Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2012 Department of Homeland Security Financial Statement Audit

OIG-13-60

April 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

April 24, 2013

MEMORANDUM FOR: Luke McCormack
Chief Information Officer
U.S. Immigration and Customs Enforcement

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

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2012 Department of Homeland Security Financial Statement Audit*

Attached for your action is our final report, *Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2012 Department of Homeland Security Financial Statement Audit.* The independent accounting firm KPMG LLP (KPMG) performed the audit of Department of Homeland Security (DHS) financial statements as of September 30, 2012, and prepared this information technology (IT) management letter.

KPMG is responsible for the attached IT management letter dated December 20, 2012, and the conclusion expressed in it. We do not express an opinion on DHS' financial statements or internal controls or conclusions on compliance with laws and regulations. The DHS management concurred with all recommendations.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Audit Division, at (202) 254-5451.

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

April 4, 2013

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, 2012, and the related statements of net cost, changes in net position, and custodial activity, and combined statement of budgetary resources for the year then ended (referred to as the "fiscal year (FY) 2012 financial statements"). We were also engaged to audit the Department's internal control over financial reporting of the FY 2012 financial statements. The objective of our audit engagement was to express an opinion on the fair presentation of the FY 2012 financial statements and the effectiveness of internal control over financial reporting of the FY 2012 financial statements.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 14, 2012, included internal control deficiencies identified during our audit engagement that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to U.S. Immigration and Customs Enforcement (ICE).

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, and segregation of duties with respect to ICE financial systems general IT controls (GITC) which we believe contribute to a DHS Department-wide material weakness in IT controls and financial system functionality. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The comments described herein have been discussed with the appropriate members of management, or communicated through Notices of Findings and Recommendations (NFRs), 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 ICE financial systems and IT infrastructure within the scope of the FY 2012 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of 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 (OIG) and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS 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 engagement to audit the financial statements of DHS as of and for the year ended September 30, 2012, we performed an evaluation of the general Information Technology (IT) controls (GITCs) at ICE to assist in planning and performing our audit engagement. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A.

FISCAM was designed to inform financial statement 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 statement audit. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a Federal agency. FISCAM defines the following five control functions to be essential to the effective operation of GITCs and the IT 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 assessed corrective actions implemented to address prior year findings over technical security testing for key network and system devices and key financial application controls in the ICE environment.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2012, ICE took corrective action to address some prior year IT control weaknesses. For example, ICE made improvements in removing terminated network user accounts in a timely manner. However, during FY 2012, we continued to identify GITC weaknesses that could potentially impact ICE's financial data. The most significant findings were related to Federal Financial Management System (FFMS) configuration and patch management, and weaknesses over physical security and FFMS segregation of duties. 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 1996*.

Of the 13 findings identified during our FY 2012 testing, 3 were new. 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. Security awareness.

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 us 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.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following ICE GITC deficiencies that in the aggregate contribute to the IT material weakness at the Department level.

Configuration Management

- Security configuration management control deficiencies exist on the Active Directory Exchange (ADEX) and the Infrastructure Support systems network servers and workstations. These control deficiencies included default installation and configuration settings and protocols.
- 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.

Access Controls

- A lack of recertification of ADEX and FFMS system users.
- FFMS users were not properly authorized and approved.

Segregation of Duties

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

Security Management

- 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:

Exceptions Noted	Exceptions Noted at PCN – 4th Floor	Exceptions Noted at Portals III – 4th Floor	Exceptions Noted at 801 I St – 7th Floor
Passwords	1	2	10
For Official Use Only (FOUO)	3	4	15
Keys	1	0	3
Personally Identifiable Information (PII)	2	3	1
Unlocked Laptops	1	2	6
Server Names/Internet Protocol (IP) Addresses	0	1	0
Credit Cards	0	0	2
Total Exceptions at ICE	**8**	**12**	**37**

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.

Configuration Management

- Implement continuous monitoring of the IT environment to assess, evaluate, and identify security vulnerabilities on a scheduled and recurring basis;
- 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; and
- Implement appropriate FFMS database and network server patches and configuration baseline parameters consistent with DHS guidelines.

Access Controls

- Enforce the existing policies and procedures to recertify FFMS user privileges at the end of each calendar year;
- Ensure ADEX user account recertification is completed annually; and
- Maintain FFMS access forms as evidence of approval and authorization of user accounts.

Segregation of Duties

- Enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions. Continue with the initiative to remove existing access conflicts and implement a monitoring plan to identify potential conflicts among user roles.

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; and
- Prioritize security awareness in the Annual Information Assurance Awareness Training.

APPLICATION CONTROLS

Select application controls were tested for the year ending September 30, 2012, and no issues were identified associated with those controls selected for test work.

Appendix A

Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2012 DHS Financial Statement Audit

Below is a description of significant ICE financial management systems and supporting IT infrastructure included in the scope of the ICE component of the DHS FY 2012 financial statement audit.

Federal Financial Management System (FFMS)

The FFMS is a Chief Financial Officer 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 that is used by average users, and a National Finance Center payroll interface. The FFMS mainframe component and 14 servers are hosted at the DHS DC2 facility located in Virginia. FFMS currently interfaces with Treasury, BMIS Web, and FedTraveler.

ICE Network

The ICE Network, also known as the ADEX E-mail System, is a major application for ICE. The ADEX servers and infrastructure for the headquarters and National Capital Area are located in Mississippi and Virginia. ADEX currently interfaces with the Diplomatic Telecommunications Service Program Office ICENet Infrastructure.

Appendix B
FY 2012 Notices of IT Findings and Recommendations at ICE

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2012

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-12-01	FFMS Network and Servers were Installed with Default Configuration Settings and Protocols	Configuration Management		X
ICE-IT-12-02	FFMS Mainframe Production Databases were Installed and Configured without Baseline Security Configurations	Configuration Management		X
ICE-IT-12-03	FFMS Servers have Inadequate Patch Management	Configuration Management		X
ICE-IT-12-04	FFMS Access Recertification Reviews are Not Completed	Access Controls		X
ICE-IT-12-05	Weak FFMA Segregation of Duties	Segregation of Duties		X
ICE-IT-12-06	Security Awareness Issues Identified During After-Hours Walkthrough	Security Management		X
ICE-IT-12-07	Lack of Procedures for Transferred/Terminated Personnel Exit Processing	Access Controls		X
ICE-IT-12-08	ICE Servers and Workstation have Inadequate Patch Management	Access Controls		X
ICE-IT-12-09	ICE Servers and Workstations were Installed with Default Configuration Settings and Protocols	Configuration Management	X	
ICE-IT-12-10	Lack of Recertification for ADEX Users	Access Control	X	
ICE-IT-12-11	Inadequate FFMS User Access Request Forms	Access Control	X	

Appendix C

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

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2012

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

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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