Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2011 DHS Financial Statement Audit

OIG-12-50

March 2012

Office of Inspector General

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

Homeland
Security

March 14, 2012

Preface

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

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

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

Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

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

February 16, 2012

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
U.S. Immigration and Customs Enforcement

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

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

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

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to DHS' financial systems general Information Technology (IT) controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. We also noted that in some cases, financial system functionality is inhibiting

DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

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

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and are intended For Official Use Only. We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key DHS financial systems within the scope of the FY 2011 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls (comments not related to IT) have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General (OIG), U.S. Office of Management and Budget (OMB), U.S. Government Accountability Office (GAO), and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our audit of DHS' balance sheet as of September 30, 2011 and the related statement of custodial activity for the year then ended, we performed an evaluation of the general information technology general controls (GITC) at ICE, to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A.

The FISCAM, issued by GAO, formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A. FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the 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 GITC audit procedures, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls in the ICE environment. The technical security testing was performed both over the Internet and from within select ICE facilities, and focused on test, development, and production devices that directly support key general support systems.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2011, ICE took corrective action to address some prior year IT control weaknesses. For example, ICE made improvements over mandatory training for IT security personnel, and Federal Financial Management Systems (FFMS) password configurations. However, during FY 2011, 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 FFMS configuration and patch 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. In addition, based upon the results of our test work, we noted that ICE contributes to the DHS' non-compliance with the requirements of the *Federal Financial Management Improvement Act*.

Of the 11 findings identified during our FY 2011 testing; only 2 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 a financial application, 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.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2011 DHS Financial Statement Audit, we identified the following ICE IT and financial system control deficiencies that in the aggregate contribute to the material weakness at the Department level.

<u>Configuration Management</u>

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

<u>Access Control</u>

- A lack of recertification of FFMS system users.
- ADEX system access was not consistently removed for terminated employees and contractors.

<u>Security Management</u>

- Procedures for transferred and terminated personnel exit processing have not been reviewed, implemented, nor authorized by ICE management.

After-Hours Physical Security Testing:

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to media and equipment that housed financial data and information residing within an 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 by Type**
Exceptions Noted	**OCIO/OFM TechWorld 10th floor**	**OCIO PCN 3rd floor**	**OCFO PCN 4th floor**	
User Name and Passwords	5	3	1	**9**
Keys/Badges	2	0	1	**3**
Personally Identifiable	7	3	2	**12**

Information (PII)				
Server Names/IP Addresses	0	5	0	**5**
Laptops	6	1	6	**13**
External Drives	0	3	0	**3**
Credit Cards	1	0	1	**2**
Air Card	1	0	0	**1**
FOUO	8	6	3	**17**
Total Exceptions by Location	**30**	**21**	**14**	**65**

In addition, a KPMG team member was able to access the Techworld facility using their KPMG badge, which is not assigned nor recognized by any of the agencies within the Techworld facility.

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
36	25	1 – Both User Name and Password

Segregation of Duties

- FFMS roles and responsibilities for the 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.

For Configuration Management

- Implement an immediate and long term remediation strategy to resolve the ADEX authentication weaknesses. In addition, configuration management procedures and templates should be reviewed and modified as appropriate.
- Examine the default configuration installations and system services installed on FFMS network devices and remove unnecessary system services.
- Ensure that password configuration settings are properly and effectively applied.
- Assess the patch deployment and testing processes and develop a process for patching applications across the enterprise.
- Implement appropriate FFMS database and network server patches and configuration baseline parameters consistent with DHS guidelines.

For Access Controls

- Enforce the existing policies and procedures to recertify FFMS user privileges at the end of each calendar year.
- 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.

For Security Management

- Complete the implementation of the 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.
- Continue prioritizing security awareness and social engineering risks in the Annual Information Assurance Awareness Training.

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.

Appendix A

Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2011 DHS Financial Statement Audit

Federal Financial Management System (FFMS)

The FFMS is a CFO designated financial system and certified software application that conforms to OMB Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS is a commercial off-the-shelf financial reporting system. It includes the core system used by accountants, FFMS Desktop for users, and a National Finance Center (NFC) payroll interface. FFMS currently interfaces with the following systems:

- Direct Connect for transmission of DHS payments to the U.S. Treasury
- Fed Traveler
- The Biweekly Examination Analysis Reporting and Controlling Accounting Data Inquiry, for the purpose of processing NFC user account and payroll information.
- The Debt Collection System
- Bond Management Information System 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 Immigration Services. 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, D.C. ADEX currently interfaces with the Diplomatic Telecommunications Service Program Office ICENet Infrastructure.

Appendix B

FY 2011 Notices of IT Findings and Recommendations at ICE

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

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

1 – Not substantial

2 – Less significant

3 – More significant

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

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

Appendix B

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2011

Notice of Findings

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
ICE-IT-11-01	ADEX Resource Servers and Workstations have Inadequate Patch Management	Configuration Management	3	X	
ICE-IT-11-02	Terminated/Transferred Personnel are not Removed from ADEX in a Timely Manner	Access Controls	2		X
ICE-IT-11-03	Access Recertification Review is not completed for FFMS	Access Controls	2	X	
ICE-IT-11-04	Weak FFMS Segregation of Duties	Segregation of Duties	2		X
ICE-IT-11-05	Security Awareness issues were identified during Social Engineering	Security Management	3		X
ICE-IT-11-06	FFMS Network and Servers were installed with Default Configuration Settings and Protocols	Configuration Management	3		X
ICE-IT-11-07	FFMS Mainframe Production databases were installed and configured without baseline security configurations	Configuration Management	3		X
ICE-IT-11-08	FFMS servers have inadequate patch management	Configuration Management	3		X
ICE-IT-11-09	Default installation and configuration of Cisco routers on ICE Network	Access Controls\ Configuration Management	3		X
ICE-IT-11-10	Security Awareness issues identified during After-Hours Walkthrough	Security Management	3		X
ICE-IT-11-11	Lack of procedures for transferred/terminated personnel exit processing	Security Management	2		X

Appendix C

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

Appendix C

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
ICE-IT-10-01	Procedures for Transferred/Terminated Personnel Exit Processing are not Followed		X
ICE-IT-10-02	Ineffective Password Settings in FFMS	X	
ICE-IT-10-03	Formal policy for FFMS Access Recertification is not Documented and Approved	X	
ICE-IT-10-04	Weak FFMS Segregation of Duties		X
ICE-IT-10-05	Audit Log Policies and Procedures are not Documented for FFMS.	X	
ICE-IT-10-06	Terminated/transferred personnel are not removed from ADEX in a timely manner		X
ICE-IT-10-07	Weak Environmental Controls at the OCS Datacenter	X	
ICE-IT-10-08	Weak Environmental Controls at the PCN Computer Room	X	
ICE-IT-10-09	Security Awareness Issues Identified during Social Engineering		X
ICE-IT-10-10	Security Awareness issues Identified during After-Hours Walkthrough		X
ICE-IT-10-11	Training for IT Security Personnel is not Mandatory	X	
ICE-IT-10-12	Physical Safeguard Weaknesses exist at DHS DC2 Datacenter	X	
ICE-IT-10-13	FFMS Network and Servers were Installed with Default Configuration Settings and Protocols		X
ICE-IT-10-14	FFMS Mainframe Production databases were Installed and Configured without Baseline Security Configurations		X
ICE-IT-10-15	FFMS Servers have Inadequate Patch Management		X
ICE-IT-10-16	Default Installation and Configuration of Cisco Routers on ICE Network		X

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2010

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 Policy
Assistant Secretary for Public Affairs
Assistant Secretary for 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 e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603
- Fax the complaint directly to us at (202)254-4292
- E-mail us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:

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

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