not enforced through access authorizations in CLAIMS 4.

Recommendations: 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:

1. Configuration Management:

   - Redistribute procedures and train employees on continuously monitoring and mitigating vulnerabilities. In addition, we recommend that ICE periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, in addition to deploying patches.
   - Perform vulnerability assessments and penetration tests on all offices of the ICE, from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with NIST guidance.
   - Develop a more thorough approach to track and mitigate configuration management and resource vulnerabilities identified during monthly scans. ICE should monitor the vulnerability reports for necessary or required configuration changes to their environment.
   - Develop a process to verify that systems identified with "HIGH/MEDUIM Risk" configuration vulnerabilities do not appear on subsequent monthly vulnerability scan reports, unless they are verified and documented as a false-positive. All risks identified during the monthly scans should be mitigated immediately, and not be allowed to remain dormant.
   - Implement the corrective actions identified during the audit vulnerability assessment as identified in the issued NFR.

2. Security Management:

   - Periodically review personnel files to confirm background investigations have been completed in accordance with DHS standards.
   - Adhere to exit clearance procedures and enforce personnel adherence in the event of transfer\termination.
   - Implement mandatory requirements for IT security personnel to complete training consistent with their job duties.
   - Establish and implement requirements for personnel to complete Computer Security Awareness training annually. Also, develop a process to disable user accounts and access privileges for non compliant staff.

3. Access Controls:

   - Establish and implement emergency exit and re-entry procedures at the Technology Engineering Consolidation Center (TECC).

- Implement effective physical access controls over the server cage which houses USCIS servers at the TECC.
- Conduct and document annual reviews of application users and users with system administrator access to ADEX.
- Establish and enforce procedures for the completion and maintenance of user access forms for CLAIMS 3 LAN and CLAIMS 4 across all service centers.
- Establish a process to ensure CLAIMS 3 LAN and CLAIMS 4 are configured to meet DHS password configuration requirements.
- Develop and implement policies and procedures to remove terminated users and generic accounts from the CLAIMS 3 LAN.
- Establish a process to review and maintain system audit logs.

4. Segregation of Duties:
   - Define and document the policies and procedures for identifying and approving CLAIMS 4 user roles\profiles to include user responsibilities and segregation of duties initiatives.

USCIS Specific Recommendations:

5. We recommend that the offices of the USCIS CIO, ICE CIO, and DHS CIO coordinate to develop an Interagency Agreement for the ICE/USCIS relationship. The agreement should be developed using appropriate guidance from NIST 800-53. Specific to this NFR, the Interagency Agreement should document the processes by which ICE will notify USCIS of its planned remediation of the ADEX security vulnerabilities. USCIS should further take a proactive approach in monitoring the resolution of the ADEX vulnerabilities.
6. The USCIS CIO should ensure that USCIS has a sound understanding of the ICE security vulnerabilities that affect USCIS data integrity. USCIS should then develop remediation plans and compensating controls, as applicable, to address potential data integrity issues. For example, more frequent reconciliation of financial accounts may be required.

Cause\Effect:
The ICE agency is not continuously monitoring the ICE ADEX General Support System (GSS) vulnerability assessment scans for patch and configuration management vulnerabilities. USCIS management has not proactively coordinated with ICE to establish a detailed and documented Interagency Agreement for the IT services provided by ICE. As a result, default configuration installations and unnecessary services operating on the ICE ADEX devices increases the ability to compromise the availability, integrity, and confidentiality of financial data on the network. Additionally, failure to apply critical vendor security patches exposes system and network devices to new and existing vulnerabilities. This can expose the information system controls environment

to security breaches, unauthorized access, service interruptions, and denial of service attacks. These weak IT controls at ICE, specifically with ADEX, have a direct and significant negative impact on USCIS financial data integrity. Consequently, USCIS requires additional resources to implement compensating controls needed to ensure fair presentation of its financial statements.

Due to a lack of USCIS management oversight, the controls environment remains weak and needs overall improvement. The lack of a strong controls environment increases the risk of improper handling of sensitive information, unauthorized access to financial data, improper staff training, and improper segregation of duties and least privilege principles.

Reasonable assurance should be provided that system user access levels are limited and monitored for appropriateness. The weaknesses identified within USCIS's access controls increases the risk that staff may have access to a system that is outside the realm of their job responsibilities. This access could allow a person to intentionally or inadvertently use various functions to alter the integrity of executable files and scripts within the financial system.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is to: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of the Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

APPLICATION CONTROL FINDINGS

We did not identify any IT findings in the area of application controls during the FY 2009 Financial Statement Audit Engagement.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the USCIS management. USCIS management agreed with 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, 2009

Appendix A

Description of Key USCIS Financial Systems and IT Infrastructure within the Scope of the FY 2009 Financial Statement Audit

Department of Homeland Security
United States Citizenship and Immigration Services

Information Technology Management Letter

September 30, 2009

Below is a description of significant USCIS and ICE financial management systems and supporting information technology (IT) infrastructure included in the scope of USCIS's fiscal year (FY) 2009 Financial Statement Audit.

Locations of Review: USCIS Headquarters, Washington, DC; Verizon Data Center, Manassas, VA; Vermont Service Center, Burlington, VT.

ICE Headquarters, Washington, DC; The Burlington Finance Center (BFC), Burlington, VT; Department of Commerce (DOC) Office of Computer Services (OCS), Springfield, VA.

Systems Subject to Audit:

- *Federal Financial Management System (FFMS):* 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.
- *ICE Network:* The ICE Network, also known as the Active Directory\Exchange (ADEX) E-mail System, is the general support system (GSS) for ICE and other DHS components, such as the USCIS.
- *Computer-Linked Application Management System (CLAIMS)3 Local Area Network (LAN):* Provides a decentralized LAN based system that 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 each of the service centers (Nebraska, California, Texas, Vermont, and the National Benefits Center).
- *CLAIMS 4:* The system is a client/server application that tracks and manages naturalization applications. The central Oracle Database is located in Washington, DC while application servers and client components are located throughout USCIS service centers and district offices.

Appendix B

FY 2009 Notices of IT Findings and Recommendations at USCIS

Department of Homeland Security
United States Citizenship and Immigration Services

Information Technology Management Letter

September 30, 2009

<u>Notice of Findings and Recommendations (NFR) – Definition of Severity Ratings:</u>

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 USCIS in 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, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-01	We inspected the National Benefits Center (NBC) CLAIMS 3 LAN user role/responsibilities documentation and determined that the system settings and assigned user roles within the system do not accurately reflect documented user responsibilities.	Continue to define and document the various CLAIMS 3 LAN roles and their associated responsibilities for the remaining service centers.		X	2
CIS-IT-09-02	NBC does not perform periodic CLAIMS 3 LAN user access reviews to ensure that users' level of access remains appropriate and there are no procedures established for performing periodic reviews.	Establish and implement policies and procedures for handling, reviewing, and retention of Claims 3 LAN user account request forms.		X	2
CIS-IT-09-03	Management at the USCIS Headquarters (HQ) and the Service Center, Vermont has not completed or inadequately documented access forms for CLAIMS 3 LAN and CLAIMS 4, system users.	Establish and enforce procedures for the completion and maintenance of user access forms for CLAIMS 3LAN and CLAIMS 4 for all the service centers.		X	2
CIS-IT-09-04	The USCIS HQ has not maintained or documented a selection of system administrator's access authorization forms.	Conduct and document annual reviews of all users with Active Directory system administrator access.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-06	The biometric facial recognition scanner allowed unauthorized personnel access to USCIS server room, and procedures regarding removal, authorization, and logging of USCIS backup media are not in place for the Technology Engineering Consolidation Center (TECC).	• Establish and implement backup media retention and rotation policies. • Establish and implement emergency exit and re-entry procedures. • Develop a process that assures all resources with access to the USCIS resources adhere to the policy and procedure. • Implement stronger physical access controls over the server cage door to prevent further unauthorized access		X	2
CIS-IT-09-07	USCIS has not finalized a policy that outlines the process for developing forms for labeling and tracking the disposition process or provided clear instructions for conducting media wipes or purges of data.	Update and finalize their policies and procedures to reflect their current media sanitization operation.		X	2
CIS-IT-09-08	USCIS does not recertify its system administrator accounts on an annual basis.	Management should establish a more timely process to perform a periodic review of user accounts ensuring proper authorization and training.		X	2
CIS-IT-09-09	CLAIMS 3 LAN password re-use and length configurations does not meet DHS standards. CLAIMS 3 LAN generic user accounts was not timely removed because of a lack of user account recertification.	• Establish a process to ensure that USCIS systems are configured to meet minimum DHS password configurations and requirements. • Remove all generic accounts to CLAIMS 3 LAN production systems and perform periodic reviews of the user access list to ensure compliance.	X		2

Department of Homeland Security
United States Citizenship and Immigration Services
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-10	CLAIMS 4 LAN password configuration settings does not meet DHS4300A password standards.	We recommend that USCIS establish a process to ensure CLAIMS 4 LAN is configured to meet DHS4300A password configuration standards.	X		2
CIS-IT-09-11	We identified that an inadequate background investigation was performed and documented for one new hire personnel from a sample of 25.	We recommend that USCIS management periodically review personnel files to confirm background investigations have been completed in accordance with DHS standards.	X		2
CIS-IT-09-12	We inspected a sample of personnel that had terminated/transferred from their employment with USCIS. Of the 28 terminated/transferred USCIS personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 19 employees.	We recommend that USCIS management adhere to exit clearance procedures and require personnel to follow them in an event of transfer/termination.	X		2
CIS-IT-09-13	Vermont Service Center (VSC) has ineffective safeguards over the computer room in the Office of Information Technology (OIT). VSC procedures regarding the removal, authorization and logging of backup media are not in place. VSC procedures for ensuring accuracy and completeness over visitor logs are not enforced.	• Establish and implement procedures for maintaining and authorizing the OIT's computer room access list. • Establish and implement backup media retention and rotation policies. • Enforce completeness and accuracy over visitor information in logs.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-14	During our testing of access controls for FFMS, in our sample of 25 active users, we noted one user's access was excessive, based on the access approved by their present supervisor. We learned that this user's profile was changed as the user relocated to a different service center. However, when the profile change was requested, the FFMS administrator did not remove all previous access nor assure that the access rights were current and authorized. As a result, the user had excessive privileges for her role and responsibilities. We also noted that the USCIS SOP did not reflect this procedure though we learned through inquiry that the FFMS administrators are required to remove all prior access when performing a profile change. As a result of our test work, USCIS responded by removing the excessive access to reflect the user's role and responsibilities. In addition, USCIS updated their SOP to require all previous access to be confirmed and removed prior to granting new access roles.	We recommend that USCIS establish and enforce policies and procedures that ensure that roles and responsibilities are commensurate with their job function.	X		2
CIS-IT-09-15	We identified a lack of audit logging policies over the application and server logs for the CLAIMS 3 and CLAIMS 4 LAN system.	We recommend that USCIS establish and enforce policies and procedures for maintenance and review of audit logging.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-16	We identified weaknesses within access controls for CLAIMS 4 over lack of procedures for recertifying user access, lack of evidence of least privilege and segregation of duties controls, and untimely removal of terminated personnel accounts.	• Establish and implement policies and procedures for the handling, periodically reviewing, and retaining CLAIMS 4 user account request forms. • Define and document policies and procedures for identifying and approving CLAIMS 4 user roles/profiles to include the user's responsibilities. In addition, the policies and procedures should address and implement segregation of duties procedures. • Develop policies and procedures for the removal of transferred/terminated users within CLAIMS 4 upon their separation from USCIS.	X		2
CIS-IT-09-17	We identified weaknesses within monthly trainings of USCIS' ISSOs.	We recommend that USCIS management implement mandatory training requirements for IT security personnel to complete training consistent with their job function duties.	X		2
CIS-IT-09-18	We determined that weaknesses exist related to CLAIMS3 LAN access. Specifically, we identified 21 users which were separated from USCIS and still retained access to the CLAIM3 LAN.	We recommend that USCIS management develop and implement policies and procedures for the removal of separated users within CLAIMS 3 LAN upon their separation.	X		2
CIS-IT-09-19	We tested a sample of personnel that were required to complete annual Computer Security Awareness Training during the fiscal year. Of the thirty (30) personnel sampled, evidence of compliance could not be provided for two (2) employees. Additionally, procedures are not in place to disable user accounts	• Establish and implement requirements for personnel to complete Computer Security Awareness Training annually. • Develop a process to disable user accounts and access privileges in accordance with DHS policies for employees not in compliance.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	and access privileges if annual training is not completed on a timely basis.				
CIS-IT-09-20	During the internal vulnerability assessment efforts of network servers and systems we identified several High/ Medium Risk vulnerabilities, related to configuration management. We determined that security configuration management weaknesses (i.e., missing security patches and incorrect configuration settings) exist on hosts supporting the ICE.	In addition to addressing the specific vulnerabilities identified in the condition, ICE should: • Redistribute procedures and train employees on continuously monitoring and mitigating vulnerabilities. In addition, we recommend that ICE periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, in addition to deploying patches. • Perform vulnerability assessments and penetration tests on all offices of the ICE, from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with NIST guidance. • Develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans. ICE should monitor the vulnerability reports for necessary or required configuration changes to their environment.	X		N\A- Issued after release of DHS audit report

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		• Develop a process to verify that systems identified with "HIGH/MEDUIM Risk" configuration vulnerabilities do not appear on subsequent monthly vulnerability scan reports, unless they are verified and documented as a false-positive. All risks identified during the monthly scans should be mitigated immediately, and not be allowed to remain dormant. USCIS should: • We recommend that the offices of the USCIS CIO, ICE CIO, and DHS CIO coordinate to develop an Interagency Agreement for the ICE/USCIS relationship. The agreement should be developed using appropriate guidance from NIST 800-53. Specific to this NFR, the Interagency Agreement should document the processes by which ICE will notify USCIS of its planned remediation of the ADEX security vulnerabilities. USCIS should further take a proactive approach in monitoring the resolution of the ADEX vulnerabilities. • The USCIS CIO should ensure that USCIS has a sound understanding of the ICE security vulnerabilities that affect USCIS data integrity. USCIS should then develop remediation plans and compensating controls,			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		as applicable, to address potential data integrity issues. For example, more frequent reconciliation of financial accounts may be required.			

Appendix C

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

Appendix C

Department of Homeland Security
United States Citizenship and Immigration Services

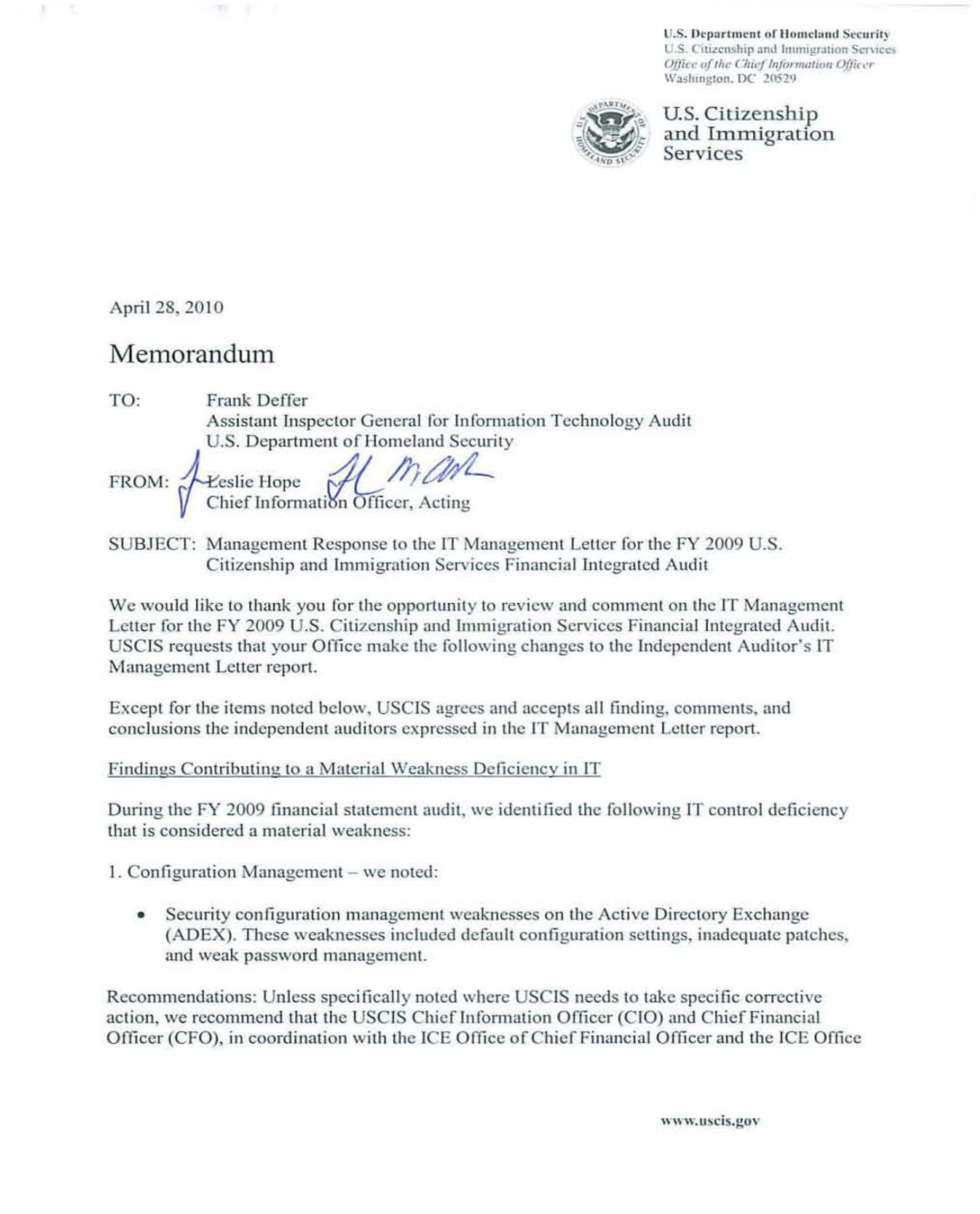
Information Technology Management Letter

September 30, 2009

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
CIS-IT-08-01	Lack of Definition and Documentation of Access Roles at the National Benefits Center for CLAIMS 3 LAN		09-01
CIS-IT-08-02	Periodic CLAIMS 3 LAN User Access Reviews are not Performed at the NBC		09-02
CIS-IT-08-03	Incomplete or Inadequate Access Request Forms for CLAIMS 3 LAN, CLAIMS 4, and CISCOR System Users at Headquarters and the Service Centers		09-03
CIS-IT-08-04	Ineffective Controls for Restricting Security Software Exist		09-04
CIS-IT-08-06	Weak Data Center Access Controls		09-06
CIS-IT-08-07	Equipment and Media Policies and Procedures are not Current		09-07
CIS-IT-08-08	Weak Access Controls for Security Software Exist		09-08

Appendix D

USCIS Management's Comments



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

April 28, 2010

Memorandum

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

FROM: Leslie Hope
Chief Information Officer, Acting

SUBJECT: Management Response to the IT Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Integrated Audit

We would like to thank you for the opportunity to review and comment on the IT Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Integrated Audit. USCIS requests that your Office make the following changes to the Independent Auditor's IT Management Letter report.

Except for the items noted below, USCIS agrees and accepts all finding, comments, and conclusions the independent auditors expressed in the IT Management Letter report.

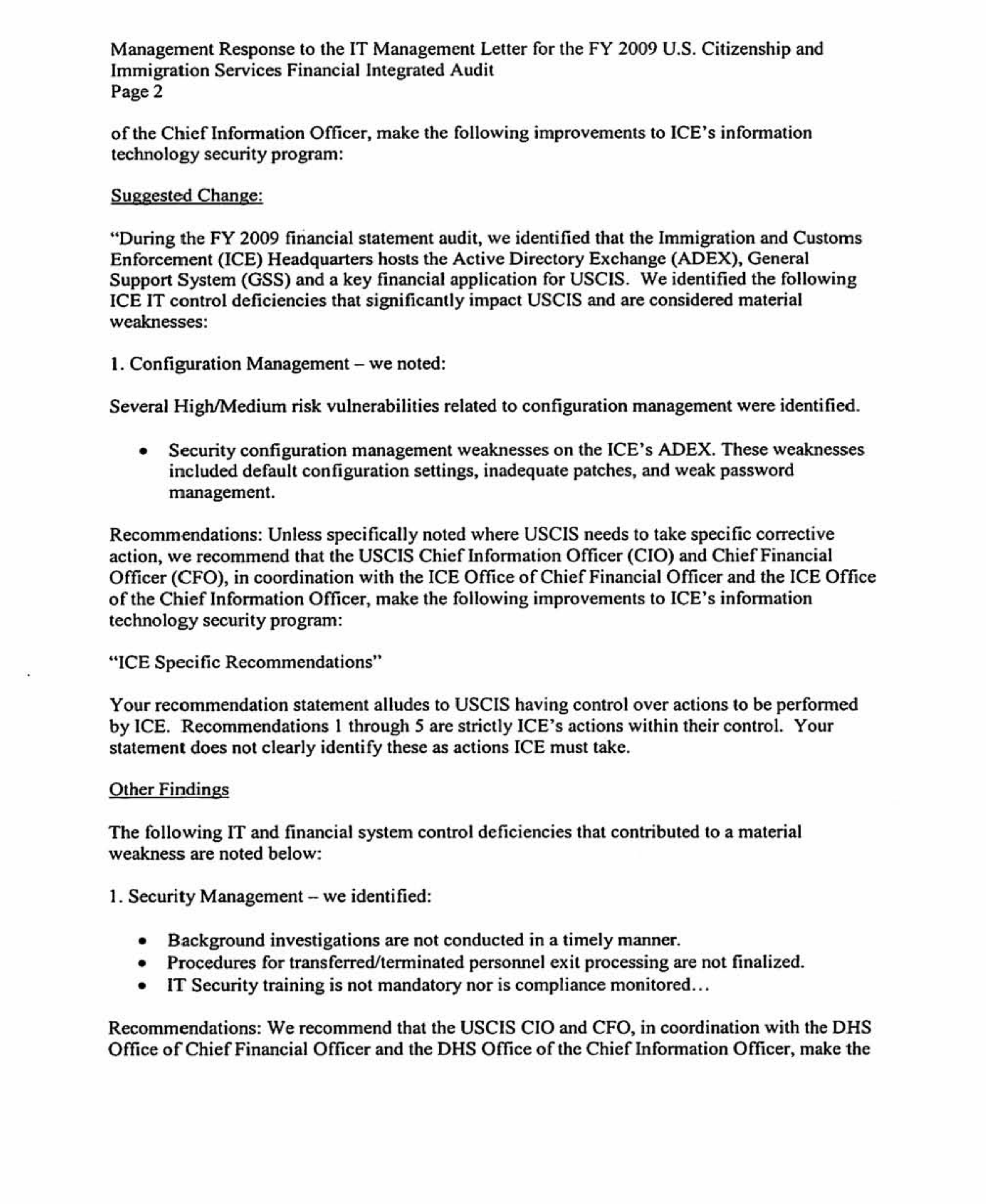
Findings Contributing to a Material Weakness Deficiency in IT

During the FY 2009 financial statement audit, we identified the following IT control deficiency that is considered a material weakness:

1. Configuration Management – we noted:

- Security configuration management weaknesses on the Active Directory Exchange (ADEX). These weaknesses included default configuration settings, inadequate patches, and weak password management.

Recommendations: 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 security program:

Suggested Change:

"During the FY 2009 financial statement audit, we identified that the Immigration and Customs Enforcement (ICE) Headquarters hosts the Active Directory Exchange (ADEX), General Support System (GSS) and a key financial application for USCIS. We identified the following ICE IT control deficiencies that significantly impact USCIS and are considered material weaknesses:

1. Configuration Management – we noted:

Several High/Medium risk vulnerabilities related to configuration management were identified.

- Security configuration management weaknesses on the ICE's ADEX. These weaknesses included default configuration settings, inadequate patches, and weak password management.

Recommendations: 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 security program:

"ICE Specific Recommendations"

Your recommendation statement alludes to USCIS having control over actions to be performed by ICE. Recommendations 1 through 5 are strictly ICE's actions within their control. Your statement does not clearly identify these as actions ICE must take.

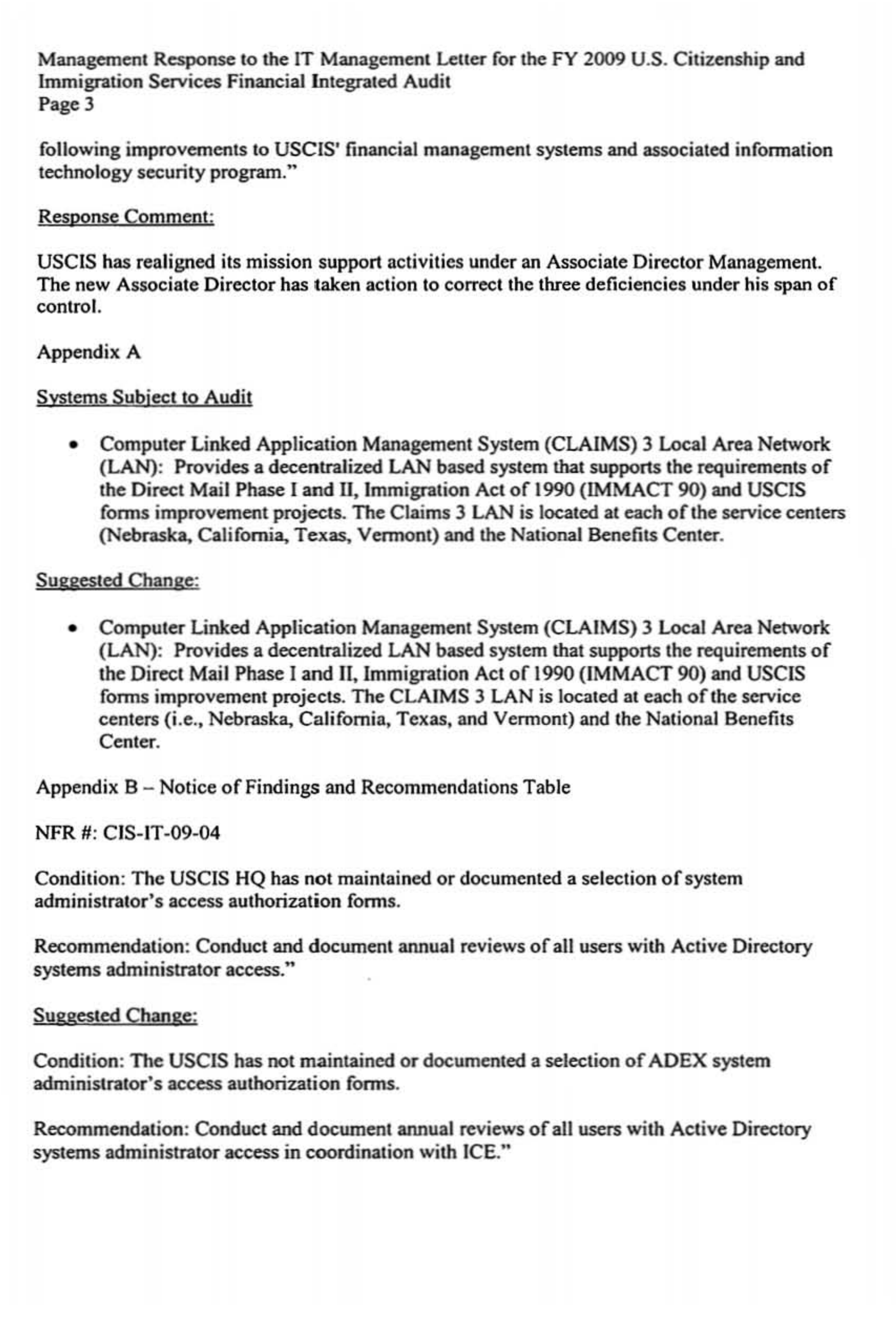
Other Findings

The following IT and financial system control deficiencies that contributed to a material weakness are noted below:

1. Security Management – we identified:

- Background investigations are not conducted in a timely manner.
- 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 CIO and CFO, in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer, make the



Management Response to the IT Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Integrated Audit
Page 3

following improvements to USCIS' financial management systems and associated information technology security program."

Response Comment:

USCIS has realigned its mission support activities under an Associate Director Management. The new Associate Director has taken action to correct the three deficiencies under his span of control.

Appendix A

Systems Subject to Audit

- Computer Linked Application Management System (CLAIMS) 3 Local Area Network (LAN): Provides a decentralized LAN based system that 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 each of the service centers (Nebraska, California, Texas, Vermont) and the National Benefits Center.

Suggested Change:

- Computer Linked Application Management System (CLAIMS) 3 Local Area Network (LAN): Provides a decentralized LAN based system that 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 each of the service centers (i.e., Nebraska, California, Texas, and Vermont) and the National Benefits Center.

Appendix B – Notice of Findings and Recommendations Table

NFR #: CIS-IT-09-04

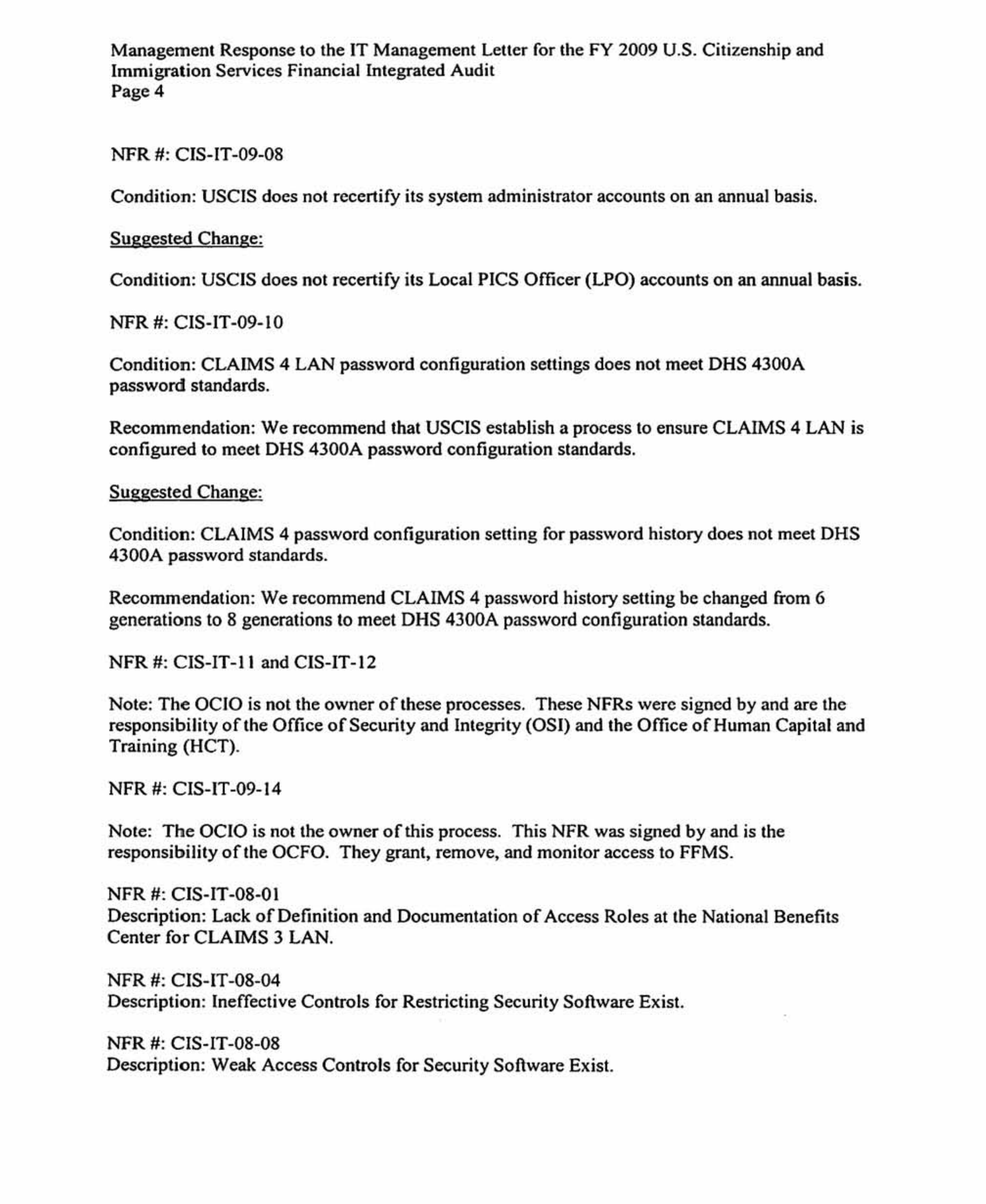
Condition: The USCIS HQ has not maintained or documented a selection of system administrator's access authorization forms.

Recommendation: Conduct and document annual reviews of all users with Active Directory systems administrator access."

Suggested Change:

Condition: The USCIS has not maintained or documented a selection of ADEX system administrator's access authorization forms.

Recommendation: Conduct and document annual reviews of all users with Active Directory systems administrator access in coordination with ICE."



Management Response to the IT Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Integrated Audit
Page 4

NFR #: CIS-IT-09-08

Condition: USCIS does not recertify its system administrator accounts on an annual basis.

Suggested Change:

Condition: USCIS does not recertify its Local PICS Officer (LPO) accounts on an annual basis.

NFR #: CIS-IT-09-10

Condition: CLAIMS 4 LAN password configuration settings does not meet DHS 4300A password standards.

Recommendation: We recommend that USCIS establish a process to ensure CLAIMS 4 LAN is configured to meet DHS 4300A password configuration standards.

Suggested Change:

Condition: CLAIMS 4 password configuration setting for password history does not meet DHS 4300A password standards.

Recommendation: We recommend CLAIMS 4 password history setting be changed from 6 generations to 8 generations to meet DHS 4300A password configuration standards.

NFR #: CIS-IT-11 and CIS-IT-12

Note: The OCIO is not the owner of these processes. These NFRs were signed by and are the responsibility of the Office of Security and Integrity (OSI) and the Office of Human Capital and Training (HCT).

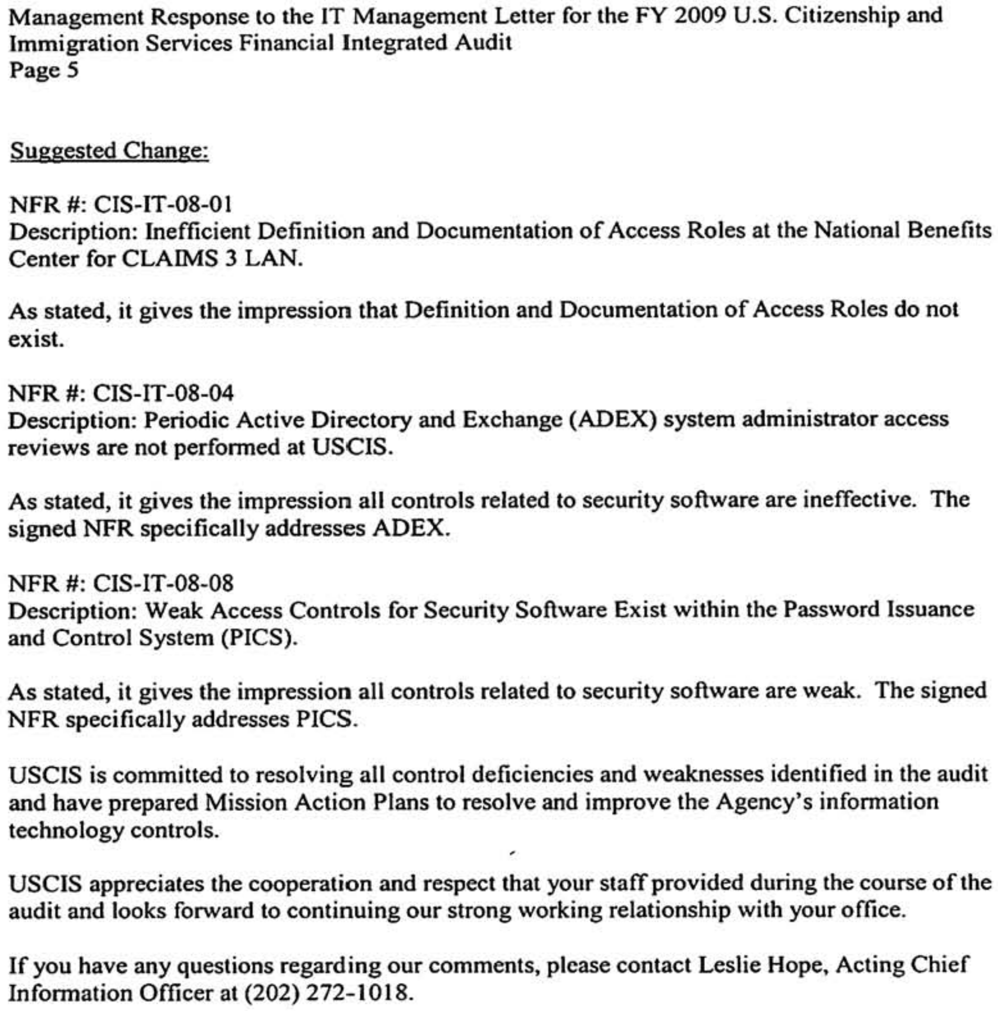
NFR #: CIS-IT-09-14

Note: The OCIO is not the owner of this process. This NFR was signed by and is the responsibility of the OCFO. They grant, remove, and monitor access to FFMS.

NFR #: CIS-IT-08-01
Description: Lack of Definition and Documentation of Access Roles at the National Benefits Center for CLAIMS 3 LAN.

NFR #: CIS-IT-08-04
Description: Ineffective Controls for Restricting Security Software Exist.

NFR #: CIS-IT-08-08
Description: Weak Access Controls for Security Software Exist.



Management Response to the IT Management Letter for the FY 2009 U.S. Citizenship and Immigration Services Financial Integrated Audit
Page 5

Suggested Change:

NFR #: CIS-IT-08-01
Description: Inefficient Definition and Documentation of Access Roles at the National Benefits Center for CLAIMS 3 LAN.

As stated, it gives the impression that Definition and Documentation of Access Roles do not exist.

NFR #: CIS-IT-08-04
Description: Periodic Active Directory and Exchange (ADEX) system administrator access reviews are not performed at USCIS.

As stated, it gives the impression all controls related to security software are ineffective. The signed NFR specifically addresses ADEX.

NFR #: CIS-IT-08-08
Description: Weak Access Controls for Security Software Exist within the Password Issuance and Control System (PICS).

As stated, it gives the impression all controls related to security software are weak. The signed NFR specifically addresses PICS.

USCIS is committed to resolving all control deficiencies and weaknesses identified in the audit and have prepared Mission Action Plans 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.

If you have any questions regarding our comments, please contact Leslie Hope, Acting Chief Information Officer at (202) 272-1018.

Appendix D

Report Distribution

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, Policy
Assistant Secretary for Public Affairs
Assistant Secretary for 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.