Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2010 DHS Financial Statement Audit

OIG-11-70

April 2011

Office of Inspector General

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

Homeland
Security

APR 07 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 Immigration and Customs Enforcement (ICE) 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 ICE 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 1, 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.

Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036

March 1, 2011

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
Immigration and Customs Enforcement

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.

Immigration and Customs Enforcement (ICE), is a component of DHS. During our audit engagement, we noted certain matters in the areas of information technology (IT) configuration management, access controls, security management, and segregation of duties with respect to ICE's 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.

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 ICE 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 ICE financial systems and IT infrastructure within the scope of our engagement to audit the FY 2010 DHS financial statements 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 ICE Chief Financial Officer.

ICE's 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 ICE 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
Immigration and Customs Enforcement
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 Control	**3**
Security Management	**3**
After-Hours Physical Security Testing	**4**
Social Engineering Testing	**4**
Segregation of Duties	**4**
Application Controls	**6**
Management's Comments and OIG Response	**6**

APPENDICES

Appendix	Subject	Page
A	Description of Key ICE 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 ICE	**9**
	• Notice of Findings and Recommendations – Definition of Severity Ratings	**10**
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at ICE	**20**
D	Management Response	**22**

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 ICE, to assist in planning and performing our audit. 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 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 key general support systems.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2010, ICE took corrective action to address some prior year IT control weaknesses. For example, ICE made improvements over physical controls at facility entrances, and Active Directory Exchange (ADEX) user account lockout settings and recertifications. However, during FY 2010, we continued to identify IT general control weaknesses that could potentially impact ICE's financial data. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System (FFMS) configuration and patch management, FFMS user account management, and weaknesses over physical security and security awareness. Collectively, the IT control deficiencies limited ICE'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 ICE 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 16 findings identified during our FY 2010 testing, 9 were new IT findings. These findings represent control deficiencies in four of the five FISCAM key control areas: configuration management, access controls, security management, and segregation of duties. Specifically, these control deficiencies include: 1) inadequately designed and operating configuration management, 2) lack of effective segregation of duties controls within financial applications, 3) lack of FFMS patch management, and 4) weak FFMS account management. These control deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and ICE 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 ICE, it is the ultimate responsibility of ICE 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 AND RECOMMENDATIONS

Findings:

During the FY 2010 DHS Financial Statement Audit, we identified the following ICE 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

- FFMS password settings are not compliant with DHS policy.
- A lack of recertification of FFMS system users.
- Audit log policies and procedures have not been finalized, approved, and implemented.
- ADEX system access was not consistently removed for terminated employees and contractors.
- Weak physical and environmental controls at the ADEX and FFMS datacenters:
  - Department of Commerce Office of Computer Services (OCS) (up to July 2010)
    - Lack of OCS Data Center risk assessment.
    - Lack of re-entry procedures for personnel after an emergency evacuation.
    - Fire suppression testing documentation is not maintained.
    - Water damage was visible on the data center wall where FFMS servers are housed with no incident report of the event.
    - Uninterruptible Power Supply (UPS) testing documentation is not maintained.
  - Clarksville Data Center (DC2) (as of July 2010)
    - Emergency re-entry procedures have not been documented and authorized.
    - FFMS server is inappropriately marked with a label that identifies the application/data on the server.
  - Potomac Center North (PCN)
    - Environmental test results are not documented and maintained for the Heating, Ventilating, Air Conditioning (HVAC), fire extinguishers, and the UPS.

Security Management

- Procedures for transferred and terminated personnel exit processing are not being consistently followed.
- IT Security training is not mandatory nor is compliance monitored.

After-Hours Physical Security Testing:

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to media and equipment that housed financial data and information residing within a ICE employee's or contractor's work area, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various ICE locations that process and/or maintain financial data. The specific results are listed as shown in the following table:

	Total Exceptions by Type			**Total**
Exceptions Noted	**TechWorld 10th floor**	**PCN 3rd floor**	**PCN 4th floor**	**Exceptions by Type**
User Name and Passwords	13	6	13	**32**
Keys/Badges	1	0	0	**1**
Personally Identifiable Information (PII)	9	2	2	**13**
Server Names/IP Addresses	1	0	2	**3**
Laptops	2	2	1	**5**
External Drives	0	0	1	**1**
Credit Cards	2	0	0	**2**
Internal Drive	1	0	1	**2**
Total Exceptions by Location	**29**	**10**	**20**	**59**

Social Engineering Testing:

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to deception for the purpose of information gathering, or gaining computer system access, as shown in the following table:

Total Called	**Total Answered**	**Number of people who provided a username and/or password**
25	14	1 – Both User Name and Password

<u>Segregation of Duties</u>

- FFMS roles and responsibilities for the Originator, Funds Certification Official, and Approving Official profiles were not effectively segregated.

Recommendations:

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

<u>For Configuration Management</u>

- 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 Access Controls

- Update the FFMS password configuration settings to ensure that they are in compliance with DHS 4300A policies.
- Establish and implement policies and procedures to formally document the recertification of FFMS user privileges. This process should include a method to document user recertification and a process to maintain evidence of the reviews.
- Finalize, approve, and implement the draft FFMS audit log policy and procedures.
- Ensure implementation of the ICE Exit Clearance Directive which will establish the process for separating employees, both Federal and contractors, and formalize a process to ensure that separating employees have their access to all ICE information technology systems removed.
- As of July 2010, FFMS was moved from the OCS to Clarksville Data Center (DC2). Therefore, we recommend that the Clarksville Data Center (DC2) be reviewed and monitored to ensure compliance with all physical and data security requirements.
- Ensure that re-entry procedures are properly documented at the Clarksville Data Center (DC2) and that servers are not inappropriately identified.
- Ensure that the HVAC, fire extinguishers, and UPS environmental systems are tested annually and the results are documented and maintained.

For Security Management

- Establish and implement a policy which governs the exit clearance process and identifies the procedures that separating employees and contractors must take to ensure the return and\or safeguarding of government property, equipment, and systems; and the roles and responsibilities of ICE offices involved in the exit clearance process.
- OCIO provide management oversight and guidance for training personnel with significant responsibilities for information security.
- Continue prioritizing security awareness and social engineering risks in the Annual Information Assurance Awareness Training (IAAT).

For Segregation of Duties

- Enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.

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'S COMMENTS AND OIG RESPONSE

The OIG received written comments on a draft of this report from ICE management. Generally, ICE management agreed with all of our findings and recommendations. ICE 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 ICE management is taking to satisfy these recommendations.

Appendix A

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

Federal Financial Management System (FFMS)

The FFMS is a Chief Financial Officer (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 Department of Homeland Security (DHS) Clarksville Data Center (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 National Finance Center (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 Active Directory/Exchange (ADEX) E-mail System, is a major application for ICE and other DHS components, such as the United States Citizenship and Immigration Services (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

Appendix B

FY 2010 Notices of IT Findings and Recommendations at ICE

<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 the DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Notice of Findings and Recommendations – Detail

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-10-01	During the FY 2009 financial statement audit, KPMG performed an inspection of a sample of personnel that had terminated/transferred from their employment with ICE during the fiscal year. KPMG requested evidence that exit clearance forms were completed for each employee to determine ICE management's compliance with exit clearance procedures. Of the 25 terminated/transferred ICE personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 12 employees. During the FY 2010 financial statement audit, KPMG was informed that a policy and procedure has not been developed for the Personnel Exiting Process. ICE management stated that the Office of Human Capital (OHC) has implemented a multi-year mission action plan to address this and various other issues, but there has been no corrective action taken at this time.	ICE should establish and implement a policy governing the exit clearance process, identifying the procedures separating employees and contractors must take to ensure the return and\or safeguarding of government property, equipment, and systems; and the roles and responsibilities of ICE offices involved in the exit clearance process.	X		3
ICE-IT-10-02	During the FY 2009 audit, KPMG inquired of ICE OCIO personnel about FFMS password settings. We determined that the FFMS password settings require the use of an underscore and does not allow the use of any other special characters such as !, @, #, $, %, or *, which is not compliant with DHS policy. The DHS policy requires that passwords contain a combination of alphabetic, numeric, and special characters. During the FY 2010 audit, we performed follow-up inquiry to determine the status of this weakness and	ICE should update the FFMS password configuration settings to ensure that they are in compliance with DHS 4300A policies.	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	learned that the FFMS password setting control weakness has not been remediated. ICE management stated that a change to the system has been requested to include two additional characters in the password complexity. The special characters that will be added once the change is implemented are the #, $, and underscore. KPMG noted that Oracle uses the following characters (!, @, %, ^, &, *) as function key, therefore, they cannot be included in the password complexity. The remediation completion date is scheduled for November 2010.				
ICE-IT-10-03	During the FY 2009 audit, KPMG inquired of ICE OCIO personnel about the process for recertifying FFMS user access (review of access privileges) and found that this process is not formally documented. Furthermore, KPMG found that the review for the access privileges for each FFMS account is not adequately recorded and no audit trail is available to support that a recertification was completed. During the FY 2010 financial statement audit, we performed follow-up inquiry to determine the status of this weakness and learned that procedures have been documented and implemented for the FFMS recertification process, however, a formal policy has not been documented. KPMG found that users' logical access privileges were reviewed, recorded, and maintained, therefore this portion of the PY NFR as been remediated. However, per inquiry with ICE management KPMG found that a formal policy still does not exist for the recertification of FFMS accounts.	ICE management should establish and implement policies and procedures to formally document the recertification of FFMS user privileges. This activity is the responsibility of OFM and the ISSO. This process should include a method to document user recertification and a process to maintain evidence of the reviews.	X		2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-10-04	During the FY 2009 financial statement audit, KPMG performed an inspection of a listing of FFMS users and their assigned roles/responsibilities and determined that 6 users had Originator, Funds Certification Official, and Approving Official profiles that were in violation of FFMS segregation of duties policies. During the FY 2010 financial statement audit, we performed follow-up inquiry to determine the status of this weakness and learned that draft FFMS segregation of duty policy is in place, but, is not being followed. In addition, KPMG inspected a listing of FFMS users and their assigned roles/responsibilities and determined that one user had Originator, Funds Certification Official, and a Approving Official profile, which is a violation of the FFMS segregation of duties policy.	ICE should enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.	X		3
ICE-IT-10-05	During the FY 2010 financial statement audit, KPMG determined that FFMS audit logs were not generated or reviewed during the period October 2009 through February 2010. As of March 2010, the logs were generated and reviewed, however, no supporting evidence could be provided. Additionally, we determined that audit log policy and procedures have been drafted; however, they have not been finalized, approved, and implemented.	ICE OFM will finalize, seek approval, and formally implement the draft policy and procedures. In the meantime, the draft policy will be used to provide an accurate audit log.	X		3
ICE-IT-10-06	During the FY 2009 financial statement audit, KPMG determined that weaknesses exist over ADEX access. Specifically, KPMG found that 14 users, which were separated from ICE, still had active ADEX accounts that were not removed upon their termination/transfer.	Ensure implementation of the ICE Exit Clearance Directive which will establish the process for separating employees, both Federal and contractors, and formalize a process to ensure that separating employees have their access to all ICE	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	During the FY 2010 financial statement audit, we performed follow-up inquiry to determine the status of this weakness and learned that ICE has implemented a compensating control that will disable users account after 45 days of inactivity to mitigate the control weakness. However, KPMG found that a separated employee's account was not disabled in a timely manner as the account was accessed after the employee's termination date. Therefore, the 45-day window was inappropriately delayed. In addition, we determined that DHS access controls policies are not being followed as users are not properly identified and authenticated. Based on ICE management's response to this weakness "either another user logged on as the terminated user or Information Technology Field Officer (ITFO) logged in using the terminated employee's credentials."	information technology systems removed.			
ICE-IT-10-07	During the FY 2010 financial statement audit, KPMG determined that several physical and environmental controls exist within the OCS Datacenter. Specifically, we noted the following: • OCS Data Center Risk Assessment is not documented. • Re-entry procedures for personnel after an emergency evacuation are not documented. • Fire suppression testing documentation is not maintained. • Water damage was visible on the data center wall where FFMS servers are housed with no incident report of the event. • UPS testing documentation is not maintained.	As of July 2010 FFMS has been moved from the Department of Commerce OCS to the Clarksville Data Center 2 (DC2). DC2 will be reviewed and monitored to ensure compliance with all physical and data security requirements.	X		2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-10-08	During the FY 2010 financial statement audit, we determined that the environmental controls in the PCN computer room need improvement. Specifically, we found that environmental test results are not documented and maintained for the following devices: AC units, fire extinguishers, and back-up power supply.	Ensure that environmental systems (HVAC, fire extinguishers, and UPS) are tested annually with test results made available for review.	X		2
ICE-IT-10-09	Social engineering is defined as the act of attempting to manipulate or deceive people into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing/enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or computer system access. During the course of our social engineering test work, the objective was primarily focused on attempting to identify user IDs and passwords. Posing as DHS technical support employees, attempts were made to obtain this type of account information by contacting randomly selected employees by telephone. A script was used to ask for assistance from the ICE user in resolving a network issue in the component. For each person we attempted to call, we noted whether the individual was reached and whether we obtained any information from them that should not have been shared with us according to DHS policy. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. During the FY 2010 financial statement audit, we learned that ICE continues to promote security awareness training by distributing a weekly newsletter	Social Engineering is covered in the Annual Information Assurance Awareness Training (IAAT) – which is a requirement for all ICE employees. The IAAT should continue to stress social engineering risks and greater outreach should be achieved.	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	to employees and contractors about security awareness. However, KPMG found that the prior year security weakness still exists.				
ICE-IT-10-10	We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to equipment that houses financial data and information residing on an ICE employee's desk which could be used by others to inappropriately access financial information. The testing was performed at various ICE locations that process and/or maintain component financial data. After gaining access to the facilities via an ICE employee designated to assist with and monitor our testwork, we inspected a random selection of desks and offices looking for items such as improper protection of system user names and passwords, unsecured information system hardware, documentation containing Personally Identifiable Information (PII) or marked "For Official Use Only" (FOUO), and unlocked network sessions. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. For each location visited, we noted the type of unsecured information or property we identified and included the total exceptions noted by location, as well as by type of information or property identified. During the FY 2010 financial statement audit, we learned that ICE continues to promote security awareness training and distributes a weekly newsletter to employees and contractors about security awareness. However, KPMG found that security	Security Awareness is covered in the Annual IAAT – which is a requirement for all ICE employees. The IAAT should continue to stress security awareness risks and greater outreach should be achieved.	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	weaknesses still exist.				
ICE-IT-10-11	In FY 2009, we found that ICE lacked policies and procedures requiring completion of a training program by personnel in IT security positions. During the FY 2010 financial statement audit, we learned that to correct the prior year NFR, ICE follows DHS 4300A policy for training personnel in IT security positions, therefore, this portion of the NFR is closed. However, during our testwork we determined that weaknesses still exist over training personnel in IT security positions. Specifically, we determined that 27 out of 45 IT security personnel have not completed specialized training.	OCIO will provide management oversight and guidance for training personnel with significant responsibilities for information security.	X		2
ICE-IT-10-12	During the FY 2010 financial statement audit, KPMG determined that physical safeguard weaknesses exist at the Clarksville Data Center (DC2). 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.	ICE should ensure that re-entry procedures are properly documented at the Clarksville Data Center (DC2) and make certain that servers are not inappropriately identified.	X		2
ICE-IT-10-13	During KPMG's internal vulnerability assessment efforts of ICE's FFMS network, servers and databases performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to configuration management such as: • Hot Standby Router Protocol (HSRP) default installation on Cisco routers and switches • Default "Oracle Listener Program (tnslsnr)" service password on server installation	ICE should take the necessary steps to begin examining the default configuration installations and system services installed on FFMS devices and determine if the default configurations can be set to increase FFMS's security or, in the case of unnecessary system services, deleted to reduce FFMS vulnerability to attack.	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• Outdated Microsoft Operating Systems • Bonjour (also known as ZeroConf or mDNS) listening protocol • Remote web server HTML form fields transmits data in clear text				
ICE-IT-10-14	During KPMG's internal vulnerability assessment efforts of ICE's FFMS network servers and databases performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to several configuration and patch management weaknesses within the configuration of the FFMS ICE and United State Citizenship and Immigration Service (USCIS) Oracle database instances such as: • Clear text passwords stored in database • Outdated patches • Table security configurations • User account privileges • Password settings for users and database	ICE should take the necessary steps to begin applying the appropriate FFMS database patches to ensure patch compliance.	X		3
ICE-IT-10-15	During KPMG's internal vulnerability assessment efforts of ICE's FFMS network servers and databases performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to missing or inadequate patches such as: • Microsoft Patches • Adobe Reader • Apache Tomcat • Java Runtime Environment (JRE) • Oracle Database (server installation) • HP System Management • Internet Explorer	ICE should take the necessary steps to begin applying the appropriate FFMS patches to the FFMS network servers and databases to ensure patch compliance.	X		3

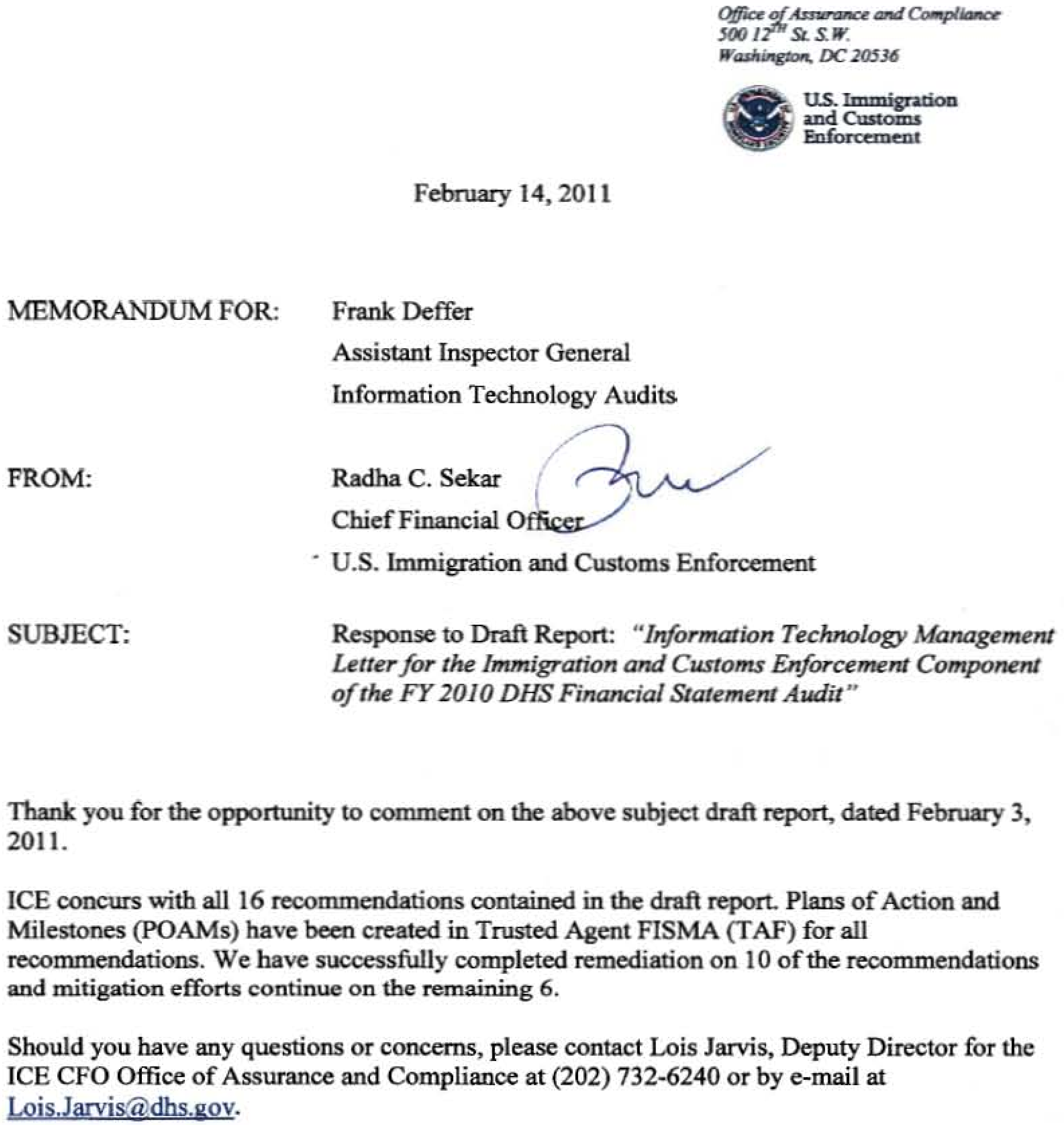
NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• MySQL database				
ICE-IT-10-16	During KPMG's internal vulnerability assessment efforts of ICE's ADEX network servers and devices performed in August 2010, KPMG identified a default installation and configurations for the Hot Standby Router Protocol (HSRP) on the Cisco routers.	ICE should ensure that password configuration settings are properly and effectively applied.	X		3

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison to

Current Year Notices of Findings and Recommendations at ICE

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
ICE-IT-09-11	Ineffective physical security controls at facility entrances	X	
ICE-IT-09-12	Ineffective/non-compliant account lockout counter settings	X	
ICE-IT-09-13	Ineffective password settings in FFMS		10-02
ICE-IT-09-14	Ineffective ADEX user access recertification process	X	
ICE-IT-09-15	Ineffective FFMS access recertification process		10-03
ICE-IT-09-16	Terminated/transferred personnel are not removed from ADEX in a timely manner		10-06
ICE-IT-09-17	Segregation of duty policies are not enforced in FFMS		10-04
ICE-IT-09-18	Background reinvestigations are not conducted in a timely manner for contractors	X	
ICE-IT-09-19	Procedures for transferred/terminated personnel exit processing are not allowed	X	10-01
ICE-IT-09-20	Training for IT security personnel is not mandatory		10-11
ICE-IT-09-21	Vulnerability Assessment - Network devices were installed with default configuration settings and protocols; inadequate patches; and weak/ generic passwords		10-13 through 10-16
ICE-IT-09-22	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		10-09
ICE-IT-09-23	IT Security Awareness Training requirements are not enforced	X	



Office of Assurance and Compliance
500 12TH St. S.W.
Washington, DC 20536

U.S. Immigration
and Customs
Enforcement

February 14, 2011

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Radha C. Sekar
Chief Financial Officer
U.S. Immigration and Customs Enforcement

SUBJECT: Response to Draft Report: *"Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2010 DHS Financial Statement Audit"*

Thank you for the opportunity to comment on the above subject draft report, dated February 3, 2011.

ICE concurs with all 16 recommendations contained in the draft report. Plans of Action and Milestones (POAMs) have been created in Trusted Agent FISMA (TAF) for all recommendations. We have successfully completed remediation on 10 of the recommendations and mitigation efforts continue on the remaining 6.

Should you have any questions or concerns, please contact Lois Jarvis, Deputy Director for the ICE CFO Office of Assurance and Compliance at (202) 732-6240 or by e-mail at Lois.Jarvis@dhs.gov.

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Assistant Secretary, ICE
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, ICE
Chief Information Officer, ICE
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
ICE 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.